

Cisco IOS Voice Command Reference - T through Z

First Published: 2015-08-04

Last Modified: 2026-04-25

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **target carrier-id through timeout tsmax** 1

target carrier-id 3

target trunk-group-label 4

tbct clear call 5

tbct max call-duration 7

tbct max calls 8

tcp-retry 9

tdm-group 10

tech-prefix 12

tel-config to-hdr 14

telephony-service 16

telephony-service ccm-compatible (H.323 voice-class) 20

telephony-service ccm-compatible (H.323 voice-service) 22

test dsmp delete-stream 24

test voice mos-calc 25

text relay modulation 26

text relay protocol 28

text relay rtp 29

tftp-server address 31

tgrep address-family 32

tgrep advertise (dial peer) 33

tgrep advertise (trunk group) 34

tgrep local-itad 36

threshold noise 37

timeout (auto-config application) 38

timeout leg3 39

timeout ptt 40
timeout tcrit 41
timeout tdinit 43
timeout tdmax 45
timeout tdmin 47
timeout thist 49
timeout tone busy 50
timeout tone cot1 51
timeout tone cot2 52
timeout tone dial 53
timeout tone dial stutter 54
timeout tone mwi 55
timeout tone network 56
timeout tone reorder 58
timeout tone ringback 59
timeout tone ringback connection 60
timeout tone ringing 61
timeout tone ringing distinctive 62
timeout tpar 63
timeout tsmax 65

CHAPTER 2 **timeouts call-disconnect through timing clear-wait** 67

timeouts call-disconnect 69
timeouts initial 71
timeouts interdigit (voice port) 72
timeouts power-denial 73
timeouts ringing 74
timeouts wait-release 75
timeouts teardown lmr 76
timer accessrequest sequential delay 77
timer cluster-element 78
timer irr period 80
timer lrq seq delay 81
timer lrq seq delay centisec 82

timer lrq window 83
timer lrq window decisec 84
timer media-inactive 85
timer receive-rtcp 87
timer receive-rtp 89
timer server retry 90
timer server timeout 91
timers 92
timers buffer-invite 94
timers comet 95
timers connect 96
timers connection aging 98
timers connection establish 99
timers disconnect 100
timers dns 102
timers expires 103
timers hold 105
timers info 106
timers keepalive 107
timers notify 109
timers options 111
timers prack 112
timers refer 114
timers register 115
timers rel1xx 116
timers trying 118
timers update 120
timing answer-winkwidth 121
timing clear-wait 122

CHAPTER 3 **timing delay-duration through type (voice)** 125
timing delay-duration 127
timing delay-start 129
timing delay-voice tdm 131

timing delay-with-integrity 133
timing dialout-delay 135
timing dial-pulse min-delay 137
timing digit 139
timing guard-out 141
timing hangover 142
timing hookflash-in 143
timing hookflash-out 145
timing ignore m-lead 146
timing interdigit 147
timing opx-ringwait 149
timing percentbreak 150
timing pulse 151
timing pulse-interdigit 153
timing sup-disconnect 155
timing wait-wink 157
timing wink-duration 159
timing wink-wait 161
tls 163
toggle-between-two-calls 164
token-root-name 166
tone busytone 168
tone dialtone 169
tone incoming 171
tone incoming system 173
tone ringback alert-no-PI 174
trace (voice service voip) 175
transfer 177
translate 179
translate (translation profiles) 181
translate-outgoing 183
translation-profile (dial peer) 185
translation-profile (source group) 186
translation-profile (trunk group) 187

translation-profile (voice port) 188
translation-profile (voice service POTS) 189
translation-rule 191
transport (sip-ua) 193
transport switch 197
trunk group (global) 198
trunk-group (CAS custom) 200
trunkgroup (dial peer) 202
trunk-group (interface) 204
trunk-group (voice port) 206
trunk-group-label (dial peer) 208
trunk-group-label (voice source group) 209
trustpoint (DSP farm profile) 210
trustpoint (voice class) 211
ttl 213
type (settlement) 214
type (voice) 216

CHAPTER 4 U 219
uc wsapi 220
uc secure-wsapi 221
unbundle vfc 222
update-callerid 223
url 224
url (dial peer) 226
url (SIP) 227
usage-indication 229
use-proxy 230
user-id 233

CHAPTER 5 vad (dial peer) through voice-class sip encap clear-channel 235
vad (dial peer) 238
vad (SPA-DSP) 240
vbd-playout-delay 242

vbr-rt 244
vcci 246
video codec (dial peer) 247
video codec (voice class) 249
video screening 251
violation 252
violation (media profile) 254
vmwi 256
vofr 257
voice 260
voicecap configure 261
voicecap entry 262
voice call capacity mir 264
voice call capacity reporting 266
voice call capacity stw 268
voice call capacity timer interval 270
voice call convert-discpi-to-prog 271
voice call csr data-points 273
voice call csr recording interval 274
voice call csr reporting interval 275
voice call debug 276
voice call disc-pi-off 279
voice call rate monitor 280
voice call send-alert 281
voice call trap deviation 282
voice call trigger hwm 283
voice call trigger lwm 285
voice call trigger percent-change 287
voice-card 289
voice cause-code 291
voice class aaa 292
voice class busyout 294
voice class called number 296
voice class cause-code 298

voice class codec 299
voice class custom-cptone 301
voice class dscp-profile 302
voice class dualtone 303
voice class dualtone-detect-params 305
voice class e164-pattern-map 306
voice-class dpg 307
voice class e164-pattern-map load 309
voice class e164-translation 310
voice class h323 311
voice class media 312
voice class permanent 313
voice class resource-group 315
voice class route-string 316
voice class server-group 317
voice class sip-copylist 319
voice class sip-hdr-passthrulist 320
voice class sip-profiles 321
voice class srtp-crypto 322
voice class tenant 324
voice class tls-profile 325
voice class tls-cipher 327
voice class tone-signal 328
voice class uri 330
voice class uri sip preference 332
voice-class aaa (dial peer) 334
voice-class called-number (dial peer) 335
voice-class called-number-pool 336
voice-class codec (dial peer) 337
voice-class h323 (dial peer) 339
voice-class permanent (dial-peer) 340
voice-class permanent (voice-port) 342
voice-class sip anat 344
voice-class sip asserted-id 345

voice-class sip associate registered-number 347
voice-class sip asymmetric payload 348
voice-class sip audio forced 349
voice-class sip authenticate redirecting-number 350
voice-class sip bind 352
voice-class sip block 353
voice-class sip call-route 356
voice-class sip calltype-video 358
voice-class sip content sdp version increment 359
voice-class sip copy-list 360
voice-class sip e911 361
voice-class sip-event-list 362
voice-class sip early-media update block 363
voice-class sip encap clear-channel 364

CHAPTER 6 **voice-class sip error-code-override through vxml version 2.0** 367

voice-class sip error-code-override 370
voice-class sip g729 annexb-all 373
voice-class sip history-info 375
voice-class sip localhost 376
voice-class sip map resp-code 378
voice-class sip midcall-signaling 380
voice-class sip nat media-keepalive 382
voice-class sip options-keepalive 384
voice-class sip options-keepalive profile 386
voice-class sip outbound-proxy 387
voice-class sip preloaded-route 389
voice-class sip privacy 390
voice-class sip privacy-policy 393
voice-class sip random-contact 395
voice-class sip random-request-uri validate 397
voice-class sip referto-passing 399
voice-class sip registration passthrough 400
voice-class sip rel1xx 402

voice-class sip requri-passing 404
voice-class sip reset timer expires 405
voice-class sip resource priority dscp-profile 407
voice-class sip resource priority mode (dial-peer) 408
voice-class sip resource priority namespace (dial-peer) 409
voice-class sip rsvp-fail-policy 411
voice-class sip send 180 sdp 413
voice-class sip srtp-auth 414
voice-class sip srtp-crypto 416
voice-class sip srtp negotiate 418
voice-class sip tel-config to-hdr 420
voice-class sip tenant 421
voice-class sip transport switch 422
voice-class sip url 423
voice-class source interface 425
voice-class stun-usage 426
voice-class tone-signal 427
voice-ctl-file 428
voice confirmation-tone 429
voice dnis-map 430
voice dnis-map load 432
voice dsp crash-dump 433
voice dsp invalid-msg drop 435
voice echo-canceller extended 436
voice enum-match-table 439
voice hpi capture 441
voice hunt 443
voice iec syslog 448
voice local-bypass 449
voice mlpp 450
voicemail (stcapp-fsd) 451
voice pcm capture 453
voice-phone-proxy 455
voice-phone-proxy file-buffer 456

voice-phone-proxy tftp-address 457
voiceport 458
voice-port 460
voice-port (MGCP profile) 462
voice-port busyout 463
voice rtp send-recv 464
voice rtp source-filter 465
voice-service dsp-reservation 466
voice service 467
voice sip sip-profiles 468
voice sip oauth get-keys 469
voice source-group 470
voice statistics accounting method 471
voice statistics display-format separator 473
voice statistics field-params 475
voice statistics max-storage-duration 477
voice statistics push 479
voice statistics time-range 481
voice statistics type csr 484
voice statistics type iec 486
voice translation-profile 487
voice translation-rule 488
voice vad-time 489
voice vrf 490
voip-incoming translation-profile 491
voip-incoming translation-rule 492
voip trunk group 494
volume 495
vxml allow-star-digit 497
vxml logging-tag 498
vxml audioerror 499
vxml tree memory 500
vxml version 2.0 501

CHAPTER 7 W 503

watcher all 504

xsvc 505

CHAPTER 8 X 507

xfer target 508

CHAPTER 9 Z 509

zone access 510

zone bw 512

zone circuit-id 513

zone cluster local 515

zone cluster remote 516

zone qos 518

zone local 520

zone prefix 522

zone remote 526

zone subnet 529



target carrier-id through timeout tsmax

- target carrier-id, on page 3
- target trunk-group-label, on page 4
- tbct clear call, on page 5
- tbct max call-duration, on page 7
- tbct max calls, on page 8
- tcp-retry, on page 9
- tdm-group, on page 10
- tech-prefix, on page 12
- tel-config to-hdr, on page 14
- telephony-service, on page 16
- telephony-service ccm-compatible (H.323 voice-class), on page 20
- telephony-service ccm-compatible (H.323 voice-service), on page 22
- test dsmp delete-stream, on page 24
- test voice mos-calc, on page 25
- text relay modulation, on page 26
- text relay protocol, on page 28
- text relay rtp, on page 29
- tftp-server address, on page 31
- tgrep address-family, on page 32
- tgrep advertise (dial peer), on page 33
- tgrep advertise (trunk group), on page 34
- tgrep local-itad, on page 36
- threshold noise, on page 37
- timeout (auto-config application), on page 38
- timeout leg3, on page 39
- timeout ptt, on page 40
- timeout tcrit, on page 41
- timeout tdinit, on page 43
- timeout tdmax, on page 45
- timeout tdmin, on page 47
- timeout thist, on page 49
- timeout tone busy, on page 50
- timeout tone cot1, on page 51

- timeout tone cot2, on page 52
- timeout tone dial, on page 53
- timeout tone dial stutter, on page 54
- timeout tone mwi, on page 55
- timeout tone network, on page 56
- timeout tone reorder, on page 58
- timeout tone ringback, on page 59
- timeout tone ringback connection, on page 60
- timeout tone ringing, on page 61
- timeout tone ringing distinctive, on page 62
- timeout tpar, on page 63
- timeout tsmax, on page 65

target carrier-id



Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

To configure debug filtering for the target carrier ID, use the **target carrier-id** command in call filter match list configuration mode. To disable, use the **no** form of this command.

target carrier-id *string*
no target carrier-id *string*

Syntax Description

string	Alphanumeric identifier for the carrier ID.

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the voice call debug filter set to match target carrier ID 4321:

```
call filter match-list 1 voice
 target carrier-id 4321
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
show call filter match-list	Display call filter match lists.
source carrier-id	Configure debug filtering for the source carrier ID.
source trunk-group-label	Configure debug filtering for a source trunk group.
target trunk-group-label	Configure debug filtering for a target trunk group.

target trunk-group-label

To configure debug filtering for a target trunk group, use the **target trunk-group-label** command in call filter match list configuration mode. To disable, use the **no** form of this command.

target trunk-group-label *group-number*
no target trunk-group-label *group-number*

Syntax Description

group-number	A value from 0 to 23 that identifies the trunk group.

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the voice call debug filter set to match target trunk group 21:

```
call filter match-list 1 voice
 target trunk-group-label 21
```

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
show call filter match-list	Display call filter match lists.
source carrier-id	Configure debug filtering for the source carrier ID.
source trunk-group-label	Configure debug filtering for a source trunk group.
target carrier-id	Configure debug filtering for the target carrier ID.

tbct clear call

To terminate billing statistics for one or more active Two B-Channel Transfer (TBCT) calls, use the **tbct clear call** command in privileged EXEC mode.

tbct clear call {**all** | *interface* [*call-tag*]}

Syntax Description

all	Active TBCT calls on all interfaces.
interface	Active TBCT calls on a specified interface. Range is platform-dependent.
call -tag	(Optional) A specific active TBCT call on the specified interface, as identified by the unique call tag number. Range is 1 to 4,294,967,295.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

- Use this command to manually clear a specific active call or a group of active calls, if, for instance, the ISDN switch goes down. You should not have to manually clear calls with this command unless there is a problem with the switch.
- This command terminates billing information that is being sent to the RADIUS server if, for some reason, the gateway did not receive a notify message from the switch that a call has cleared.
- To automatically clear calls after a specified duration, use the **tbct max call-duration** command.
- To determine the *interface* and *call -tag* arguments to use with this command, use the **show call active voice redirect** command.

Examples

The following example clears calls on T1 interface 6/0:

```
Router# tbct clear call T1-6/0
```

Related Commands

Command	Description
isdn supp -service tbct	Enables ISDN TBCT on PRI trunks.
show call active voice redirect	Displays information about active calls that are being redirected using RTPvt or TBCT.
tbct max call -duration	Sets the maximum duration allowed for a call that is redirected using TBCT.

Command	Description
tbct max calls	Sets the maximum number of active calls that can use TBCT.

tbct max call-duration

To set the maximum duration allowed for a call that is redirected using Two B-Channel Transfer (TBCT), use the **tbct max call-duration**command in global configuration mode. To reset to the default, use the **no** form of this command.

tbct max call-duration *minutes*
no tbct max call-duration

Syntax Description

minutes	Maximum duration, in minutes, allowed for a single TBCT call. Range is 1 to 9999, in recommended increments of 5 minutes. Default is no limit.

Command Default

No limit

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

- Use this command to automatically clear stale calls, for instance if the PRI trunk goes down. To manually clear calls, use the **tbct clear call** command.
- Cisco recommends that you set the call duration in increments of 5 minutes.

Note The call duration limit set by this command is not precisely enforced; calls may not be cleared after the exact number of minutes specified by this command.

Examples

The following example clears TBCT calls that last longer than 10 minutes:

```
tbct max call-duration 10
```

Related Commands

Command	Description
isdn supp -service tbct	Enables ISDN TBCT on PRI trunks.
show call active voice redirect	Displays information about active calls that are being redirected using RTPvt or TBCT.
tbct clear call	Terminates billing statistics for one or more active TBCT calls.
tbct max calls	Sets the maximum number of active calls that can use TBCT.

tbct max calls

To set the maximum number of active calls that can use Two B-Channel Transfer (TBCT), use the **tbct max calls** command in global configuration mode. To reset to the default, use the **no** form of this command.

tbct max calls *number*
no tbct max calls

Syntax Description

number	Maximum number of currently active calls that can invoke TBCT at any one time. Range is 1 to 1,000,00. Default is no limit.

Command Default

No limit, except as allowed by memory resources

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use this command to control memory resources on the gateway by limiting the amount of memory consumed by TBCT calls.

Examples

The following example sets the maximum number of calls using TBCT to 500:

```
tbct max calls 500
```

Related Commands

Command	Description
isdn supp -service tbct	Enables ISDN TBCT on PRI trunks.
show call active voice redirect	Displays information about active calls that are being redirected using RTPvt or TBCT.
tbct clear call	Terminates billing statistics for one or more active TBCT calls.
tbct max call -duration	Sets the maximum duration allowed for a call that is redirected using TBCT.

tcp-retry

To configure the maximum number of retry attempts for sending messages from the SIP-TCP connection, use the **tcp-retry** command in SIP user-agent configuration mode. To reset to the default value, use the **no** form of this command.

tcp-retry {*count* **close-connection** | **nolimit**}
no tcp-retry

Syntax Description

count	Count range is 100-2000. Default retry count is 200.
close-connection	(Optional) Closes the connections after the configured number of retries.
nolimit	Retry value is set to unlimited.

Command Default

TCP retry count is 200.

Command Modes

SIP user-agent configuration (config-sip-ua)

Command History

Release	Modification
15.6(1)T	This command was introduced.

Usage Guidelines

Use this command to configure the maximum number of attempts to be tried while trying to send out messages from the SIP-TCP connection. Once the retry attempts are exhausted, all the pending messages on that TCP connection are deleted. If the **close-connection** keyword is used, the TCP connection is closed.

Examples

The following example sets the maximum number of retry attempts to 500:

```
Router (config-sip-ua)# tcp-retry 500
```

The following example sets the maximum number of retry attempts to 100, and also the configuration to close the connection after all the retry attempts are exhausted:

```
Router (config-sip-ua)# tcp-retry 100 close-connection
```

The following example shows that CUBE is configured to retry unlimitedly until the message goes out or until the connection is closed:

```
Router (config-sip-ua)# tcp-retry nolimit
```

tdm-group

To configure a list of time slots for creating clear channel groups (pass-through) for time-division multiplexing (TDM) cross-connect, use the **tdm-group** command in controller configuration mode. To delete a clear channel group, use the **no** form of this command.

tdm-group *tdm-group-no* **timeslot** *timeslot-list* [**type** {**em** | **fxs** [**loop-start** | **ground-start**] | **fxo** [**loop-start** | **ground-start**] | **fxs-melcas** | **fxo-melcas** | **e&m-melcas**}]
no tdm-group *tdm-group-no* **timeslot** *timeslot-list* [**type** {**em** | **fxs** [**loop-start** | **ground-start**] | **fxo** [**loop-start** | **ground-start**] | **fxs-melcas** | **fxo-melcas** | **e&m-melcas**}]

Syntax Description

tdm -group-no	TDM group number.
timeslot	Time-slot number.
timeslot -list	Time-slot list. T1 range is 1 to 24. E1 range is 1 to 15 and 17 to 31.
type	(Optional) (Valid only when the mode cas command is enabled.) Voice signaling type of the voice port. If configuring a TDM group for data traffic only, do not specify the type keyword. Choose from one of the following options: • e&m--E&M signaling • fxs--Foreign Exchange Station signaling (optionally, you can also specify loop-start or ground-start) • fxo--Foreign Exchange Office signaling (optionally, you can also specify loop-start or ground-start) • fxs-melcas--Foreign Exchange Station MEL CAS • fxo-melcas--Foreign Exchange Office MEL CAS • e&m-melcas--E&M Mercury Exchange Limited Channel-Associated signaling (MEL CAS) The MELCAS options apply only to E1 lines and are used primarily in the United Kingdom.

Command Default

No TDM group is configured.

Command Modes

Controller configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on Cisco MC38310.
12.1(1)T	This command was modified to include voice WAN interface cards (VWICs) for Cisco 2600 series and Cisco 3600 series.

Release	Modification
12.1(2)T	This command was modified for the OC-3/STM-1 ATM Circuit Emulation Service network module on Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

The **tdm-group** command allows specific timeslots to switch from port 0 to port 1 and vice versa. This command is similar to the **channel-group** command, but it does not create a serial interface to terminate the specified channels.



Note Channel groups, CAS voice groups, DS0 groups, and TDM groups all use group numbers. All group numbers configured for channel groups, CAS voice groups, DS0 groups, and TDM groups must be unique on the local router. For example, you cannot use the same group number for a channel group and for a TDM group.

Examples

The following example configures TDM group 1 to include timeslots 13 through 20:

```
controller T1 1
 tdm-group 1 timeslots 13-20
```

The following example configures TDM group number 20 on controller T1 1 to support Foreign Exchange Office (FXO) ground-start:

```
controller T1 1
 tdm-group 20 timeslot 20 type fxs ground-start
```

Related Commands

Command	Description
connect	Starts passage of data between ports for cross-connect TDM.

tech-prefix

To specify that a particular technology prefix be prepended to the destination pattern of a specific dial peer, use the **tech-prefix** command in dial peer configuration mode. To disable the defined technology prefix for this dial peer, use the **no** form of this command.

tech-prefix *number*
no tech-prefix

Syntax Description

number	Defines the numbers used as the technology prefix. Each technology prefix can contain up to 11 characters. Although not strictly necessary, a pound (#) symbol is frequently used as the last character in a technology prefix. Valid characters are 0 though 9, the pound (#) symbol, and the asterisk (*).

Command Default

No technology prefix is defined.

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on Cisco 2600 series and Cisco 3600 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Technology prefixes are used to distinguish between gateways that have specific capabilities within a given zone. In the exchange between the gateway and the gatekeeper, the technology prefix is used to select a gateway after the zone has been selected. Use the **tech-prefix** command to define technology prefixes.

Technology prefixes can be used as a discriminator so that the gateway can tell the gatekeeper that a certain technology is associated with a particular call (for example, 15# could mean a fax transmission), or a technology prefix can be used like an area code for more generic routing. No standard defines what the numbers in a technology prefix mean; by convention, technology prefixes are designated by a pound (#) symbol as the last character.

In most cases, there is a dynamic protocol exchange between the gateway and the gatekeeper that enables the gateway to inform the gatekeeper about technology prefixes and where to forward calls. If, for some reason, that dynamic registry feature is not in effect, you can statically configure the gatekeeper to query the gateway for this information by configuring the **gw-type-prefix** command on the gatekeeper. Use the **show gatekeeper gw-type-prefix** commandto display how the gatekeeper has mapped the technology prefixes to local gateways.



Note Cisco gatekeepers use the asterisk (*) as a reserved character. If you are using Cisco gatekeepers, do not use the asterisk as part of the technology prefix.

Examples

The following example defines a technology prefix of 14# for the specified dial peer. In this example, the technology prefix means that the H.323 gateway asks the RAS gatekeeper to direct calls using the technology prefix of 14#.

```
dial-peer voice 10 voip
 destination-pattern 14...
 tech-prefix 14#
```

Related Commands

Command	Description
gw -type-prefix	Configures a technology prefix in the gatekeeper.
show gatekeeper gw -type-prefix	Displays the gateway technology prefix table.

tel-config to-hdr

To configure the To: Header (to hdr) Request URI to telephone (TEL) format for VoIP Session Initiation Protocol (SIP) calls, use the **tel-config to-hdr** command in SIP configuration mode or voice class tenant configuration mode. To reset to the default, use the **no** form of this command.

tel-config to-hdr [**phone-context**] **[system]**
no tel-config to-hdr

Syntax Description

phone-context	(Optional) Appends the phone context parameter to the TEL URL.
system	(Optional) Specifies that the To: Header (to hdr) Request URI to telephone (TEL) format use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

The To: Header Request Line URIs are not configured to telephone format.

Command Modes

SIP configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.

Usage Guidelines

The **voice-class tel-config to-hdr**command takes precedence over the **tel-config to-hdr** command configured in SIP configuration mode. However, if the **voice-class tel-config to-hdr** command is configured with the **system** keyword, the gateway uses the global settings configured by the **tel-config to-hdr** command.

Enter SIP configuration mode after entering voice-service VoIP configuration mode, as shown in the "Examples" section.

Examples

The following example configures the To: header in TEL format, and appends the phone-context parameter to the header:

```
voice service voip
sip
 tel-config to-hdr phone-context
```

The following example configures the To: header in TEL format in the voice class tenant configuration mode:

```
Router(config-class)# tel-config to-hdr system
```

Related Commands

Command	Description
sip	Enters SIP configuration mode from voice-service VoIP configuration mode.
voice -class tel-config to-hdr	Configures the To: Header request URI to telephone format for dial-peer VoIP SIP calls.

telephony-service

To enter telephony-service configuration mode for configuring Cisco Unified CME, use the **telephony-service** command in global configuration mode. To remove the entire Cisco Unified CME configuration for SCCP IP phones, use the **no** form of this command.

telephony-service [**setup**]
no telephony-service

Syntax Description

setup	(Optional) Interactive setup tool for configuring Cisco Unified IP Phone 7910s, 7940s, and 7960s in Cisco Unified CME. **Note** This interactive Cisco CME setup tool is restricted to generating basic configuration files for Cisco Unified IP Phone 7910s, 7940s, and 7960s running SCCP protocol only.

Command Default

No Cisco Unified CME configuration for SCCP IP phones is present.

Command Modes

Global configuration (config)

Command History

Cisco IOS Release	Cisco Product	Modification
12.1(5)YD	Cisco ITS 1.0	This command was introduced.
12.2(8)T	Cisco ITS 2.0	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(15)ZJ	Cisco CME 3.0	The **setup** keyword was added.
12.3(4)T	Cisco CME 3.0	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

This command enters the telephony-service configuration mode for configuring system wide parameters for SCCP IP phones in Cisco Unified CME.



Note The voice-gateway system is tied to the telephony service. The **telephony-service** command must be configured before the voice-gateway system is configured; otherwise, the voice gateway is hidden from the user.

Use the **setup** keyword to start the interactive setup tool to automatically configure only Cisco Unified IP Phone 7910s, 7940s, and 7960s in Cisco Unified CME.

For alternate methods of automatically configuring Cisco Unified CME, including Cisco Unified IP Phone 7910s, 7940s, and 7960s and other Cisco Unified IP phones, see the Cisco Unified CME Administrator Guide.

The **setup** keyword is not stored in the router nonvolatile random-access memory (NVRAM).

If you attempt to use the **setup** option for a system that already has a telephony-service configuration, the command is rejected. To use the **setup** option after an existing telephony-service configuration has been created, first remove the existing configuration using the **no telephony-service** command.

The table below shows a sample dialog with the Cisco CME setup tool and explains possible responses to the Cisco CME setup tool prompts.

Table 1: Cisco CME Setup Tool Dialog Prompts

Cisco CME Setup Tool Prompt	Description

`Do you want to setup DHCP service for your IP phones? [yes/no]:`
 	
If you respond yes, you see the following prompts:
 	
`IP network for telephony-service DHCP Pool:`
`Subnet mask for DHCP network :`
`TFTP Server IP address (Option 150) :`
`Default Router for DHCP Pool :`
	• Yes--Configures the Cisco Unified CME router to act as a Dynamic Host Configuration Protocol (DHCP) server, automatically providing IP addresses to your IP phones and provisioning the default gateway and TFTP IP addresses to be used by the phones. This method creates a single pool of IP addresses. If you need a pool for non-IP phones or if the Cisco router cannot act as the DHCP router, answer no and manually define the DHCP server.
	• No--Indicates that you have already configured DHCP or static IP addresses for the IP phones.

`Do you want to start telephony-service setup? [yes/no]:`	• **Yes**-- Starts the interactive setup tool for configuring Cisco Unified IP Phone 7910s, 7940s, and 7960s. • **No** --Terminates the Cisco CME setup tool.
`Enter the IP source address for Cisco CallManager Express:` `Enter the Skinny Port for Cisco CallManager Express: [2000]:`	IP address on which the router provides Cisco Unified CME services, usually the default gateway for the IP subnet that you are using for the IP phones, and the port for Skinny Client Control Protocol (SCCP) messages.
`How many IP phones do you want to configure : [0]:`	Enter the maximum number of IP phones that this Cisco Unified CME system will support. This number can be increased later, to the maximum allowed for this version and your router. **Note** The Cisco CME setup tool associates one number with each newly registering phone. You can manually add additional numbers on a phone at a later time.
`Do you want dual-line extensions assigned to phones? [yes for dual-line / no for single-line]:`	• **Yes** --Each newly registering IP phones is assigned a single number that is associated with a single phone button. The system generates a dual-line ephone-dn entry for each ephone-dn. • **No** --IP phones are linked directly to one or more PSTN trunk lines. Using keyswitch mode requires manual configuration in addition to using the Cisco CME setup tool. The system generates two ephone-dn entries for each ephone-dn, and they are both assigned to a single phone.

Cisco CME Setup Tool Prompt	Description

`What language do you want on IP phones?`
`0 English`
`1 French`
`2 German`
`3 Russian`
`4 Spanish`
`5 Italian`
`6 Dutch`
`7 Norwegian`
`8 Portuguese`
`9 Danish`
`10 Swedish`
`[0]:`
	Language for IP phone displays, selected from the list.
	• Default is 0, English.

`Which Call Progress tone set do you want on IP phones :`
`0 United States`
`1 France`
`2 Germany`
`3 Russia`
`4 Spain`
`5 Italy`
`6 Netherlands`
`7 Norway`
`8 Portugal`
`9 UK`
`10 Denmark`
`11 Switzerland`
`12 Sweden`
`13 Austria`
`14 Canada`
`[0]:`
	Locale for the tone set used to indicate call status or progress, selected from the list.
	• Default is 0, United States.

`What is the first extension number you want to configure :[0]:`	First number in pool of extension numbers to be created for IP phones connected to the Cisco router to be configured. • Starting with this number, remaining extension numbers are automatically configured in a contiguous manner. • This number must be compatible with your telephone number plan, and, if you use Direct Inward Dialing (DID) service, with public switched telephone network (PSTN) numbering requirements.
`Do you have Direct-Inward-Dial service for all your phones? [yes/no]:`	• Yes--If you have trunk access to public telephone service by ISDN or VoIP for all extension numbers. The system creates an appropriate dial plan. • No--If you have simple analog phone lines only (for example, foreign exchange office [FXO] interfaces) or if you have trunk access for some lines but not all lines.

Cisco CME Setup Tool Prompt	Description
If you answer yes to the previous question, you see the following prompt: `Enter the full E.164 number for the first phone:`	Complete 10-digit telephone number, including area code, that corresponds to the first extension number.
`Do you want to forward calls to a voice message service? [yes/no]:`	• Yes--To forward calls to a single voice message service number when an IP phone is busy or does not answer. All phone extensions forward their calls to the same voice message service pilot number. • No--Not to forward calls to a single voice message service number. Answer no if you do not have a voice message system or if you want to customize call-forwarding behavior for each extension.
If you answer yes to the previous question, you see the following prompt: `Enter the extension or pilot number of the voice message service:`	Voice message service pilot number. • This step can be ignored during the setup dialog and manually configured later.
`Call forward No Answer Timeout: [18]:`	Timeout, in seconds, after which to forward calls to voice mail if they are not answered. • Default is 18.
`Do you wish to change any of the above information? [yes/no]:`	• **Yes** --Starts the dialog over again without implementing any of the answers that you previously gave. • **No** --Uses specified values to automatically build basic configuration for Cisco Unified IP Phone 7910s, 7940s, and 7960s in Cisco Unified CME.

Examples

The following example shows how to enter telephony-service configuration mode for manually configuring Cisco Unified CME. This example also configures the maximum number of phones to 12:

```
Router(config)# telephony-service
Router(config-telephony)# max-ephones 12
```

The following example shows how to start the Cisco CME setup tool:

```
Router(config)# telephony-service setup
```

telephony-service ccm-compatible (H.323 voice-class)

To enable, for an individual dial peer, the detection of a Cisco CallManager system in the network and allow the exchange of calls, use the **telephony-service ccm-compatible** command in voice-class configuration mode. To disable the detection capability and the exchange of calls on an individual dial peer, use the **no** form of this command.

telephony-service ccm-compatible
no telephony-service ccm-compatible

Syntax Description

This command has no arguments or keywords.

Command Default

Detection of Cisco CallManager systems is enabled.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command is used with Cisco CallManager Express (Cisco CME) 3.1 or a later version.

When a voice class that contains this command is applied to a dial peer, this command enables detection of and call exchange with Cisco CallManager for all calls from that dial peer. Use the **telephony-service ccm-compatible**command in H.323 voice-service configuration mode to create a voice class to apply this capability globally. If the capability is specified at both the global and dial-peer level, the dial-peer setting has precedence for that dial peer.

Examples

The following example globally enables detection of Cisco CallManager systems in the network, creates voice class 4 to disable the capability on individual dial peers, and applies voice class 4 to dial peer 36. Although the **telephony-service ccm-compatible** command in H.323 voice-service configuration mode is not required because this condition is the default, the command is shown here for illustration purposes.

```
Router(config)# voice service voip
Router(config-voi-serv)# h323
Router(conf-serv-h323)# telephony-service ccm-compatible
Router(conf-serv-h323)# exit
Router(config-voi-serv)# exit
Router(config)# voice class h323 4
Router(config-class)# no
 telephony-service ccm-compatible
Router(config-class)# exit
Router(config)# dial-peer voice 36 voip
Router(config-dial-peer)# destination-pattern 555....
Router(config-dial-peer)# session target ipv4:10.5.6.7

Router(config-dial-peer)# voice-class h323 4
```

Related Commands

Command	Description
telephony-service ccm-compatible (H.323 voice-service)	Globally enables detection of Cisco CallManager in a network for all dial peers.
voice class h323	Creates an H.323 voice class to apply to a dial peer.
voice-class h323	Applies an H.323 voice class to a dial peer.

telephony-service ccm-compatible (H.323 voice-service)

To globally enable the detection of a Cisco CallManager system in the network and allow the exchange of calls, use the **telephony-service ccm-compatible** command in H.323 voice-service configuration mode. To disable the detection capability and the exchange of calls globally, use the **no** form of this command.

telephony-service ccm-compatible
no telephony-service ccm-compatible

Syntax Description

This command has no arguments or keywords.

Command Default

Detection of Cisco CallManager systems is enabled.

Command Modes

H.323 voice-service configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command is used with Cisco CallManager Express (Cisco CME) 3.1 or a later version.

This command globally enables call exchange with Cisco CallManager for all calls from this router. Use the **telephony-service ccm-compatible**command in voice-class configuration mode to create a voice class in order to apply this capability to an individual dial peer. If the capability is specified at both the global and dial-peer level, the dial-peer setting has precedence for that dial peer.

Examples

The following example globally enables detection of Cisco CallManager systems in the network, creates voice class 4 to disable the capability on individual dial peers, and applies voice class 4 to dial peer 36. Although the **telephony-service ccm-compatible** command in H.323 voice-service configuration mode is not required because this condition is the default, the command is shown here for illustration purposes.

```
Router(config)# voice service voip
Router(config-voi-serv)# h323
Router(conf-serv-h323)# telephony-service ccm-compatible
Router(conf-serv-h323)# exit
Router(config-voi-serv)# exit
Router(config)# voice class h323 4
Router(config-class)# no
 telephony-service ccm-compatible
Router(config-class)# exit
Router(config)# dial-peer voice 36 voip
Router(config-dial-peer)# destination-pattern 555....
Router(config-dial-peer)# session target ipv4:10.5.6.7

Router(config-dial-peer)# voice-class h323 4
```

Related Commands

Command	Description
h323	Enters H.323 voice-service configuration mode.
telephony-service ccm-compatible (H.323 voice-class)	Enables Cisco CallManager detection in a network by individual dial peers.
voice service voip	Enters voice-service configuration mode.

test dsmp delete-stream

To clear one or more inactive Distributed Stream Media Processor (DSMP) media stream sessions that are hung and is not cleared, use the **test dsmpdelete-stream** command in the privileged EXEC mode.

test dsmpdelete-stream *stream-id*

Syntax Description

stream-id	The specific stream-id that is hung and should be deleted.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.4(3)M	This command was introduced.

Examples

The following example shows the voice :

```
Router #test dsmp delete-stream 7973
test_dsmp: id is 7973
% Stream 7973 does not exist
```

test voice mos-calc

To test the MOS computation algorithm voice quality metrics related to media (voice) quality, such as conversational mean opinion score (MOS), packet loss rate, and so on, use the **test voice mos-calc** command in the privileged EXEC mode.

test voice mos-calc *Packet Loss RTT Jitter*

Syntax Description

Packet Loss	Enter the packet loss, in percentage. Range is from 0 to 100.
RTT	Enter the round trip time, in ms (range 0 - 5000).
Jitter	Enter the jitter value caused by switches in the WAN, in ms (range 0 - 2000).

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Examples

The following example shows the voice :

```
Router#test voice mos-calc ?
  <0-100>  Packet Loss in percentage

Router#test voice mos-calc 5 ?
  <0-5000>  RTT in milliseconds

Router#test voice mos-calc 5 16 ?
  <0-2000>  Jitter in milliseconds

Router#test voice mos-calc 5 16 6 ?
  Mean Opinion Score= 3.7841
  <cr>
```

text relay modulation

To configure the teletype text phone (TTY) modulation used on the gateway for Cisco text relay for Baudot text phones, use the **text relay modulation**command in dial peer voice configuration mode or voice service configuration mode. To disable text relay modulation, use the **no** form of this command.

text relay modulation {**baudot45.45** | **baudot50**} {**autobaud-on** | **autobaud-off**}
no text relay modulation

Syntax Description

baudot45.45	Configures baudot 45.45 TTY modulation. This is the default baud rate.
baudot50	Configures baudot 50 TTY modulation.
autobaud-on	Enables the digital signal processors (DSPs) to autodetect the baud rate. This is the default autobaud setting.
autobaud-off	Disables the DSP capability to autodetect the baud rate.

Command Default

The TTY modulation is **baudot45.45 autobaud-on**.

Command Modes

Dial peer voice configuration
Voice service configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You must select a baud rate and enable or disable the autobaud functionality on the DSP.

Use this command in voice service configuration mode to set the TTY modulation globally. A global configuration is the system-wide configuration that is applied to any VoIP call on the gateway.

Use this command in dial peer voice configuration mode to set the TTY modulation for calls that match a specific dial peer. The dial peer voice configuration takes precedence over the global configuration.

Examples

The following example shows how to globally set the text relay TTY modulation to Baudot 50:

```
Router(config)# voice service voip
Router(config-voi-serv)# text relay modulation baudot50 autobaud-off
```

The following example shows how to set the text relay TTY modulation to Baudot 50 for calls that match a specific dial peer:

```
Router(config)# dial-peer voice 2000 voip
Router(config-dial-peer)# text relay modulation baudot50 autobaud-off
```

Related Commands

Command	Description
text relay protocol	Configures the system-wide protocol type for text packets transmitted between gateways.
text relay rtp	Configures the RTP payload type and redundancy level.

text relay protocol

To enable Cisco text relay for Baudot text phones, use the **text relay protocol**command in dial peer voice configuration mode or voice service configuration mode. To disable text relay capabilities, use the **no** form of this command.

text relay protocol [**cisco** | **system**]
no text relay protocol

Syntax Description

cisco	(Optional) Uses the Cisco proprietary text relay protocol.
system	(Optional; dial peer voice configuration only) Uses the global configuration settings.

Command Default

The text relay protocol is disabled.

Command Modes

Dial-peer configuration
Voice-service configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Use this command in voice-service configuration mode to enable text relay globally for H.323, Session Initiation Protocol (SIP), Skinny Client Control Protocol (SCCP), and Media Gateway Control Protocol (MGCP). A global configuration is the system-wide configuration that is applied to any VoIP call on the gateway.

Use this command in dial peer voice configuration mode to enable text relay for calls that match a specific dial peer. The dial peer voice configuration takes precedence over the global configuration.

Examples

The following example shows how to enable text relay for all VoIP calls on the gateway:

```
Router(config)# voice service voip
Router(config-voi-serv)# text relay protocol cisco
```

The following example shows how to enable text relay for calls that match a specific dial peer:

```
Router(config)# dial-peer voice 2000 voip
Router(config-dial-peer)# text relay protocol cisco
```

Related Commands

Command	Description
text relay modulation	Configures the TTY modulation on the gateway.
text relay rtp	Configures the RTP payload type and redundancy level.

text relay rtp

To configure the Real-Time Transport Protocol (RTP) payload type and redundancy level for Cisco text relay for Baudot text phones, use the **text relay rtp**command in dial peer voice configuration mode or voice service configuration mode. To disable the text relay RTP payload type and redundancy level, use the **no** form of this command.

text relay rtp {[**payload-type** {*value* | **default**}] [**redundancy** *level*] | **redundancy** *level*}
no text relay rtp

Syntax Description

payload-type { *value* | **default** }	The RTP payload is the data transported by RTP in a packet. • The *value*range is 98 to 117 for dynamic RTP payload types. • The **default** value is 119, which is a static payload type.
redundancy *level*	Use the redundancy option to repeat data for redundancy and to lower the risk of packet loss. The redundancy level is the number of redundant text packets sent across the VoIP network. The range is 1 to 3. The default value is 2.

Command Default

Text relay RTP is disabled.

Command Modes

Dial peer voice configuration
Voice service configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When using the **text relay rtp** command, you can either configure the **payload-type**, or the redundancy level, or both.

- Use this command in voice service configuration mode to set the RTP payload type and redundancy level globally for H.323, Session Initiation Protocol (SIP), Skinny Client Control Protocol (SCCP), and Media Gateway Control Protocol (MGCP). A global configuration is the system-wide configuration that is applied to any VoIP call on the gateway.
- Use this command in dial-peer configuration mode to set the RTP payload type and redundancy level for calls that match a specific dial peer. The dial peer voice configuration takes precedence over the global configuration.

Examples

The following example shows how to globally configure text relay RTP payload type 117 and redundancy level 2:

```
Router(config)# voice service voip
Router(config-voi-serv)# text relay rtp payload-type 117 redundancy 2
```

The following example shows how to configure the default text relay RTP payload type and redundancy level 1 for calls that match a specific dial peer:

```
Router(config)# dial-peer voice 2000 voip
Router(config-dial-peer)# text relay rtp payload-type default redundancy 1
```

Related Commands

Command	Description
text relay modulation	Configures the TTY modulation on the gateway.
text relay protocol	Configures the system-wide protocol type for text packets transmitted between gateways.

tftp-server address

To specify the address of the TFTP servers in a Cisco Unified Communications Manager (CUCM) cluster use the **tftp-server address** command in phone proxy configuration mode. To remove the address of the TFTP server from the phone proxy configuration, use the **no** form of the command.

tftp-server address [**ipv4** *server-ip-address* | *domain-name*] **local-addr ipv4** *local-ip-address* **acc-addr ipv4** *access-ip-address*
no tftp-server address [**ipv4** *server-ip-address* | *domain-name*] **local-addr ipv4** *local-ip-address* [**acc-addr ipv4** *access-ip-address*]

Syntax Description

domain-name	Domain name of the TFTP server.
local-addr ipv4 *local-ip-address*	Specifies the local interface IPv4 address to connect to the core side server.
acc-addr ipv4 *access-ip-address*	Specifies the access side local interface IPv4 address.

Command Default

No TFTP server addresses are specified.

Command Modes

Phone proxy configuration mode (config-phone-proxy)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Example

The following example shows how to command to specify the TFTP server addresses for the phone proxy configuration:

```
Device(config)# voice-phone-proxy first-pp
Device(config-phone-proxy)# tftp-server address ipv4 198.51.100.101 local-addr ipv4
192.168.0.109 acc-addr 198.51.100.1
```

tgrep address-family

To set the address family to be used on a local dial peer, use the tgrep address-family command in dial peer configuration mode. To return to the global setting, use the **no** form of this command.

tgrep address family {**e164** | **decimal** | **penta-decimal**}
no tgrep address family {**e164** | **decimal** | **penta-decimal**}

Syntax Description

e164	E.164 address family.
decimal	Decimal address family
penta-decimal	Penta-decimal address family

Command Default

No default behavior or values.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The E. 164 address family is used if the telephony network is a public telephony network. Decimal and pentadecimal options can be used to advertise private dial plans. For example if a company wants to use TRIP in within their enterprise telephony network using 5-digit extensions, then the gateway would advertise the beginning digits of their private numbers as a decimal address family. These calls cannot be sent out of the company's private telephony network because they are not E.164-compliant.

The pentadecimal family allows numbers 0 through 9 and alphabetic characters A through E and can be used in countries where letters are also carried in the called number.

Examples

The following example shows that POTS dial peer 10 has the address family set for E.164 addresses:

```
Router(config)# dial-peer voice pots 10
Router(config-dial-peer)# tgrep address family e164
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice-related encapsulation.

tgrep advertise (dial peer)

To set the attributes for advertisement of the prefix on this dial peer or to disable advertisement on this dial peer altogether, use the tgrep advertise command in dial peer configuration mode. To return to using the global setting, use the **no** form of this command.

tgrep advertise [**csr**] [**ac**] [**tc**] [**carrier** | **trunk-group**] [**disable**]
no tgrep advertise [**csr**] [**ac**] [**tc**] [**carrier** | **trunk-group**] [**disable**]

Syntax Description

csr	Call success rate.
ac	Available circuits.
tc	Total circuits.
carrier	Carrier-code address family.
trunk-group	Trunk-group address family.
disable	Disables advertisement of this dial peer.

Command Default

Prefix advertisement is not sent.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

When only tgrep advertise is entered, the dial peer is advertised without any other attribute.

When no tgrep advertise is used on the dial peer, the dial peer inherits the attributes set in the global advertise command.

When the global no advertise command is used, it forbids advertisement of that particular address family altogether. The **tgrep advertise** command has no effect until the advertisement of the address family is enabled globally.

Examples

The following example shows a TGREP advertisement that sends call success rate, available circuits, total circuits, and carrier address family attribute information:

```
Router(config)# dial-peer voice pots 10
Router(config-dial-peer)# tgrep advertise csr ac tc carrier
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice-related encapsulation.

tgrep advertise (trunk group)

To turn on the advertisement of this trunk group for resource availability and other carrier information, use the tgrep advertise command in trunk group configuration mode. To turn off local trunk group advertisement and use the global setting, use the **no** form of this command.

tgrep advertise [**csr**] [**ac**] [**tc**] [**disable**]
no tgrep advertise [**csr**] [**ac**] [**tc**] [**disable**]

Syntax Description

csr	Call success rate.
ac	Available circuits.
tc	Total circuits.
disable	Disables advertisement on the trunk group.

Command Default

Trunk group advertisement is not sent

Command Modes

Trunk group configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

When only tgrep advertise is entered, the trunk group is advertised without any other attribute. When no tgrep advertise is used, the trunk group uses the global setting configured with the advertise command in TGREP configuration mode. To turn off advertisement of this trunk group, the disable keyword should be used.

There is a subtle difference between the no form of this command and the no form of the global advertise command. When no tgrep advertise is used on the trunk group, the trunk group inherits the attributes set in the global advertise command.

When the global no advertise command is used, it forbids advertisement of that particular address family altogether. The **tgrep advertise** command has no effect until the advertisement of the address family is enabled globally.

When the **carrier** keyword is used, the carrier defined under the trunk group assumes the configuration. Because multiple trunk groups can have the same carrier defined, the same configuration will show up under all trunk groups that have the same carrier defined. When the **no tgrep advertise carrier** command is used to revert to the global carrier configuration for the carrier under this trunk group, the same will happen to all the trunk groups who have the same carrier defined under them.



Note This command overrides the attributes set for advertisement using the global advertise (tgrep) command.

Examples

The following example shows that trunk group 101 has been configured to send a TGREP advertisement that sends call success rate, available circuits, total circuits, and prefix attribute information:

```
Router(config)# trunk group 101
Router(config-dial-peer)# tgrep advertise csr ac tc carrier
```

Related Commands

Command	Description
advertise (tgrep)	Turns on reporting for a specified address family.
trunk group	Defines the trunk group and enters trunk group configuration mode.

tgrep local-itad

To enable Telephony Gateway Registration Protocol (TGREP) on the gateway and enter TGREP configuration mode, use the **tgrep local-itad** command in global configuration mode. To disable the configuration on the gateway, use the **no** form of this command.

tgrep local-itad [*itad-number*]
no tgrep local-itad [*itad-number*]

Syntax Description

itad-number	(Optional) IP Telephony Administrative Domain (ITAD) number associated with the gateway. The range is from 1 to 4294967295.

Command Default

TGREP is disabled on the gateway.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples

The following example shows how to enable TGREP for ITAD number 1234:

```
Router# enable
Router(config)# tgrep local-itad 1234
```

Related Commands

Command	Description
address-family	Sets the global address family to be used on all dial peers.
advertise (tgrep)	Turns on reporting for a specified address family.
neighbor	Creates a TGREP session with another device.

threshold noise

To configure a noise threshold for incoming calls, use the **threshold noise**command in voice-port configuration mode. To restore the default, use the no form of this command.

threshold noise *value*
no threshold noise *value*

Syntax Description

value	Number that establishes a noise threshold. Valid values are from -30 to -90 decibels (dBs). The default is -62 dB.

Command Default

-62 dB

Command Modes

Voice-port configuration

Command History

Release	Modification
12.2(13b)	This command was introduced on the following platforms: Cisco 1700 Cisco 1751, Cisco 2600 (with and without the NM-HDA), Cisco 3600 (with and without the NM-HDA), Cisco 7200 (with and without the NM-HDA), Cisco AS5300, Cisco AS5800, and Cisco MC3810.
12.2(16)	This command was integrated into Cisco IOS Release 12.2(16).

Usage Guidelines

Cisco voice activity detection (VAD) has two layers: application programming interface (API) layer and processing layer. There are 3 states that the processing layer classifies incoming signals: speech, unknown, and silence. The state of the incoming signals is determined by the noise threshold.

In earlier Cisco IOS releases, the noise threshold is fixed between -62 dB and -78 dB. If the voice level is below the noise threshold, then the signal is classified as silence. If the incoming signal cannot be classified, the variable thresholds that are computed with the statistics of speech and noise that VAD gathers is used to make a determination. If the signal still cannot be classified, then it is marked as unknown. The final decision is made by the API. For applications such as hoot-n-holler, you could have the noise create unwanted spurious packets (for example, a voice stream) taking up bandwidth.

With Cisco IOS Release 12.2(16), the noise threshold is configurable using the threshold noise command.

Examples

The following sample configuration shows a noise threshold level of -50 dB:

```
voice-port 1/0/0
 threshold noise -50
```

timeout (auto-config application)

To configure the download timeout value for an auto-configuration application, use the **timeout** command in auto-config application configuration mode. To reset to the default, use the **no** form of this command.

timeout *time-in-seconds*
no timeout

Syntax Description

time -in-seconds	Specifies the download timeout value in seconds. The range is from 0 to 3600. The default is 180.

Command Default

The default value is 180 seconds.

Command Modes

Auto-config application configuration

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines

A value of 0 specifies continuous download retry.

Examples

The following example shows the **timeout** command used to specify continuous retry for downloading an auto-configuration application:

```
Router(auto-config-app)# timeout 0
```

Related Commands

Command	Description
auto -config	Enables auto-configuration or enters auto-config application configuration mode for the SCCPapplication.
show auto -config	Displays the current status of auto-configuration applications.

timeout leg3

To set the timeout value for a leg 3 AAA preauthentication request, use the **timeout leg3** command in AAA preauthentication configuration mode. To return the timeout value to its default, use the **no** form of this command.

timeout leg3 *milliseconds*
no timeout leg3 *milliseconds*

Syntax Description

milliseconds	Timeout value for leg 3 preauthentication, in milliseconds. Range is from 100 to 1000. The default is 100.

Command Default

100 milliseconds.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

If the timeout timer expires before AAA has responded to a preauthentication request, the call is rejected.

The term leg 3 refers to a call segment from the IP network to a terminating (outgoing) gateway that takes traffic from an IP network to a PSTN network.

Examples

The following example sets the timeout for a leg 3 AAA preauthentication request to 250 milliseconds:

```
Router(config)# aaa preauth
Router(config-preauth)# timeout leg3 250
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication configuration mode.

timeout ptt

To specify a maximum time for transmitting or receiving a voice packet, use the **timeout ptt** command in voice-port configuration mode. To return to the default, use the **no** form of this command.

timeout ptt {**rcv** | **xmt**} *minutes*
no timeout ptt {**rcv** | **xmt**} *minutes*

Syntax Description

rcv	Applies the specified time limit to the reception of voice packets.
xmt	Applies the specified time limit to the transmission of voice packets.
minutes	Maximum time, in minutes, allowed for transmitting or receiving a voice packet. Range is integers from 1 to 30.

Command Default

minutes : 0 minutes

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

The **timeout ptt** command is available on an ear and mouth (E&M) analog or digital voice port only if the signal type for that port is Land Mobile Radio (LMR). The purpose of this command is to limit extended radio transmission. When the time limit configured with this command expires, the radio transmitter unkeys, so that listeners on the channel cannot hear the speaker, even if the speaker continues to talk. When the speaker unkeys the radio, the timer is reactivated.

Examples

The following example specifies a maximum time of 10 minutes for transmitting a voice packet:

```
voice-port 1/0/0
 timeout ptt xmt 10
```

timeout tcrit

To configure the critical timeout value, T(critical), for the interdigit timer used in digit map matching, use the **timeout tcrit** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tcrit *tcrit-value*
no timeout tcrit

Syntax Description

tcrit -value	Critical timeout value, T(critical), in seconds. Range is from 1 to 600. Default is 4.

Command Default

4 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The interdigit timer is used when matching a digit map, which is a representation of the number and type of digits that a gateway can expect to collect in a buffer, based on the network dial plan. The interdigit timer is started when the first digit is entered and is restarted after each new digit is entered, until a digit map match or mismatch occurs.

The interdigit timer takes on one of two values, T(partial) or T(critical). When at least one more digit is required to make a match to any of the patterns in the digit map, the value of T(partial) is used for the timer. If a timer is all that is required to produce a match according to the digit map, T(critical) is used for the timer.

When the interdigit timer is used without a digit map, it takes on the value T(critical). It is started immediately and is simply canceled (but not restarted) as soon as a digit is entered.

Examples

The following example sets the T(critical) value to 15 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tcrit 15
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

Command	Description
timeout tpar	Configures the MGCP partial timeout value, T(partial), for the interdigit timer used in digit map matching.

timeout tdinit

To configure the initial waiting delay value (Tdinit) for the disconnected procedure, use the **timeout tdinit** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tdinit *tdinit-value*
no timeout tdinit

Syntax Description

tdinit -value	Initial waiting delay (Tdinit) for the disconnected procedure, in seconds. The disconnected timer is initialized to a randomly selected value between 0 and Tdinit. Range is from 1 to 30. Default is 15.

Command Default

15 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

When a gateway recognizes that an endpoint has lost its communication with the call agent (has become *disconnected)* , a timer known as the disconnected timer is initialized to a random value between 0 and the disconnected initial waiting delay (Tdinit), which is configured with the **timeout tdinit** command. The gateway then waits for one of three things: the end of this timer, the reception of a command from the call agent, or the detection of local user activity for the endpoint, such as an off-hook transition. When one of the first two cases occurs, the gateway initiates the *disconnected procedure* for that endpoint. In the third case, the detection of local user activity, a minimum waiting delay (Tdmin) also must have elapsed. This value is configured with the **timeout tdmin** command.

The disconnected procedure consists of the endpoint sending a RestartInProgress (RSIP) message to the call agent, stating that it was disconnected and is now trying to reestablish connectivity.

If the disconnected procedure is unsuccessful and the endpoint is still disconnected, the disconnected timer is doubled; this process is repeated until the timer value reaches the maximum waiting delay (Tdmax), which is configured with the **timeout tdmax** command.

Examples

The following example sets the initial waiting delay value (Tdinit) to 25 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tdinit 25
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.
timeout tdmax	Configures the maximum timeout for the MGCP disconnected procedure.
timeout tdmin	Configures the minimum timeout for the MGCP disconnected procedure.

timeout tdmax

To configure the maximum timeout value (Tdmax) for the disconnected procedure, use the **timeout tdmax** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tdmax *tdmax-value*
no timeout tdmax

Syntax Description

tdmax -value	Maximum timeout value (Tdmax) for the disconnected procedure, in seconds. Range is from 300 to 600. The default is 600.

Command Default

600 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

When a gateway recognizes that an endpoint has lost its communication with the call agent (has become *disconnected)* , a timer known as the disconnected timer is initialized to a random value between 0 and the disconnected initial waiting delay (Tdinit), which is configured with the **timeout tdinit** command. The gateway then waits for one of three things: the end of this timer, the reception of a command from the call agent, or the detection of local user activity for the endpoint, such as an off-hook transition. When one of the first two cases occurs, the gateway initiates the *disconnected procedure* for that endpoint. In the third case, the detection of local user activity, a minimum waiting delay (Tdmin) also must have elapsed. This value is configured with the **timeout tdmin**command.

The disconnected procedure consists of the endpoint sending a RestartInProgress (RSIP) message to the call agent, stating that it was disconnected and is now trying to reestablish connectivity.

If the disconnected procedure is unsuccessful and the endpoint is still disconnected, the disconnected timer is doubled; this process is repeated until the timer value reaches the maximum waiting delay (Tdmax), which is configured with the **timeout tdmax** command.

Examples

The following example sets the maximum timeout value (Tdmax) to 450 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tdmax 450
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.
timeout tdinit	Configures the initial timeout for the MGCP disconnected procedure.
timeout tdmin	Configures the minimum timeout for the MGCP disconnected procedure.

timeout tdmin

To configure the minimum timeout value (Tdmin) for the disconnected procedure, use the **timeout tdmin** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tdmin *tdmin-value*
no timeout tdmin

Syntax Description

tdmin -value	Minimum timeout (Tdmin) for the disconnected procedure, in seconds. Range is from 1 to 30. The default is 15.

Command Default

15 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

When a gateway recognizes that an endpoint has lost its communication with the call agent (has become *disconnected)* , a timer known as the disconnected timer is initialized to a random value between 0 and the disconnected initial waiting delay (Tdinit), which is configured with the **timeout tdinit**command. The gateway then waits for one of three things: the end of this timer, the reception of a command from the call agent, or the detection of local user activity for the endpoint, such as an off-hook transition. When one of the first two cases occurs, the gateway initiates the *disconnected procedure* for that endpoint. In the third case, the detection of local user activity, a minimum waiting delay (Tdmin) also must have elapsed. This value is configured with the **timeout tdmin**command.

The disconnected procedure consists of the endpoint sending a RestartInProgress (RSIP) message to the call agent, stating that it was disconnected and is now trying to reestablish connectivity.

If the disconnected procedure is unsuccessful and the endpoint is still disconnected, the disconnected timer is doubled; this process is repeated until the timer value reaches the maximum waiting delay (Tdmax), which is configured with the **timeout tdmax**command.

Examples

The following example sets the minimum timeout value (Tdmin) to 20 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tdmin 20
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.
timeout tdinit	Configures the initial timeout for the MGCP disconnected procedure.
timeout tdmax	Configures the maximum timeout for the MGCP disconnected procedure.

timeout thist

To configure the packet storage timeout value (Thist), use the **timeout thist**command inMGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout thist *thist-value*
no timeout thist

Syntax Description

thist -value	Package storage timeout (Thist), in seconds. Range is from 1 to 60. The default is 30.

Command Default

30 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

MGCP messages are carried over User Datagram Protocol (UDP), and are therefore subject to packet loss. When a response to a message is not received promptly, the sender retransmits the message. The gateway keeps in memory a list of the responses it has sent for the number of seconds in the Thist timeout value. The gateway also keeps a list of the messages currently being processed, with their transaction identifiers, to prevent processing or acknowledging the same message more than once.

Examples

The following example sets the packet storage timeout value (Thist) to 15 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout thist 15
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints, or to configure the default profile.

timeout tone busy

To configure the busy-tone timeout value, use the **timeout tone busy**command inMGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone busy *busy-tone-value*
no timeout tone busy

Syntax Description

busy -tone-value	Busy-tone timeout, in seconds. Range is from 1 to 600. The default is 30.

Command Default

30 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the busy-tone timeout value when the call agent does not provide a timeout value associated with the request to generate a busy tone signal.

Examples

The following example sets the busy tone timeout value to 45 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone busy 45
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tone cot1

To configure the continuity1 (cot1) tone timeout value, use the **timeout tone cot1**command inMGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone cot1 *cot1-tone-value*
no timeout tone cot1

Syntax Description

cot1 -tone-value	Continuity1 (cot1) tone timeout, in seconds. Range is from 1 to 600. The default is 3.

Command Default

3 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the continuity1 (cot1) tone timeout value when the call agent does not provide a timeout value associated with the request to generate a cot1 tone signal.

Continuity1 and continuity2 tone signals are used in Integrated Services Digital Networks User Part (ISUP) calls to determine that a call path has been established before connecting a call. The call agent is provisioned to know which test to apply to a given endpoint.

Examples

The following example sets the continuity1 tone timeout value to 25 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone cot1 25
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.
timeout tone cot2	Sets the continuity2 tone timeout value for MGCP.

timeout tone cot2

To configure the continuity2 (cot2) tone timeout value, use the **timeout tone cot2**command inMGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone cot2 *cot2-tone-value*
no timeout tone cot2

Syntax Description

cot2 -tone-value	Continuity2 (cot2) tone timeout, in seconds. Range is from 1 to 600. The default is 3.

Command Default

3 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the continuity2 (cot2) tone timeout value when the call agent does not provide a timeout value associated with the request to generate a cot2 tone signal.

Continuity1 and continuity2 tone signals are used in Integrated Services Digital Networks User Part (ISUP) calls to determine that a call path has been established before connecting a call. The call agent is provisioned to know which test to apply to a given endpoint.

Examples

The following example sets the continuity2 tone timeout value to 50 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone cot2 50
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.
timeout tone cot1	Sets the continuity1 tone timeout value for MGCP.

timeout tone dial

To configure the dial tone timeout value, use the **timeout tone dial**command inMGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone dial *dial-tone-value*
no timeout tone dial

Syntax Description

dial -tone-value	Dial tone timeout value, in seconds. Range is from 1 to 600. The default is 16.

Command Default

16 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the dial tone timeout value when the call agent does not provide a timeout value associated with the request to generate a dial tone signal.

Examples

The following example sets the dial tone timeout value to 25 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone dial 25
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tone dial stutter

To configure the stutter dial tone timeout value, use the **timeout tone dial stutter**command inMGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone dial stutter *stutter-value*
no timeout tone dial stutter

Syntax Description

stutter -value	Timeout value for the stutter dial tone, in seconds. Range is from1 to 600. The default is 16.

Command Default

16 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the stutter dial tone timeout value when the call agent does not provide a timeout value associated with the request to generate a stutter dial tone signal.

Examples

The following example sets the stutter dial tone timeout value to 25 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone dial stutter 25
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tone mwi

To configure the timeout value for the message-waiting indicator tone, use the **timeout tone mwi** command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone mwi *mwi-tone-value*
no timeout tone mwi

Syntax Description

mwi -tone-value	Message-waiting-indicator (MWI) tone timeout value, in seconds. Range is from 1 to 600. The default is 16.

Command Default

16 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the *mwi-tone-value* when the call agent does not provide a timeout value for a request to generate the message-waiting indicator tone signal.

Examples

The following example sets the timeout value for the message-waiting indicator tone to 100 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone mwi 100
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tone network

To configure the network congestion tone timeout value, use the **timeout tone network**command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone network {**congestion** | **busy**} *tone-value*
no timeout tone network

Syntax Description

congestion	Timeout for network congestion.
busy	Timeout for network busy.
tone -value	Tone timeout value, in seconds. Range is from 1 to 600. The default is 180.

Command Default

180 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.
12.4(9)T	The **busy** keyword was introduced.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the tone timeout value when the call agent does not provide a timeout value associated with the request to generate a network congestion or network busy tone signal.

Examples

The following example sets the network congestion tone timeout value to 240 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone network congestion 240
```

The following example shows the network busy timeout value being set to 300 seconds.

Router(config)# **mgcp profile sample**

```
Router(config-mgcp-profile)# timeout tone network busy 300
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.

Command	Description
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tone reorder

To configure the reorder tone timeout value, use the **timeout tone reorder**command inMGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone reorder *reorder-tone-value*
no timeout tone reorder

Syntax Description

reorder -tone-value	Reorder-tone timeout value, in seconds. Range is from 1 to 600. The default is 30.

Command Default

30 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the reorder tone timeout value when the call agent does not provide a timeout value associated with the request to generate a reorder tone signal.

Examples

The following example sets the reorder tone timeout value to 60 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone reorder 60
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tone ringback

To configure the ringback tone timeout value, use the **timeout tone ringback**command inMGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone ringback *ringback-tone-value*
no timeout tone ringback

Syntax Description

ringback -tone-value	Ringback-tone timeout value, in seconds. Range is from 1 to 600. The default is 180.

Command Default

180 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the ringback tone timeout value when the call agent does not provide a timeout value associated with the request to generate a ringback tone signal.

Examples

The following example sets the ringback tone timeout value to 120 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone ringback 120
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tone ringback connection

To configure the timeout value for the ringback tone on connection, use the **timeout tone ringback connection**command inMGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone ringback connection *connect-tone-value*
no timeout tone ringback connection

Syntax Description

connect -tone-value	Timeout value for the ringback tone on connection, in seconds. Range is from 1 to 600. The default is 180.

Command Default

180 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses this value when the call agent does not provide a timeout value associated with the request to generate the ringback tone signal on connection.

Examples

The following example sets the timeout value for the ringback tone on connection to 120 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone ringback connection 120
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tone ringing

To configure the ringing tone timeout value, use the **timeout tone ringing**command inMGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone ringing *ringing-tone-value*
no timeout tone ringing

Syntax Description

ringing -tone-value	Ringing tone timeout value, in seconds. Range is from 1 to 600. The default is 180.

Command Default

180 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the ringing tone timeout value when the call agent does not provide a timeout value associated with the request to generate a ringing tone signal.

Examples

The following example sets the ringing tone timeout value to 240 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone ringing 240
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tone ringing distinctive

To configure the distinctive ringing tone timeout value, use the **timeout tone ringing distinctive**command inMGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tone ringing distinctive *distinct-tone-value*
no timeout tone ringing distinctive

Syntax Description

distinct -tone-value	Distinctive-ringing tone timeout value, in seconds. Range is from 1 to 600. the default is 180.

Command Default

180 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the distinctive ringing tone timeout value when the call agent does not provide a timeout value associated with the request to generate a signal for distinctive ringing.

Examples

The following example sets the distinctive ringing tone timeout value to 240 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tone ringing distinctive 240
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

timeout tpar

To configure the partial timeout value, T(partial), for the interdigit timer used in digit map matching, use the **timeout tpar**command inMGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tpar *tpar-value*
no timeout tpar

Syntax Description

tpar -value	Partial timeout value, T(partial), in seconds. Range is from 1 to 60. The default is 16.

Command Default

16 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The interdigit timer is used when matching digit maps. It is started when the first digit is entered, and is restarted after each new digit is entered, until a digit map match or mismatch occurs.

The interdigit timer takes on one of two values, T(partial) or T(critical). When at least one more digit is required to make a match to any of the patterns in the digit map, the value of T(partial) is used for the timer. If a timer is all that is required to produce a match according to the digit map, T(critical) is used for the timer.

When the interdigit timer is used without a digit map, it takes on the value T(critical). It is started immediately and is simply canceled (but not restarted) as soon as a digit is entered.

Examples

The following example sets the partial timeout value to 15 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tpar 15
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.

Command	Description
timeout tcrit	Configures the MGCP critical timeout value, T(critical), for the interdigit timer used in digit map matching.

timeout tsmax

To configure the maximum timeout value after which MGCP messages are removed from the retransmission queue, use the **timeout tsmax**command in MGCP profile configuration mode. To reset to the default, use the **no** form of this command.

timeout tsmax *tsmax-value*
no timeout tsmax

Syntax Description

tsmax -value	Timeout value for MGCP messages to be removed from the retransmission queue, in seconds. Range is from 1 to 100. The default is 20.

Command Default

20 seconds

Command Modes

MGCP profile configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

The gateway uses the *tsmax-value* argument to determine how long to store MGCP messages before they are removed from the retransmission queue.

Examples

The following example sets the timeout value for the maximum retransmission of MGCP messages to 45 seconds:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# timeout tsmax 45
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.



timeouts call-disconnect through timing clear-wait

- timeouts call-disconnect, on page 69
- timeouts initial, on page 71
- timeouts interdigit (voice port), on page 72
- timeouts power-denial, on page 73
- timeouts ringing, on page 74
- timeouts wait-release, on page 75
- timeouts teardown lmr, on page 76
- timer accessrequest sequential delay, on page 77
- timer cluster-element, on page 78
- timer irr period, on page 80
- timer lrq seq delay, on page 81
- timer lrq seq delay centisec, on page 82
- timer lrq window, on page 83
- timer lrq window decisec, on page 84
- timer media-inactive, on page 85
- timer receive-rtcp, on page 87
- timer receive-rtp, on page 89
- timer server retry, on page 90
- timer server timeout, on page 91
- timers, on page 92
- timers buffer-invite, on page 94
- timers comet, on page 95
- timers connect, on page 96
- timers connection aging, on page 98
- timers connection establish, on page 99
- timers disconnect, on page 100
- timers dns, on page 102
- timers expires, on page 103
- timers hold, on page 105
- timers info, on page 106
- timers keepalive, on page 107

- timers notify, on page 109
- timers options, on page 111
- timers prack, on page 112
- timers refer, on page 114
- timers register, on page 115
- timers rel1xx, on page 116
- timers trying, on page 118
- timers update , on page 120
- timing answer-winkwidth, on page 121
- timing clear-wait, on page 122

timeouts call-disconnect

To configure the delay time for which a Foreign Exchange Office (FXO) voice port waits before disconnecting an incoming call after disconnect tones are detected, use the **timeouts call-disconnect command in**voice-port configuration mode. To reset to the default, use the **no** form of this command.

timeouts call-disconnect {**seconds** | **infinity**}
no timeouts call-disconnect

Syntax Description

seconds	Duration in seconds for which an FXO voice port stays in the connected state after the voice port detects a disconnect tone. Range is 1 to 120. The default is 60.
infinity	Disables disconnect supervision. The voice port does not disconnect when a disconnect tone is detected.

Command Default

60 seconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(9)T	This command was introduced on Cisco 3600 series routers.
12.0(4)T	This command was introduced on Cisco 3600 series routers.
12.2(2)T	This command was implemented on Cisco 1750, Cisco 2600 series, and Cisco MC3810. The **infinity** keyword was added.

Usage Guidelines

Use this command to change the time for which an FXO voice port remains connected after the calling party hangs up, when a call is not answered. Use of the **infinity** keyword is not recommended for disabling the disconnect supervision feature.

Examples

The following example configures voice port 0/0/1 to remain connected for 3 seconds while a disconnect tone is received by the voice port:

```
voice-port 0/0/1
 timeouts call-disconnect 3
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Specifies the delay time for releasing the calling voice port after a disconnect tone is received from the called voice port.

Command	Description
timing delay-duration	Configures the delay dial signal duration for a specified voice port.

timeouts initial

To configure the initial digit timeout value for a specified voice port, use the **timeouts initial**command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timeouts initial *seconds*
no timeouts initial *seconds*

Syntax Description

seconds	Initial timeout duration, in seconds. Range is 0 to 120. The default is 10.

Command Default

10seconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series routers.

Usage Guidelines

Use the **timeouts initial**command to specify the number of seconds for which the system waits for the caller to input the first digit of the dialed digits. The timeouts initial timer is activated when the call is accepted and is deactivated when the caller inputs the first digit. If the configured timeout value is exceeded, the caller is notified through the appropriate tone and the call is terminated.

To disable the timeouts initial timer, set the *seconds* value to 0.

Examples

The following example sets the initial digit timeout value to 10 seconds:

```
voice-port 1/0/0
 timeouts initial 10
```

Related Commands

Command	Description
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.

timeouts interdigit (voice port)

To configure the interdigit timeout value for a specified voice port, use the **timeouts interdigit**command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timeouts interdigit *seconds*
no timeouts interdigit *seconds*

Syntax Description

seconds	Interdigit timeout duration, in seconds. Range is 0 to 120. The default is 10.

Command Default

10seconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.

Usage Guidelines

Use this command to specify the number of seconds for which the system waits (after the caller inputs the initial digit) for the caller to input a subsequent digit of the dialed digits. The timeouts interdigit timer is activated when the caller inputs a digit and is restarted each time the caller inputs another digit until the destination address is identified. If the configured timeout value is exceeded before the destination address is identified, the caller is notified through the appropriate tone and the call is terminated.

To disable the timeouts interdigit timer, set the *seconds* value to 0.

Examples

The following example sets the interdigit timeout value on the Cisco 3600 series for 10 seconds:

```
voice-port 1/0/0
 timeouts interdigit 10
```

The following example sets the interdigit timeout value on the Cisco MC3810 for 10 seconds:

```
voice-port 1/1
 timeouts interdigit 10
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.

timeouts power-denial

To set the duration of the power denial timeout for the specified FXS voice port, use the **timeouts power-denial** command in voice-port configuration mode. To reset the timeout to the default, use the **no** form of this command.

timeouts power-denial *ms*
no timeouts power-denial

Syntax Description

ms	Length of power denial, in milliseconds (ms). Range: 0 to 2500. Default: 750.

Command Default

Default is 750 ms.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.4(2)T	The maximum value of the *ms* argument was increased from 1500 to 2500.

Usage Guidelines

This command sets the duration of the power denial that the voice gateway applies to the FXS port when a call disconnects. During the power denial duration the caller hears silence. To disable the power denial on a port, use the **no supervisory disconnect lcfo** command.

Examples

The following example sets the power-denial duration to 500 ms:

```
voice-port 2/0
 timeouts power-denial 500
```

Related Commands

Command	Description
supervisory disconnect lcfo	Signals a disconnect on an FXS loop-start port by applying a power denial using a LCFO.

timeouts ringing

To configure the timeout value for ringing, use the **timeouts ringing** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timeouts ringing {*seconds* | **infinity**}
no timeouts ringing

Syntax Description

seconds	Duration, in seconds, for which a voice port allows ringing to continue if a call is not answered. Range is 5 to 60000. Default is 180 for nonSCCP-controlled ports.
infinity	Ringing continues until the caller goes on-hook. Default value for SCCP-controlled analog ports.

Command Default

infinity for SCCP-controlled analog ports; 180 seconds for all other ports.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.4(11)T	The command default value was increased from 180 seconds to infinity for SCCP-controlled analog ports.

Usage Guidelines

This command allows you to limit the length of time for which a caller can continue ringing a telephone when there is no answer.

In Cisco IOS Release 12.4(11)T and later the default for this command is set to **infinity** for SCCP-controlled analog ports to prevent this timeout from expiring before the ringing no-answer timeout that is configured on Cisco Unified CallManager Express with the **timeouts ringing** command in telephony-service mode.

Examples

The following example configures voice port 0/0/1 to allow ringing for 600 seconds:

```
voice-port 0/0/1
 timeouts ringing 600
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a voice port.
timeouts interdigit	Configures the interdigit timeout value for a voice port.
timeouts ringing (telephony-service)	Sets the timeout value for ringing in a Cisco Unified CallManager Express system.

timeouts wait-release

To configure the delay timeout before the system starts the process for releasing voice ports, use the **timeouts wait-release** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timeouts wait-release {*seconds* | **infinity**}
no timeouts wait-release

Syntax Description

seconds	Duration, in seconds, for which a voice port stays in the call-failure state while the Cisco router or concentrator sends a busy tone, reorder tone, or out-of-service tone to the port. Range is 1 to 3600. Default is 30.
infinity	The voice port is never released as long as the call-failure state remains.

Command Default

30 seconds.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1) MA	This command was introduced on Cisco MC3810.
12.0(7)XK	This command was implemented on Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use this command to limit the time a voice port can be held in a call failure state. After the timeout, the release sequence is enabled.

You can also use this command for voice ports with Foreign Exchange Station (FXS) loop-start signaling to specify the time allowed for a caller to hang up before the voice port goes into the parked state.

Examples

The following example configures voice port 0/0/1 to stay in the call-failure state for 180 seconds while a busy tone, reorder tone, or out-of-service tone is sent to the voice port:

```
voice-port 0/0/1
 timeouts wait-release 180
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a voice port.
timeouts interdigit	Configures the interdigit timeout value for a voice port.

timeouts teardown lmr

To configure the time for which a Land Mobile Radio (LMR) voice port waits before tearing down an LMR connection after detecting no voice activity, use the **timeouts teardown lmr** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timeouts teardown lmr {*seconds* | **infinity**}
no timeouts teardown lmr {*seconds* | **infinity**}

Syntax Description

seconds	Duration in seconds for which an LMR voice port waits before tearing down an LMR connection after detecting no voice activity. Valid values are 5 to 60000. The default is 1800 seconds.
infinity	Disables disconnect supervision. The voice port does not disconnect when no voice activity is detected.

Command Default

1800 seconds

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

The **timeouts teardown lmr**command has an effect on an ear and mouth (E&M) voice port only if the signal type for that port is LMR.

Examples

The following example configures voice port 1/0/1 on a Cisco 3745 to remain connected for 6 seconds after no voice activity is detected by the voice port:

```
voice-port 1/0/1
 timeouts teardown lmr 6
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Specifies the delay time for releasing the calling voice port after a disconnect tone is received from the called voice port.
timeouts delay-duration	Configures the delay dial signal duration for a specified voice port.

timer accessrequest sequential delay

To configure the intermessage delay used when a border element (BE) is trying to determine a route from a list of neighboring BEs, use the **timer**accessrequest sequential delay command in Annex G configuration mode. To reset the default value, use the no form of this command.

timer accessrequest sequential delay *value*
no timer

Syntax Description

value	Amount of allowed intermessage delay (in increments of 100 ms). Range is from 0 to 10. The default is 1 (100 ms).

Command Default

1 (100 ms)

Command Modes

Annex G configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Setting the value of the delay to 0 causes the BE to broadcast or "blast" the AccessRequest messages to all eligible neighbors.

Examples

The following example shows a timer delay of 1000 ms.

```
Router(config)# call-router h323-annexg be20
Router(config-annexg)# timer accessrequest sequential delay 10
```

Related Commands

Command	Description
call -router	Enables the Annex G border element configuration commands.

timer cluster-element

To configure the length of time between dynamic capacity messages to the local gatekeeper, use the **timer cluster-element**command in gatekeeper configuration mode. To stop sending dynamic updates, use the **no** form of this command.

timer cluster-element {**announce** | **resource-update**} *seconds*
no timer cluster-element

Syntax Description

announce	Configures the lengh of time between announcement messages to the gatekeepers in the local cluster.
resource -update	Configures the lengh of time between resource update messages to gatekeepers in the local cluster.
seconds	Number of seconds between resource updates sent to the gatekeeper. The valid range is 1 to 60. There is no default value.

Command Default

Disabled by default.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on Cisco AS5850.
12.4(11)T	The **resource-update**keywordwas introduced.

Usage Guidelines

Use the **timer cluster-element**command to manage the length of time between resource updates and time between announcement messages sent to the gatekeeper. The announcement indication is exchanged at a set interval of time and carries information about the call and endpoint capacity for the zone. This allows the alternate gatekeepers to manage the bandwidth for a single zone even though the gatekeepers are in separate physical devices.

The gatekeeper assumes that the alternate gatekeeper has failed (and assumes that any previously allocated bandwidth is now available) if the gatekeeper does not receive an announcement message within six announcement periods or if the TCP connection with the gatekeeper is detected to be broken.

Lower this interval for closer tracking between elements. Raise it to lower messaging overhead.

Examples

The following command sets the announcement period to 20 seconds:

```
Router(config-gk)# timer cluster-element announce 20
```

The following command resets the announcement period to the default value:

```
Router(config-gk)# no timer cluster-element announce
```

The following example shows the time between resource update messages to gatekeepers in local cluster being set to 20 seconds:

```
Router(config-gk)# timer cluster-element resource-update 20
```

Related Commands

Command	Description
call-routing hunt-scheme	Enables capacity-based load-balancing.
zone cluster local	Defines a local grouping of gatekeepers.
zone remote	Statically specifies a remote zone if DNS is unavailable or undesirable.

timer irr period

To configure the information request response (IRR) timer, or the periodic interval of IRR messages sent by the gatekeeper, use the **timer irr period** command in gatekeeper configuration mode. To disable, use the **no** form of this command.

timer irr period *minutes*
no timer irr period

Syntax Description

minutes	Length, in minutes, of the interval between IRR messages. Range is from 1 to 60. The default is 4.

Command Default

4 minutes

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use this command to configure IRR frequency that is included in the admission confirm (ACF) message. The IRR frequency is set to 240 seconds (4 minutes), based on an average 4-minute call hold time. The IRR allows the gatekeepers to terminate calls for which a disengage request (DRQ) has not been received. If missing DRQs are not a problem, the IRR frequency can be set to a larger value than 4 minutes, minimizing the number of unnecessary IRRs sent by a gateway.

Examples

The following example shows that the IRR timer has been configured with a value of 45, meaning that IRR messages are sent by the gatekeeper every 45 minutes:

```
gatekeeper
.
.
.
lrq reject-resource-low
 no irq global-request
 timer lrq seq delay 10
 timer lrq window 6
 timer irr period 45
 no shutdown
```

Related Commands

Command	Description
timer lrq seq delay	Defines the time interval between successive LRQ messages.
timer lrq window	Defines the time window during which the gatekeeper collects responses to one or more outstanding LRQs.
timer server timeout	Specifies the timeout value for a response from a back-end GKTMP server.

timer lrq seq delay

To define the time interval between successive sequential location requests (LRQs), use the **timer lrq seq delay**command in gatekeeper configuration mode. To reset to the default, use the **no** form of this command.

timer lrq seq delay *time*
no timer lrq seq delay

Syntax Description

time	Time interval, in 100-millisecond units. Range is 1 to 10 (0.1 to 1 second). The default is 5 (500 milliseconds).

Command Default

5 units (500 milliseconds)

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on Cisco AS5850.

Usage Guidelines

The LRQ sequential timing source (SEQ) delay is used to set the time between sending LRQs to remote gatekeepers for address resolution. To resolve an address, the gatekeeper might have several remote zones configured, and it can send the LRQs simultaneously (blast) or sequentially (seq). The gatekeeper chooses the best route based on availability and cost. Using LRQs sequentially results in lower network traffic, but it can increase latency of calls when the most preferred route is unavailable.

Lowering the time increases traffic on the network but might reduce the call setup time.

Examples

The following command sets the LRQ delay timer to 100 milliseconds:

```
timer lrq seq delay 1
```

The following command resets the LRQ delay timer to the default value:

```
no timer lrq seq delay
```

Related Commands

Command	Description
timer lrq window	Defines the time window during which the gatekeeper collects responses to one or more outstanding LRQs.

timer lrq seq delay centisec

To define the time interval between successive sequential location requests (LRQs), use the **timer lrq seq delay centices**command in gatekeeper configuration mode. To reset to the default, use the **no** form of this command.

timer lrq seq delay centisec *time*
no timer lrq seq delay centisec

Syntax Description

time	Time interval, in 100-millisecond units. Range is 1 to 10 (0.1 to 1 second). The default is 1(100 milliseconds).

Command Default

Timers are set to their default value.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

The LRQ sequential timing source (SEQ) delay is used to set the time between sending LRQs to remote gatekeepers for address resolution. To resolve an address, the gatekeeper might have several remote zones configured, and it can send the LRQs simultaneously (blast) or sequentially (seq). The gatekeeper chooses the best route based on availability and cost. Using LRQs sequentially results in lower network traffic, but it can increase latency of calls when the most preferred route is unavailable.

Lowering the time increases traffic on the network but might reduce the call setup time.



Note This command cannot be configured at the same time as the **timer lrq seq delay**command.

Examples

The following command sets the LRQ delay timer to 100 milliseconds:

```
timer lrq seq delay centisec 1
```

The following command resets the LRQ delay timer to the default value:

```
no timer lrq seq delay centisec
```

Related Commands

Command	Description
timer lrq window decisec	Defines the time window during which the gatekeeper collects responses to one or more outstanding LRQs.

timer lrq window

To define the time window during which the gatekeeper collects responses to one or more outstanding LRQs, use the **timer lrq window**command in gatekeeper configuration mode. To reset to the default, use the **no** form of this command.

timer lrq window *seconds*
no timer lrq window

Syntax Description

seconds	Time window, in seconds. Range is 1 to 15. The default is 3.

Command Default

3 seconds

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on Cisco AS5850.

Usage Guidelines

Increasing the time can increase the call success rate but might reduce the overall time for call setup.

Examples

The following command sets the timer to 5 seconds:

```
timer lrq window 5
```

The following command sets the timer to the default value:

```
no timer lrq window
```

Related Commands

Command	Description
timer lrq seq delay	Defines the time interval between successive sequential LRQs.

timer lrq window decisec

To define the time window during which the gatekeeper collects responses to one or more outstanding LRQs, use the **timer lrq window decisec**command in gatekeeper configuration mode. To reset to the default, use the **no** form of this command.

timer lrq window decisec *time*
no timer lrq window decisec

Syntax Description

time	Time window, in seconds. Range is 1 to 15. The default is 2.

Command Default

Timers are set to their default value.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Increasing the time can increase the call success rate but might reduce the overall time for call setup.

Note This command cannot be in effect at the same time as the **timer lrq window**command.

Examples

The following command sets the timer to 5 seconds:

```
timer lrq window decisec 2
```

The following command sets the timer to the default value:

```
no timer lrq window decisec
```

Related Commands

Command	Description
timer lrq seq delay centsec	Defines the time interval between successive sequential LRQs.

timer media-inactive

To enable the timer for media inactivity detection using the digital signal processor (DSP) (based on RTP as the only criterion) and to configure a multiplication factor based on the real-time control protocol (RTCP) timer interval, use the **timer media-inactive** command in gateway configuration mode. To reset to the default, use the **no**form of this command.

timer media-inactive *multiple*
no timer media-inactive *multiple*

Syntax Description

multiple	Multiples of the RTCP report transmission interval. Range is 4 to 1000. The default is 5, and the recommended value is 5.

Command Default

A call is considered inactive if no RTP packet activity is detected for a period of time calculated as five times the interval set by the **ip rtcp report interval** command.

Command Modes

Gateway configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

When the **timer media-inactive** command is used, the gateway uses the inactivity timer as a combination of the **timer media-inactive** command and the **ip rtcp report interval** command. The **timer media-inactive**command uses DSP statistics. This capability is based on the configuration of callfeature parameters using application command-line interface (CLI) to enable control.

The media are considered inactive only if there is no transfer of RTP packets in the send direction and no RTP packets in the receive direction. If RTP is present in either the send or receive direction, it is considered active. In this mode, DSP filters out any comfort noise packets, and the presence of any comfort noise packet is considered inactivity in either direction.

The *multiple* argument (or multiplication factor) is multiplied by the interval that is set using the **ip rtcp report interval** command. This command configures the average interval between successive RTCP report transmissions for a given voice session. For example, if the *value* argument is set to 25,000 milliseconds, an RTCP report is sent every 25 seconds, on average. If no RTP packets are received during the calculated interval, the call is disconnected. The gateway signals the disconnect to the VoIP network and the time-division multiplexing (TDM) network so that upstream and downstream devices can clear their resources.

Examples

The following example uses the **ip rtcp report interval**command to set the reporting interval to 5000 milliseconds, and then the **timer media-inactive** command to set the multiplication factor to 10. The result is that calls detected as inactive for 50 seconds (5,000 milliseconds times 10) will be disconnected.

```
Router(config)# ip rtcp report interval 5000
Router(config)# gateway
Router(config-gateway)# timer media-inactive 10
Router(config-gateway)# exit
```

Related Commands

Command	Description
ip rtcp report interval	Configures the minimum interval of RTCP report transmissions.

timer receive-rtcp

To enable the Real-Time Control Protocol (RTCP) timer and to configure a multiplication factor for the RTCP timer interval for Session Initiation Protocol (SIP) or H.323, use the **timer receive-rtcp** command in gateway configuration mode. To reset to the default, use the **no** form of this command.

timer receive-rtcp *timer*
no timer receive-rtcp *timer*

Syntax Description

timer	Multiples of the RTCP report transmission interval. Range is 0 to 1000. Default is 0. Recommended value is 5.

Command Default

The default value for the *timer* argument is 0 multiples, which disables the timer so that no silence detection is in effect.

Command Modes

Gateway configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

The **timer receive-rtcp** command uses library-based detection and the receipt of either Real-Time Protocol (RTP) or RTCP packets is considered activity on a call. Silence detection occurs only if there are no packets received for both RTP and RTCP.

When the **ip rtcp report interval** and **timer receive-rtcp** commands are used, the gateway uses RTCP report detection, rather than RTP packet detection, to determine whether calls on the gateway are still active or should be disconnected. RTCP report detection is therefore more reliable than RTP packet detection because there can be periods during voice calls when one or both parties are not sending RTP packets.

One common example of a voice session in which no RTP is sent is when a caller dials into a conference call and mutes that endpoint. If voice activity detection (VAD, also known as silence suppression) is enabled, no RTP packets are sent while the endpoint is muted. However, the muted endpoint continues to send RTCP reports at the interval specified by the **ip rtcp report interval** command.

The **timer receive-rtcp** *timer* argument (or *m* factor for multiplication factor) is multiplied by the interval that is set using the **ip rtcp report interval**command. If no RTP or RTCP packets are received during the calculated interval, the call is disconnected. The gateway signals the disconnect to the VoIP network and the time-division multiplex (TDM) network so that upstream and downstream devices can clear their resources. The gateway sends a Q.931 DISCONNECT message to the TDM network and a SIP BYE or H.323 ReleaseComplete message to the VoIP network to clear the call when the timer expires. The Q.931 DISCONNECT message is sent with a cause code value of 3 (no route) for SIP calls and a cause code value of 41 (temporary failure) for H.323 calls. No Q.931 Progress Indicator (PI) value is included in the DISCONNECT message.

To show timer-related output for SIP calls, use the **debug ccsip events** command. To show timer-related output for H.323 calls, use the **debug cch323 h225**command.

Examples

The following example sets the multiplication factor to 10 (or *x* * 10, where *x* is the interval that is set with the **ip rtcp report interval** command):

```
Router(config)# gateway
Router(config-gateway)# timer receive-rtcp 10
Router(config-gateway)# exit
```

Related Commands

Command	Description
debug cch323 h225	Traces the state transition of the gateway H.225 state machine based on the processed events.
debug ccsip events	Displays all SIP SPI events tracing and traces the events posted to SIP SPI from all interfaces.
ip rtcp report interval	Configures the minimum interval of RTCP report transmissions.

timer receive-rtp

To configure the Real-Time Transport Protocol (RTP) timeout interval to clear connections that pause indefinitely, use the **timer receive-rtp** command in gateway configuration mode. To reset the timer to the default value, use the **no** form of this command.

timer receive-rtp *seconds*
no timer receive-rtp

Syntax Description

seconds	Timer value, in seconds. Range: 180 to 86400. Default: 1200.

Command Default

1200 seconds (20 minutes)

Command Modes

Gateway configuration (config-gateway)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(20)T	This command was modified. The recommended timer range is defined as 1200 seconds.

Usage Guidelines

This command is used to configure the RTP timeout interval in seconds. The timeout value is used to clear connections that pause indefinitely. The recommended value is 1200 seconds, or 20 minutes.

Examples

The following example shows the RTP timeout interval set to the recommended 1200 seconds (20 minutes).

```
Router(config-gateway)# timer receive-rtp 600
```

Related Commands

Command	Description
codec (dspfarm-profile)	Specifies the codecs supported by a DSP farm profile.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
maximum sessions (dspfarm-profile)	Specifies the maximum number of sessions that need to be supported by the profile.

timer server retry

To set the gatekeeper's retry timer for failed Gatekeeper Transaction Message Protocol (GKTMP) connections, use the **timer server retry** command in gatekeeper configuration mode. To reset the timer to its default, use the **no** form of this command or the **default server timer retry** command.

server timer retry *seconds*
no server timer retry
default server timer retry

Syntax Description

seconds	Number of seconds for which the gatekeeper should wait before retrying the GKTMP server. Range is from 1 through 300. The default is 30.

Command Default

30 seconds

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

After the gatekeeper detects that its GKTMP server TCP connection has failed, the gatekeeper retries the server after an interval based on the setting of this timer, and keeps retrying until the connection is established.

This timer applies only to deployments where static triggers are used between the gatekeeper and the GKTMP server. If dynamic triggers are used, the server must determine and implement a retry mechanism if the TCP connection to the gatekeeper fails.

Examples

The following example shows that the retry timer has been set to 45 seconds:

```
Router# show gatekeeper configuration
.
.
.
h323id tet
 gw-type-prefix 1#* default-technology
 gw-type-prefix 9#* gw ipaddr 1.1.1.1 1720
 timer server retry 45
 no shutdown
.
.
.
```

Related Commands

Command	Description
timer server timeout	Specifies the timeout value for a response from a back-end GKTMP server.

timer server timeout

To specify the timeout interval for a response from a back-end Gatekeeper Transaction Message Protocol (GKTMP) application server, use the **timer server timeout**command in gatekeeper configuration mode. To reset to the default, use the **no** form of this command.

timer server timeout *time*
no timer server timeout

Syntax Description

time	Timeout interval, in 100-ms units. Range is 1 to 50 (0.1 to 5 seconds). Default is 3 (300 ms).

Command Default

3 units

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(2)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Usage Guidelines

Use this command to specify the timeout interval for a response from a back-end GKTMP application server.

Examples

The following command sets the timeout interval to 400 ms:

```
timer server timeout 4
```

The following command resets the timeout interval to the default value:

```
no timer server timeout
```

Related Commands

Command	Description
server registration -port	Configures the listener port for the server to establish a connection with the gatekeeper.
server trigger	Configures a static server trigger for external applications.

timers

To configure the Session Initiation Protocol (SIP) signaling timers, use the **timers** command in SIP user-agent configuration mode. To restore the default value, use the **no** form of this command.

timers {**trying** *number* | **connect** *number* | **disconnect** *number* | **expires** *number*}
no timers

Syntax Description

trying *number*	Time (in ms) to wait for a 100 response to an INVITE request. Range is from 100 to 1000. Default is 500.
connect *number*	Time (in ms) to wait for a 200 response to an ACK request. Range is from 100 to 1000. Default is 500.
disconnect *number*	Time (in ms) to wait for a 200 response to a BYE request. Range is from 100 to 1000. Default is 500.
expires *number*	Time (in ms) for which an INVITE request is valid. Range is from 60000 to 300000. Default is 180000.

Command Default

trying , **connect**, and **disconnect**--500 ms**expires**--180000 ms

Command Modes

SIP user-agent configuration (config-sip-ua)

Voice class tenant configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.1(3)T	This command was modified to change the names of the parameters. Two of the parameters (**invite-wait-180** and **invite-wait-200**) were combined into one (**trying**).
12.2(2)XA	This command was implemented on the Cisco AS5400 and AS5350.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series routers. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models under SIP user agent configuration mode.

Release	Modification
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models under voice class tenant configuration mode.

Usage Guidelines

If you used an earlier version of this command to configure timers, the timer settings are maintained. The output of the show running-config command reflects both previous and current timers.

To reset this command to the default value, you can also use the default command.

Examples

The following example sets the trying timers to the default of 500 ms.

```
Router(config)# sip-ua
Router(config-sip-ua)# timers trying 500
```

Related Commands

Command	Description
default	Sets a command to its default.
inband - alerting	Specifies an inband-alerting SIP header.
max - forwards	Specifies the maximum number of hops for a request.
retry (SIP user - agent)	Configures the SIP signaling timers for retry attempts.
transport	Enables SIP UA transport for TCP/UDP.

timers buffer-invite

To enable the Session Initiation Protocol (SIP) buffer-invite timer and to configure the timer interval, use the timers buffer-invite command in SIP user-agent configuration mode or voice class tenant configuration mode. To restore the default value, use the **no** form of this command.

timers buffer-invite *timer* **system**
no timers buffer-invite

Syntax Description

timer	Buffer-invite timer value, in ms. Range is 50 to 5000.
system	Specifies that the buffer-invite timer use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

Disabled

Command Modes

SIP user-agent configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.3(8)T	This command was introduced.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

Use this command to enable the SIP buffer-invite timer and to configure the timer interval. Configure the command **isdn supp-service name calling** under the serial interface before configuring the command **timers buffer-invite**. Without configuring **isdn supp-service name calling** command, the timer to buffer the outgoing invite is not triggered.

Note For more details on the command **isdn supp-service name calling**, see isdn supp-service name calling.

Examples

The following example sets retransmission time to 500 milliseconds:

```
Router(config-class)# timers buffer-invite system
```

The following example sets retransmission time in the voice class tenant configuration mode:

Related Commands

Command	Description
sip-ua	Enables SIP user-agent configuration commands.

timers comet

To set how long the Session Initiation Protocol (SIP) user agent (UA) waits before retransmitting conditions-met (COMET) requests, use the **timers comet**command in SIP user-agent configuration mode. To reset to the default, use the **no** form of this command.

timers comet *time*
no timers comet

Syntax Description

time	Waiting time, in milliseconds. Range is 100 to 1000. The default is 500.

Command Default

500 milliseconds

Command Modes

SIP user-agent configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was inplemented on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.

Usage Guidelines

COMET, or conditions met, indicates whether preconditions for a given call or session have been met. This command is applicable only with calls involving quality of service (QoS) (calls other than best-effort).

Examples

The following example sets retransmission time to 500 milliseconds:

```
Router(config)# sip-ua
Router(config-sip-ua)# timers comet 500
```

Related Commands

Command	Description
show sip -ua statistics	Displays response, traffic, timer, and retry statistics.
show sip -ua timers	Displays the current settings for SIP UA timers.
timers prack	Sets how long the UA waits before retransmitting a PRACK request.

timers connect

To set how long the Session Initiation Protocol (SIP) user agent (UA) waits for a 200 response to an ACK request, use the **timers connect** command in SIP user-agent configuration mode or voice class tenant configuration mode. To reset to the default, use the no form of this command.

timers connect *number* **system**
no timers connect *number*

Syntax Description

number	Waiting time, in milliseconds. Range is from 100 to 1000. The default is 500.
system	Use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

500 milliseconds

Command Modes

SIP user-agent configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.1(1)T	This command was introduced on Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(3)T	This command was modified to change the names of the parameters. Two of the parameters (invite-wait-180 and invite-wait-200) were combined into one (trying).
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

If you used the previous more generic **timers** command to configure timers, your previous timer settings are maintained. The output of the show running-config command reflects both timers.

To reset this command to the default value, you can also use the default command.

Examples

The following example sets connect time to 200 milliseconds:

```
sip-ua
 timers connect 200
```

The following example sets connect time in the voice class tenant configuration mode:

```
Router(config-class)# timers connect system
```

Related Commands

Command	Description
sip-ua	Enables the SIP user-agent configuration commands.

timers connection aging

To globally set the time before the Session Initiation Protocol (SIP) user agent (UA) ages out a TCP or UDP connection because of inactivity, use the **timers connection aging** command in SIP user-agent configuration mode or voice class tenant configuration mode. To reset this time to the default value, use the no form of this command.

timers connection aging *timer-value* **system**
no timers connection aging

Syntax Description

timer-value	Time to wait, in minutes, before aging out a TCP or UDP connection because of inactivity. Range is from 5 to 30. Default is 5.
system	Use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

5 minutes

Command Modes

SIP user-agent configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.3(8)T	This command was introduced.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

The minimum value of this connection is 5 minutes.

Examples

The following example ages out a connection in 10 minutes:

```
sip-ua
 timers connection aging 10
```

The following example ages out a connection in the voice class tenant configuration mode:

```
Router(config-class)# timers connection aging system
```

Related Commands

Command	Description
show sip-ua timers	Displays the current settings for the SIP UA timers.
sip-ua	Enables the SIP user-agent configuration commands.
timers expires	Sets how long a SIP INVITE request is valid.

timers connection establish

To set the time to wait for establishing TLS connection with the remote server, use the **timers connection establish tls** command in SIP user-agent configuration mode. To reset this time to the default value, use the no form of this command.

timers connection establish tls *timer-value*
no timers connection establish tls

Syntax Description

timer-value	Time to wait, in seconds, for successfully establishing a TLS connection with the remote server. Range is from 5 to 20. Default is 20.

Command Default

20 seconds

Command Modes

SIP user-agent configuration

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.4.1a	This command was introduced.

Usage Guidelines

Use this command to set the time to wait for establishing a TLS connection with the remote server. The minimum value is 5 seconds and maximum value is 20 seconds. The default value is 20 seconds.

Examples

The following example sets the time to wait before establishing a TLS connection:

```
router(config-sip-ua)#timer connection establish tls 10
```

Related Commands

Command	Description
show sip-ua timers	Displays the current settings for the SIP UA timers.

timers disconnect

To set how long the Session Initiation Protocol (SIP) user agent (UA) waits for a 200 response to a BYE request, use the **timers** command in SIP user-agent configuration mode or voice class tenant configuration modeTo reset to the default, use the no form of this command.

timers disconnect *time* **system**
no timers disconnect *time*

Syntax Description

time	Waiting time, in milliseconds. Range is 100 to 1000. The default is 500.
system	Use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

500 milliseconds

Command Modes

SIP user-agent configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.1(1)T	This command was introduced on Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(3)T	This command was modified to change the names of the parameters. Two of the parameters (invite-wait-180 and invite-wait-200) were combined into one (trying).
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS400.
12.2(2)XB1	This command was implemented on Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series. Supported for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms is not included in this release.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

If you used the previous more generic **timers** command to configure timers, your previous timer settings are maintained. The output of the show running-config command reflects both timers.

To reset this command to the default value, you can also use the default command.

Examples

The following example sets disconnect time to 200 milliseconds:

```
sip-ua
 timers disconnect 200
```

The following example sets disconnect time in the voice class tenant configuration mode:

```
Router(config-class)# timers disconnect system
```

Related Commands

Command	Description
sip-ua	Enables the SIP user-agent configuration commands.

timers dns

To set how long the Session Initiation Protocol (SIP) user agent (UA) waits for the DNS resolved address cache, use the **timersdns** command in SIP user-agent configuration mode or voice class tenant configuration mode. To reset to the default, use the no form of this command.

timers dns system
no timers dns

Syntax Description

registrar-cache	DNS cache refresh time for registrar.
time	Waiting time, in seconds. Range is 60 to 65535. The default is 65535.
system	Use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

65535 seconds

Command Modes

SIP user-agent configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
15.1(4)T	This command was introduced.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

If you used the previous more generic **timers** command to configure timers, your previous timer settings are maintained. The output of the show running-config command reflects both timers.

To reset this command to the default value, you can also use the default command.

Examples

The following example sets DNS cache refresh time to 200 seconds:

```
sip-ua
 timers dns registrar-cache 200
```

The following example sets DNS cache refresh time in the voice class tenant configuration mode:

```
Router(config-class)# timers dns registrar-cache system
```

Related Commands

Command	Description
sip-ua	Enables the SIP user-agent configuration commands.

timers expires

To set how long a Session Initiation Protocol (SIP) INVITE request is valid, use the **timers** command in SIP user-agent configuration mode or voice class tenant configuration mode. To reset to the default, use the no form of this command.

timers *expires time* **system**
no timers *expires*

Syntax Description

time	Expiration time, in ms. Range is 60,000 to 300,000. Default is 180000.
system	Use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

180000 ms

Command Modes

SIP user-agent configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(3)T	This command was modified to change the names of the parameters. Two of the parameters (invite-wait-180 and invite-wait-200) were combined into one (trying).
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

If you used the previous more generic **timers** command to configure timers, your previous timer settings are maintained. The output of the show running-config command reflects both timers.

To reset this command to the default value, you can also use the default command.

Examples

The following example sets the expiration time to 180,000 ms:

```
sip-ua
 timers expires 180000
```

The following example sets the expiration time in the voice class tenant configuration mode:

```
Router(config-class)# timers expires system
```

Related Commands

Command	Description
default	Enables a default aggregation cache.
sip-ua	Enables the SIP user-agent configuration commands.
timers	Configures the SIP signaling timers.

timers hold

To enable the Session Initiation Protocol (SIP) hold timer and configure the timer interval before disconnecting a held call, use the **timers hold** command in SIP user-agent configuration mode or voice class tenant configuration mode. To restore the default value, use the **no** form of this command.

timers *hold time* **system**
no timers *hold*

Syntax Description

time	Time (in minutes) to wait before sending a BYE request. Range is 15 to 2880. Default is 2880.
system	Use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

Enabled

time: 2880 minutes

Command Modes

SIP user-agent configuration mode

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.3(1)	This command was introduced.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.

Usage Guidelines

The hold timer is typically activated when a gateway receives a call hold request from the other endpoint, for example, a SIP phone.

Examples

The following example sets the hold timer to expire after 75 minutes:

```
Router(config-sip-ua)# timers hold 75
```

The following example sets the hold timer in the voice class tenant configuration mode:

```
Router(config-class)# timers hold system
```

Related Commands

Command	Description
show sip-ua timers	Displays the current settings for SIP user agent timers.
suspend - resume	Enables SIP Suspend and Resume (call-hold) functionality.
timer receive-rtcp	Enables media inactivity Real-Time Control Protocol (RTCP) timer.

timers info

To specify the wait time before INFO retransmission, use the **timers info** timers command in SIP user-agent configuration mode or voice class tenant configuration mode. To reset this value to the default, use the **no** form of this command.

timers info *milliseconds*
no timers info

Syntax Description

milliseconds	Waiting time, in milliseconds. Range is from 100 to 1000. Default is 500.

Command Default

500 milliseconds

Command Modes

SIP user-agent configuration

voice class tenant configuration (config-class)

Command History

Release	Modification
Cisco IOS 15.6(2)T	This command was introduced.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Example

In sip-ua mode:

```
Device> enable
Device# configure terminal
Device(config)# sip-ua
Device(config-sip-ua)# timers info 300
```

In voice class tenant mode:

```
Device> enable
Device# configure terminal
Device(config)# voice class tenant 1
Device(config-class)# timers info 300
```

timers keepalive

To set the keepalive timers interval between sending Options message requests when the session initiation protocol (SIP) servers are in the down state, use the **timers keepalive** command in SIP user agent configuration mode. To restore the keepalive timers to the default value of 120 seconds when active or 30 seconds when down, use the **no** form of this command.

timers keepalive {**active** | **down**} *seconds*
no timers keepalive {**active** | **down**} *seconds*

Syntax Description

active	SIP servers are in the active state.
down	SIP servers are in the down state.
seconds	Time in seconds between keepalive messages when the SIP servers are either active or down, as follows: • If **active** is specified, the range is from 10 to 600 seconds; the default value is 120 seconds. • If **down** is specified, the range is from 1 to 120 seconds; the default value is 30 seconds.

Command Default

The default value for the active state is 120 seconds and the default value for the down state is 30 seconds.

Command Modes

SIP user agent configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

Use this command to change the keepalive message time interval in seconds between the sending Options message requests when the SIP server or servers are either in the active or down state.

Examples

The following example sets the keepalive message time interval to 20 seconds when the SIP server is in the active state:

```
sip-ua
 timers keepalive active 20
```

The following example sets the keepalive message time interval to 10 seconds when the SIP server is in the down state:

```
sip-ua
 timers keepalive down 10
```

Related Commands

Command	Description
busyout monitor keepalive	Selects a voice port or ports to be busied out in cases of a keepalive failure.
keepalive target	Identifies a SIP server that will receive keepalive packets from the SIP gateway.
keepalive trigger	Sets number of Options message requests that must consecutively receive responses from the SIP servers in order to unbusy the voice ports when in the down state.
retry keepalive	Sets the retry keepalive count for retransmissions.

timers notify

To set how long the Session Initiation Protocol (SIP) user agent (UA) waits before retransmitting a Notify message, use the **timers notify** command in SIP user-agent configuration mode or voice class tenant configuration mode. To reset to the default, use the **no** form of this command.

timers notify *time* **system**
no timers notify

Syntax Description

time	Waiting time, in milliseconds. Range is 100 to 1000. The default is 500.
system	Use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

500 milliseconds

Command Modes

SIP user-agent configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB2	This command was implemented on Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

A Notify message informs the user agent that initiated the transfer or Refer request about the outcome of the SIP transaction.

Examples

The following example sets retransmission time to 500 milliseconds:

```
Router(config)# sip-ua
Router(config-sip-ua)# timers notify 500
```

The following example sets retransmission time in the voice class tenant configuration mode:

```
Router(config-class)# timers notify system
```

Related Commands

Command	Description
show sip -ua statistics	Displays response, traffic, timer, and retry statistics
show sip -ua timers	Displays the current settings for SIP UA timers

timers options

To specify the wait time before OPTIONS retransmission, use the **timers options** timers command in SIP user-agent configuration mode or voice class tenant configuration mode. To reset this value to the default, use the **no** form of this command.

timers options *milliseconds*
no timers options

Syntax Description

milliseconds	Waiting time, in milliseconds. Range is from 100 to 1000. Default is 500.

Command Default

500 milliseconds

Command Modes

SIP user-agent configuration

voice class tenant configuration (config-class)

Command History

Release	Modification
Cisco IOS 15.6(2)T	This command was introduced.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Example

In sip-ua mode:

```
Device> enable
Device# configure terminal
Device(config)# sip-ua
Device(config-sip-ua)# timers options 300
```

In voice class tenant mode:

```
Device> enable
Device# configure terminal
Device(config)# voice class tenant 1
Device(config-class)# timers options 300
```

timers prack

To set how long the Session Initiation Protocol (SIP) user agent (UA) wait s before retransmitting a provisional response acknowledgement (PRACK) request, use the **timers prack** command in SIP user-agent configuration mode or voice class tenant configuration mode. To reset to the default, use the **no** form of this command.

timers prack *time* **system**
no timers prack

Syntax Description

time	Waiting time, in milliseconds. Range is 100 to 1000. The default is 500.
system	Use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

500 milliseconds

Command Modes

SIP user-agent configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was applicable to the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

PRACK allows reliable exchanges of SIP provisional responses between SIP endpoints. When the retransmission value is set, retransmissions are sent with an exponential backoff of up to 4 seconds. That is, the retransmission interval for each packet increases exponentially until 4 seconds is reached.

Examples

The following example sets retransmission time to 500 milliseconds:

```
Router(config)# sip-ua
Router(config-sip-ua)# timers prack 500
```

The following example sets retransmission time in the voice class tenant configuration mode:

```
Router(config-class)# timers prack system
```

Related Commands

Command	Description
show sip -ua statistics	Displays response, traffic, timer, and retry statistics.
show sip -ua timers	Displays the current settings for SIP UA timers.
timers comet	Sets how long the UA waits before retransmitting a COMET request.

timers refer

To set how long the Session Initiation Protocol (SIP) user agent (UA) waits before retransmitting a Refer request, use the **timers refer** command in SIP user-agent configuration mode or voice class tenant configuration mode. To reset to the default, use the **no** form of this command.

timers refer *time* **system**
no timers refer

Syntax Description

time	Waiting time, in milliseconds. Range is from 100 to 1000. Default is 500.
system	Use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

500 milliseconds

Command Modes

SIP user-agent configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.2(11)YT	This command was introduced.
12.2(15)T	This command is supported on the Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, and the Cisco 7200 series routers in this release.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

A SIP Refer request is sent by the originating gateway to the receiving gateway and initiates call forward and call transfer capabilities.

Examples

The following example sets retransmission time to 500 milliseconds:

```
Router(config)# sip-ua
Router(config-sip-ua)# timers refer 500
```

The following example sets retransmission time in the voice class tenant configuration mode:

```
Router(config-class)# timers refer system
```

Related Commands

Command	Description
show sip -ua statistics	Displays response, traffic, timer, and retry statistics.
show sip -ua timers	Displays the current settings for SIP UA timers.

timers register

To set how long the Session Initiation Protocol (SIP) user agent (UA) waits before sending register requests, use the **timers register** command in SIP user-agent configuration mode or voice class tenant configuration mode. To reset this value to the default, use the **no** form of this command.

timers register *milliseconds* **system**
no timers register

Syntax Description

milliseconds	Waiting time, in milliseconds. Range is from 100 to 1000. Default is 500.
system	Use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

500 milliseconds

Command Modes

SIP user-agent configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(22)T	Support for IPv6 was added.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Examples

The following example sends register requests every 500 milliseconds:

```
sip-ua
 retry invite 9
 retry register 9
 timers register 500
```

The following example sends register requests in the voice class tenant configuration mode:

```
Router(config-class)# timers register system
```

Related Commands

Command	Description
retry register	Sets the total number of SIP registers to send.

timers rel1xx

To set how long the Session Initiation Protocol (SIP) user agent (UA) waits before retransmitting a reliable1xx response, use the **timers rel1xx** command in SIP user-agent configuration mode or voice class tenant configuration mode. To reset to the default, use the **no** form of this command.

timers rel1xx *time* **system**
no timers rel1xx

Syntax Description

time	Waiting time, in milliseconds. Range is 100 to 1000. The default is 500.
system	Use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

500 milliseconds

Command Modes

SIP user-agent configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Examples

The following example sets retransmission time to 400 milliseconds:

```
Router(config)# sip-ua
Router(config-sip-ua)# timers rel1xx 400
```

The following example sets retransmission time in the voice class tenant configuration mode:

```
Router(config-class)# timers rel1xx system
```

Related Commands

Command	Description
retry rel1xx	Configures how many times the reliable1xx response is retransmitted.

Command	Description
show sip -ua statistics	Displays response, traffic, timer, and retry statistics.
show sip -ua timers	Displays the current settings for SIP UA timers.

timers trying

To set how long the Session Initiation Protocol (SIP) user agent (UA) wait s for a 100 response to a SIP INVITE request, use the **timers** command in SIP user-agent configuration mode or voice class tenant configuration mode. To reset to the default, use the no form of this command.

timers *trying time* **system**
no timers *trying*

Syntax Description

time	Waiting time, in milliseconds. Range is 100 to 1000. The default is 500.
system	Use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

500 milliseconds

Command Modes

SIP user-agent configuration

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(3)T	This command was modified to change the names of the parameters. Two of the parameters (invite-wait-180 and invite-wait-200) were combined into one (trying).
12.2(2)XA	This command was implemented on Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series routers. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

If you used the previous more generic **timers** command to configure timers, your previous timer settings are maintained. The output of the show running-config command reflects both timers.

To reset this command to the default value, you can also use the default command.

Examples

The following example sets trying time to 500 milliseconds.

```
sip-ua
 timers trying 500
```

The following example sets trying time in the voice class tenant configuration mode:

```
Router(config-class)# timers trying system
```

Related Commands

Command	Description
sip-ua	Enables the SIP user-agent configuration commands.

timers update

To set how long the Session Initiation Protocol (SIP) user agent (UA) waits before sending update requests, use the **timers update** timers command in SIP user-agent configuration mode or voice class tenant configuration mode. To reset this value to the default, use the **no** form of this command.

timers update *milliseconds* **[system]**
no timers update

Syntax Description

milliseconds	Waiting time, in milliseconds. Range is from 100 to 1000. Default is 500.
system	Uses the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

500 milliseconds

Command Modes

SIP user-agent configuration

voice class tenant configuration (config-class)

Command History

Release	Modification
Cisco IOS 15.6(2)T and Cisco IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

Executing this command sets the wait time before sending update requests.

Example

In sip-ua mode:

```
Device> enable
Device# configure terminal
Device(config)# sip-ua
Device(config-sip-ua)# timers update 300
```

In voice class tenant mode:

```
Device> enable
Device# configure terminal
Device(config)# voice class tenant 1
Device(config-class)# timers update 300
```

timing answer-winkwidth

To specify the minimum duration delay between start of incoming seizure and wink in signal. Use the timing answer-winkwidth command in voice-port configuration mode. To reset to the default, use the no form of this command.

timing answer-winkwidth *time*
no timing answer-winkwidth *time*

Command History

Syntax Description

Syntax Description

time	Duration of the answer winkwidth delay in milliseconds. Range is from 110 to 290. The default is 210

Command Default

no timing answer-winkwidth

or

timing answer-winkwidth 210

Command Modes

Voice-port configuration

timing clear-wait

To set the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port, use the **timing clear-wait**command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing clear-wait *time*
no timing clear-wait *time*

Syntax Description

time	Minimum time, in milliseconds, between an inactive seizure signal and the call being cleared. Cisco 3600 series range is from 200to 2000. The default for both is 400.

Command Default

400 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 2600 and Cisco 3600 series routers.

Usage Guidelines

This command is supported on E&M ports only.

Examples

The following example sets the clear-wait duration on a voice port to 300 milliseconds:

```
voice-port 1/0/0
 timing clear-wait 300
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.

Command	Description
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.



timing delay-duration through type (voice)

- timing delay-duration, on page 127
- timing delay-start, on page 129
- timing delay-voice tdm, on page 131
- timing delay-with-integrity, on page 133
- timing dialout-delay, on page 135
- timing dial-pulse min-delay, on page 137
- timing digit, on page 139
- timing guard-out, on page 141
- timing hangover, on page 142
- timing hookflash-in, on page 143
- timing hookflash-out, on page 145
- timing ignore m-lead, on page 146
- timing interdigit, on page 147
- timing opx-ringwait, on page 149
- timing percentbreak, on page 150
- timing pulse, on page 151
- timing pulse-interdigit, on page 153
- timing sup-disconnect, on page 155
- timing wait-wink, on page 157
- timing wink-duration, on page 159
- timing wink-wait, on page 161
- tls, on page 163
- toggle-between-two-calls, on page 164
- token-root-name, on page 166
- tone busytone, on page 168
- tone dialtone, on page 169
- tone incoming, on page 171
- tone incoming system, on page 173
- tone ringback alert-no-PI, on page 174
- trace (voice service voip), on page 175
- transfer, on page 177
- translate, on page 179
- translate (translation profiles), on page 181

- translate-outgoing, on page 183
- translation-profile (dial peer), on page 185
- translation-profile (source group), on page 186
- translation-profile (trunk group), on page 187
- translation-profile (voice port), on page 188
- translation-profile (voice service POTS), on page 189
- translation-rule, on page 191
- transport (sip-ua), on page 193
- transport switch, on page 197
- trunk group (global), on page 198
- trunk-group (CAS custom), on page 200
- trunkgroup (dial peer), on page 202
- trunk-group (interface), on page 204
- trunk-group (voice port), on page 206
- trunk-group-label (dial peer), on page 208
- trunk-group-label (voice source group), on page 209
- trustpoint (DSP farm profile), on page 210
- trustpoint (voice class), on page 211
- ttl, on page 213
- type (settlement), on page 214
- type (voice), on page 216

timing delay-duration

To specify the delay signal duration for a specified voice port, use the **timing delay-duration**command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing delay-duration *time*
no timing delay-duration *time*

Syntax Description

time	Delay signal duration for delay dial signaling, in milliseconds. Range is from 100to 5000. The default is 2000.

Command Default

2000 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.

Usage Guidelines

The call direction for the **timing delay-duration** command is out. This command is supported on E&M ports only.

Examples

The following example sets the delay signal duration on a voice port to 3000 milliseconds:

```
voice-port 1/0/0
 timing delay-duration 3000
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.

Command	Description
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing delay-start

To specify the minimum delay time from outgoing seizure to out-dial address for a specified voice port, use the **timing delay-start**command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing delay-start *time*
no timing delay-start

Syntax Description

time	Minimum delay time, in milliseconds, from outgoing seizure to outdial address. Range is from 20to 2000. The default on the Cisco 3600 series is 300.

Command Default

Cisco 3600 series: 300 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series routers.

Usage Guidelines

The call direction for the **timing delay-start** command is out. It is supported on E&M ports only.

Examples

The following example sets the delay-start duration on a voice port to 250 milliseconds:

```
voice-port 1/0/0
 timing delay-start 250
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.

Command	Description
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing delay-voice tdm

To specify the delay after which voice packets are played out, use the **timing delay-voice tdm** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing delay-voice tdm *milliseconds*
no timing delay-voice tdm *milliseconds*

Syntax Description

milliseconds	Duration, in milliseconds, of the timing delay. Range is integers from 1 to 1500. Default is 0.

Command Default

milliseconds : 0 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	This command was implemented on the Cisco 2800 series and Cisco 3800 series.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.

Usage Guidelines

The **timing delay-voice tdm** command has an effect on an ear and mouth (E&M) voice port only if the signal type for that port is Land Mobile Radio (LMR). To avoid voice loss at the receiving end of an LMR system, use this command to configure a delay for the voice packet equal to the sum of the durations of all the injected tones and pauses configured with the **inject tone** command and the **inject pause** command.

Examples

The following example configures a timing delay of 470 milliseconds before the voice packet is played out:

```
voice class tone-signal mytones
 inject tone 1 1950 3 150
 inject tone 2 2000 0 60
 inject pause 3 60
 inject tone 4 2175 3 150
 inject tone 5 1000 0 50
voice-port 1/0/0
 voice-class tone-signal mytones
 timing delay-voice tdm 470
```

Note that the delay of 470 milliseconds is equal to the sum of the durations of the injected tones and pauses in the tone-signal voice class.

Related Commands

Command	Description
inject pause	Specifies a pause between injected tones.

Command	Description
inject tone	Specifies a wakeup or frequency selection tone to be played out before the voice packet.

timing delay-with-integrity

To specify the duration of the wink pulse for the delay dial for a specified voice port, use the **timing delay-with-integrity command in**voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing delay-with-integrity *time*
no timing delay-with-integrity

Syntax Description

time	Duration of the wink pulse for the delay dial, in milliseconds. Range is from 0 to 5000. The default is 0.

Command Default

0 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.

Usage Guidelines

This command is supported on E&M ports only.

Examples

The following example sets the duration of the wink pulse for the delay dial to 10 milliseconds:

```
voice-port 1/0/0
 timing delay-with-integrity 10
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.

Command	Description
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing dialout-delay

To specify the dial-out delay for the sending digit on a specified voice port, use the **timing dialout-delay command in**voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing dialout-delay *time*
no timing dialout-delay *time*

Syntax Description

time	Dial-out delay, in milliseconds, for the sending digit or cut-through on a Foreign Exchange Office (FXO) trunk or an E&M immediate trunk. Range is from 100 to 5000. The default is 300.

Command Default

300 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on Cisco MC3810.

Examples

The following example sets the dial-out delay to 350 milliseconds:

```
voice-port 1/0/0
 timing dialout-delay 350
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.

Command	Description
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing dial-pulse min-delay

To specify the time between wink-like pulses for a specified voice port, use the **timing dial-pulse min-delay**command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing dial-pulse min-delay *time*
no timing dial-pulse min-delay

Syntax Description

time	Time between wink-like pulses, in milliseconds. Range is from 0to 5000. The default is 300.

Command Default

300 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.

Usage Guidelines

Use the **timing dial-pulse min-delay** command with PBXs that require a wink-like pulse, even though they have been configured for delay-dial signaling. If the value for this argument is set to 0, the router does not generate this wink-like pulse. The call signal direction for this command is in.

Examples

The following example sets the time between the generation of wink-like pulses on a voice port to 350 milliseconds:

```
voice-port 1/0/0
 timing dial-pulse min-delay 350
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.

Command	Description
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing digit

To specify the dual tone multifrequency (DTMF) digit signal duration for a specified voice port, use the **timing digit**command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing digit *time*
no timing digit

Syntax Description

time	The DTMF digit signal duration, in milliseconds. Range is 5 from 0to 100. The default is 100.

Command Default

100 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.

Usage Guidelines

The call signal direction for the **timing digit** command is out. This command is supported on Foreign Exchange Office (FXO), Foreign Exchange Station (FXS), and E&M ports.

Examples

The following example sets the DTMF digit signal duration on a voice port to 50 milliseconds:

```
voice-port 1/0/0
 timing digit 50
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.

Command	Description
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing guard-out

To specify the guard-out duration of a Foreign Exchange Office (FXO) voice port, use the **timing guard-out command in**voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing guard-out *time*
no timing guard-out

Syntax Description

time	Duration of the guard-out period, in milliseconds. The range is from 300 to 3000. The default is 2000.

Command Default

The default is 2000 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on Cisco MC3810.
12.0(7)XK	This command was implemented on Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

This command is supported on FXO voice ports only.

For Caller ID to work for FXO ports registered to a Cisco Unified CM, the range in milliseconds must be between 1000 to 2000.

Examples

The following example sets the timing guard-out duration on a voice port to 1000 milliseconds:

```
voice-port 1/0/0
 timing guard-out 1000
```

timing hangover

To specify the number of milliseconds of delay before the digital signal processor (DSP) tells Cisco IOS software to turn off the E-lead after the DSP detects that the voice stream has stopped, use the **timing hangover** command in voice-port configuration mode. To return to the default value, use the **no** form of this command.

timing hangover *milliseconds*
no timing hangover *milliseconds*

Syntax Description

milliseconds	The number of milliseconds for which the E-lead stays active after VAD determines that the voice stream has stopped. Valid values are 0 to 10000. The default is 250 milliseconds.

Command Default

milliseconds : 250 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

The **timing hangover**command has an effect on an ear and mouth (E&M) voice port only if the signal type for that port is Land Mobile Radio (LMR). If the voice port has been configured with the **lmr e-lead voice** command, use the **timing hangover** command to adjust the timing if the E-lead is being turned on and off too frequently.

Examples

The following example configures E-lead on voice port 1/0/1 on a Cisco 3745 to stay active for 300 milliseconds after VAD determines that the voice stream has stopped:

```
voice-port 1/0/1
 timing hangover 300
```

timing hookflash-in

To specify the maximum duration of an on-hook condition that will be interpreted as a hookflash by the Cisco IOS software, use the **timing hookflash-in** command in voice-port configuration mode. To restore the default duration for hookflash timing, use the **no** form of this command.

timing hookflash-in *milliseconds*
no timing hookflash-in

Syntax Description

milliseconds	Upper limit of the hookflash duration range, in milliseconds. • E&M voice ports--Range is 0 to 1550 milliseconds. Default is 480 milliseconds. • FXS voice ports--Range is 50 to 1550 milliseconds. Default is 1000 milliseconds.

Command Default

milliseconds : 480 milliseconds for E&M voice ports, 1000 milliseconds for FXS voice ports.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 3600 series.
12.3(7)T	Lower limit of the range for E&M voice ports was extended to 0 milliseconds.
12.3(14)T	This command was implemented on the Cisco 2800 series and Cisco 3800 series.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.

Usage Guidelines

This command is applied to E&M or Foreign Exchange Station (FXS) interfaces.

For Land Mobile Radio E&M voice ports, the **timing hookflash-in** command configures the delay between when the M-lead is raised and when voice is transmitted. Setting the hookflash duration to 0 milliseconds specifies no delay in the audio input and eliminates front-end clipping.

Analog phones connected to FXS ports use hookflash to access a second dial tone to initiate some phone features, such as transfer and conference. Hookflash is an on-hook condition of short duration that is usually generated when a phone user presses the Flash button on a phone. Cisco voice gateways measure the duration of detected on-hook conditions to determine whether they should be interpreted as hookflash or not. The duration for the on-hook conditions generated by Flash buttons on phones varies for different phone types and is interpreted by Cisco IOS software as follows:

- An on-hook condition that lasts for a time period that falls inside the hookflash duration range is considered a hookflash.
- An on-hook condition that lasts for a shorter period than the lower limit of the range is ignored.

- An on-hook condition that lasts for a longer period than the higher limit of the range is considered a disconnect.

The hookflash duration range for FXS voice ports is defined as follows:

- The lower limit of the range is set in software at 150 ms, although there is also a hardware-imposed lower limit that is typically about 20 ms, depending on platform type. An on-hook condition that lasts for a shorter time than this hardware-imposed lower limit is simply not reported to the Cisco IOS software.
- The upper limit of the range is set in software at 1000 ms by default, although this value can be changed using the **timing hookflash-in** command in voice-port configuration mode on the voice gateway. The upper limit can be set to any value from 50 to 1550 ms. For more information, see the explanations in the "Examples" section.

This command does *not* affect whether hookflash relay is enabled; hookflash relay is enabled only when the **dtmf-relay h245-signal** command is configured on the applicable VoIP dial peers. When the **dtmf-relay h245-signal** command is configured, the H.323 gateway relays hookflash by using an H.245 "signal" User Input Indication method. Hookflash is sent only when an H.245 signal is available.

Examples

The following example sets an upper limit of 200 milliseconds for the hookflash duration range:

```
voice-port 1/0/0
 timing hookflash-in 200
```

If the **timing hookflash-in** command is set to X, a value greater than 150, then any on-hook duration between 150 and X is interpreted as a hookflash. For example, if X is 1550, the hookflash duration range is 150 to 1550 ms. An on-hook signal that lasts for 1250 ms is interpreted as a hookflash, but an on-hook signal of 55 ms is ignored.

```
voice-port 1/0/0
 timing hookflash-in 1550
```

If the **timing hookflash-in** command is set to X, a value less than 150, then any on-hook duration between Y, the hardware lower limit, and X is interpreted as a hookflash. For example, if X is 65, the hookflash duration range is Y to 65 ms. An on-hook signal that lasts for 1250 ms is interpreted as a disconnect, but an on-hook signal of 55 ms is interpreted as a hookflash. (This example assumes that Y for the voice gateway is lower than 55 ms.)

```
voice-port 1/0/0
 timing hookflash-in 65
```

Related Commands

Command	Description
dtmf-relay (Voice over IP)	Specifies how an H.323 gateway relays DTMF tones between telephony interfaces and an IP network.

timing hookflash-out

To specify the duration of hookflash indications that the gateway generates on a Foreign Exchange Office (FXO) interface, use the **timing hookflash-out** command in voice-port configuration mode. To restore the default duration for hookflash timing, use the **no** form of this command.

timing hookflash-out *time*
no timing hookflash-out

Syntax Description

time	Duration of the hookflash, in milliseconds. Range is from 50 to 1550. The default is 400 milliseconds.

Command Default

400 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on Cisco 2500, Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(4)T	Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on Cisco AS5850.

Usage Guidelines

This command does not affect whether hookflash relay is enabled; hookflash relay is enabled only when the **dtmf-relay h245-signal** command is configured on the applicable VoIP dial peers. Hookflash is relayed by using an H.245-signal indication and can be sent only when an H.245 signal is available.

Use the **timing hookflash-out**command on FXO interfaces to specify the duration (in milliseconds) of a hookflash indication. To set hookflash timing parameters for analog voice interfaces, use the **timing** command.

Examples

The following example implements timing for the hookflash with a duration of 200 milliseconds.

```
voice-port 1/0/0 timing hookflash-out 200
```

Related Commands

Command	Description
dtmf-relay (Voice over IP)	Specifies how an H.323 gateway relays DTMF tones between telephony interfaces and an IP network.
voice-port	Enters voice-port configuration mode.

timing ignore m-lead

To ignore M-lead or voice activity detection (VAD) changes for a specified amount of time after sending the E-lead off signal, use the **timing ignore m-lead** command in voice-port configuration mode. To return to the default value, use the **no** form of this command.

timing ignore m-lead *milliseconds*
no timing ignore m-lead *milliseconds*

Syntax Description

milliseconds	The number of milliseconds following the sending of the E-lead off signal for which the M-lead and VAD changes are ignored. Valid values are 0 to 10000. The default is 0 milliseconds.

Command Default

milliseconds : 0 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

- The **timing ignore m-lead** command has an effect on an ear and mouth (E&M) voice port only if the signal type for that port is Land Mobile Radio (LMR). Use this command to reduce echo feedback on an LMR voice port. This command has an effect only if the voice port is configured for half duplex mode.

Examples

The following example configures voice port 1/0/1 on a Cisco 3745 to ignore M-lead or VAD changes for 500 milliseconds after sending the E-lead off signal:

```
voice-port 1/0/1
 timing ignore m-lead 500
```

timing interdigit

To specify the dual-tone multifrequency (DTMF) interdigit duration for a specified voice port, use the **timing interdigit**command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing interdigit *time*
no timing interdigit *time*

Syntax Description

time	DTMF interdigit duration, in milliseconds. Range is from 50to 500. The default is 100.

Command Default

100 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.
11.3(1)MA	This command was supported on Cisco MC3810.

Usage Guidelines

The call signal direction for the **timing interdigit** command is out. This command is supported on Foreign Exchange Office (FXO), Foreign Exchange Station (FXS), and E&M ports.

Examples

The following example sets the DTMF interdigit duration on a voice port to 150 milliseconds:

```
voice-port 1/0/0
 timing interdigit 150
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.

Command	Description
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing opx-ringwait

To set the maximum wait time for detecting the next ring on FXO ports, use the **timing opx-ringwait**command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing opx-ringwait *msecs*
no timing opx-ringwait

Syntax Description

msecs	Maximum duration, in milliseconds, to wait for the next ring. Range is 2000 to 10000. Default is 6000.

Command Default

Timeout for detecting ring tones is 6000 ms (6 sec).

Command Modes

Voice-port configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

This command prevents the voice gateway from prematurely disconnecting private line automatic ring-down (PLAR) off-premises extension (OPX) calls when the duration between ring tones from the switch is more than 6 sec. The absence of a ring tone from the switch indicates that the originating party has disconnected the call. Because some analog switches take longer than 6 sec to generate the ring tone, the voice gateway could clear the call leg while it is still ringing for a PLAR OPX call, unless the 6-sec default is changed with this command.

Examples

The following example sets the timeout for the next ring to 8 sec:

```
voice-port 2/0/10
 timing opx-ringwait 8000
```

Related Commands

Command	Description
voice-port	Enters voice-port configuration mode.
show voice port	Displays configuration information about a specific voice port.

timing percentbreak

To specify the percentage of the break period for dialing pulses for a voice port, use the **timing percentbreak command in**voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing percentbreak *percent*
no timing percentbreak

Syntax Description

percent	Percentage of the break period for dialing pulses. Range is from 20 to 80. The default is 50.

Command Default

50 percent

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA4	This command was introduced on Cisco MC3810.
12.0(7)XK	This command was implemented on Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

The **timing percentbreak**command is supported on Foreign Exchange Office (FXO) and E&M voice ports only.

Examples

The following example sets the break period percentage on a voice port to 30 percent:

```
voice-port 0/0/1
 timing percentbreak 30
```

Related Commands

Command	Description
timing pulse	Configures the pulse dialing rate for a voice port.
timing pulse -interdigit	Configures the pulse interdigit timing for a voice port.

timing pulse

To specify the pulse dialing rate for a specified voice port, use the **timing pulse**command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing pulse *pulses-per-second*
no timing pulse *pulses-per-second*

Syntax Description

pulses -per-second	Pulse dialing rate, in pulses per second. Range is from 10to 20. The default is 20.

Command Default

20 pulses per seconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA	This command was supported on the Cisco MC3810.

Usage Guidelines

The call signal direction for the **timing pulse** command is out. This command is supported on Foreign Exchange Office (FXO) and E&M ports only.

Examples

The following example sets the pulse dialing rate on a voice port to 15 pulses per second:

```
voice-port 1/0/0
 timing pulse 15
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.

Command	Description
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing pulse-interdigit

To specify the pulse interdigit timing for a specified voice port, use the **timing pulse-interdigit**command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing pulse-interdigit *time*
no timing pulse-interdigit *time*

Syntax Description

time	Pulse dialing interdigit timing, in milliseconds. Range is from 100to 1000. The default is 500.

Command Default

500 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.
11.3(1)MA	This command was supported on Cisco MC3810.

Usage Guidelines

The call signal direction for the **timing pulse-interdigit** command is out. This command is supported on Foreign Exchange Office (FXO) and E&M ports only.

Examples

The following example sets the pulse-dialing interdigit timing on a voice port to 300 milliseconds:

```
voice-port 1/0/0
 timing pulse-interdigit 300
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.

Command	Description
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing sup-disconnect

To define the minimum time to ensure that an on-hook indication is intentional and not an electrical transient on the line before a supervisory disconnect occurs (based on power denial signaled by the PSTN or PBX), use the **timing sup-disconnect** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

timing sup-disconnect *milliseconds*
no timing sup-disconnect *milliseconds*

Syntax Description

milliseconds	Minimum time, in milliseconds, after detection of an on-hook indication to determine that the on-hook condition is intentional and then to hang up the POTS call leg. The range is from 50 to 1500. The default is 350.

Command Default

The default minimum time is 350 milliseconds before a supervisory disconnect occurs.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(12)	This command was introduced.
12.3(11)T6	This command was integrated into Cisco IOS Release 12.3(11)T6.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.4(12)	This command was integrated into Cisco IOS Release 12.4(12).

Usage Guidelines

Prior to the implementation of the **timing sup-disconnect** command, analog Foreign Exchange Office (FXO) ports could not detect short disconnect signals lasting fewer than 350 ms in duration. Using this command, you can specify a wait period from 50 to 1500 ms to ensure that when an on-hook indication persists for a time that is longer than the configured value, the on-hook condition is considered intentional and a hang-up is signaled on the POTS call leg.

This timer affects only analog loop-start FXO voice ports.

Even though the **timing sup-disconnect** command can be entered under the voice port in FXO ground-start signaling, the changes in the timer setting take effect only in FXO loop-start signaling.

Examples

The following example sets the timer to wait 500 ms after detecting an on-hook signal before a supervisory disconnect occurs on the POTS call leg:

```
voice-port 1/0/0
 timing sup-disconnect 500
```

Related Commands

Command	Description
show voice port	Displays configuration information about a specific voice port.

Command	Description
voice-port	Enters voice-port configuration mode.

timing wait-wink

To set the maximum time to wait for wink signal after an outgoing seizure is sent, use the **timing wait-wink**command in voice port configuration mode. To restore the default value, use the **no** form of this command.

timing wait-wink *milliseconds*
no timing wait-wink *milliseconds*

Syntax Description

milliseconds	Maximum time to wait for wink signal after an outgoing seizure is sent. Valid entries are from 100to 6500 milliseconds (ms). Supported on ear and mouth (E&M) ports only.

Command Default

milliseconds : 550 milliseconds

Command Modes

Voice port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series routers.
11.3(1)MA	This command was implemented on Cisco MC3810 multiservice concentrators.
12.4(12)	The millisecond range was extended from 5000 to 6500.

Examples

The following example configures the maximum time to wait for wink signaling after an outgoing seizure is sent on a voice port for 300 milliseconds:

```
voice-port 1/0/0
 timing wait-wink 300
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.

Command	Description
timing dialout-delay	Specifies the dial-out delay for the sending digit on a specified voice port.
timing delay-with-integrity	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing wink-duration

To specify the timing for transmit and receive wink-signal duration for a voice port, use the **timing wink-duration**command in voice-port configuration mode. To reset to the default values, use the **no** form of this command.

timing wink-duration {*time* | **receive** *minimum maximum*}
no timing wink-duration

Syntax Description

time	Maximum transmit duration, in milliseconds (ms), for a wink-start signal. The range is from 50to 3000. The default is 200.
receive	Indicates that a range is to be specified for a received wink-start signal.
minimum	Received minimum wink length, in milliseconds. The range is from 40 to 2950. The default is 140.
maximum	Received maximum wink length, in milliseconds. The range is from 150 to 3150. The default is 290.

Command Default

Transmit wink-duration timing is set to 200 ms. The received wink-duration timing minimum is set to 140 ms and the maximum is set to 290 ms.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.
11.3(1)MA	This command was integrated into Cisco IOS Release 11.3(1)MA and support was added for the Cisco MC3810.
12.4(13)	This command was integrated into Cisco IOS Release 12.4(13) and the **receive** keyword and *minimum* and *maximum* arguments were added.

Usage Guidelines

The call signal direction for the **timing wink-duration** command is out. This command is supported on ear and mouth (E&M) ports only.

When wink-start signaling is used, the originating side seizes the line by going off-hook and then waits for an acknowledgment from the other end before initiating a call. The acknowledgment is a reversal of polarity (off-hook) for a timing period referred to as a wink. A wink should occur no earlier than 100 ms after the receipt of the incoming seizure signal. In addition to the signaling function, the wink start serves as an integrity check that identifies a malfunctioning trunk and allows the network to send a reorder tone to the calling party.

When you set the receive range, the minimum and maximum values of acceptable wink must provide an acceptable range of at least 50 ms. For example, entering the command **timing wink-duration receive 160 200** results in an error message.

Examples

The following example shows how to set the transmit wink-signal duration on voice port 1/0/0 to 300 ms:

```
voice-port 1/0/0
 timing wink-duration 300
```

The following example shows how to set the range for the receive wink-signal duration on voice port 1/0/0 to 160 to 210 ms:

```
voice-port 1/0/0
 timing wink-duration receive 160 210
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.
timing delay-with-integrity	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-wait	Specifies the maximum wink-wait duration for a specified voice port.

timing wink-wait

To specify the maximum wink-wait duration for a specified voice port, use the **timing wink-wait**command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

timing wink-wait *time*
no timing wink-wait

Syntax Description

time	Maximum wink-wait duration, in milliseconds, for a wink start signal. Range is from 100to 6500. The default is 200.

Command Default

200 milliseconds

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.
11.3(1)MA	This command was supported on Cisco MC3810.
12.4(12)	The millisecond range was extended from 5000 to 6500.

Usage Guidelines

The call signal direction for the **timing wink-wait** command is out. This command is supported on ear and mouth (E&M) ports only.

Examples

The following example sets the wink-wait duration on a voice port to 300 milliseconds:

```
voice-port 1/0/0
 timing wink-wait 300
```

Related Commands

Command	Description
timeouts initial	Configures the initial digit timeout value for a specified voice port.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
timeouts wait-release	Configures the timeout value for releasing voice ports.
timing clear-wait	Indicates the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port.
timing delay-duration	Specifies the delay signal duration for a specified voice port.
timing delay-start	Specifies the minimum delay time from outgoing seizure to out-dial address for a specified voice port.

Command	Description
timing delay-with-integrity	Specifies the duration of the wink pulse for the delay dial for a specified voice port.
timing dialout-delay	Specifies the dialout delay for the sending digit on a specified voice port.
timing dial-pulse min-delay	Specifies the time between wink-like pulses for a specified voice port.
timing digit	Specifies the DTMF digit signal duration for a specified voice port.
timing interdigit	Specifies the DTMF interdigit duration for a specified voice port.
timing percentbreak	Specifies the percentage of a break period for a dialing pulse for a specified voice port.
timing pulse	Specifies the pulse dialing rate for a specified voice port.
timing pulse-interdigit	Specifies the pulse interdigit timing for a specified voice port.
timing wink-duration	Specifies the maximum wink signal duration for a specified voice port.

tls

To enable Transport Layer Security (TLS) for the Skinny Client Control Protocol (SCCP) connection between the SCCP server and the SCCP client, use the **tls**command in DSP farm profile configuration mode. To disable secure SCCP signaling, use the **no** form of this command.

tls
no tls

Syntax Description

This command has no arguments or keywords.

Command Default

Secure SCCP signaling exchange is enabled by default.

Command Modes

DSP farm profile configuration (config-dspfarm-profile #)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **tls**command to enable secure SCCP signaling exchange. The configuration can be modified only when the dspfarm profile is shut down. To shut down the dsp farm profile, configure the **no shutdown** command.

Examples

The following example shows how to configure the **tls**command to enable TLS support for digital signal processor (DSP) farm services profile 1:

```
Router(config)# dspfarm profile 1 transcode security
Router(config-dspfarm-profile)# tls
```

Related Commands

Command	Description
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.

toggle-between-two-calls

To define a Feature Access Code (FAC) to access the Toggle Between Two Calls feature in feature mode on analog phones connected to FXS ports, use the **toggle-between-two-calls** command in STC application feature-mode call-control configuration mode. To return the code to its default, use the **no** form of this command.

toggle-between-two-calls *keypad-character*
no toggle-between-two-calls

Syntax Description

keypad-character	Character string of one to four characters that can be dialed on a telephone keypad (0-9, *, #). Default is #5.

Command Default

The default value is #5.

Command Modes

STC application feature-mode call-control configuration (config-stcapp-fmcode)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

This command changes the value of the FAC for Toggle Between Two Calls from the default (#5) to the specified value.

If you attempt to configure this command with a value that is already configured for another FAC in feature mode, you receive a message. This message will not prevent you from configuring the feature code. If you configure a duplicate FAC, the system implements the first feature it matches in the order of precedence as determined by the value for each FAC (#1 to #5).

If you attempt to configure this command with a value that precludes or is precluded by another FAC in feature mode, you receive a message. If you configure a FAC to a value that precludes or is precluded by another FAC in feature mode, the system always executes the call feature with the shortest code and ignores the longer code. For example, 1 will always preclude 12 and 123. These messages will not prevent you from configuring the feature code. You must configure a new value for the precluded code in order to enable phone user access to that feature.

Examples

The following example shows how to change the value of the feature code for the Toggle Between Two Calls feature from the default (#5). With this configuration, a phone user in basic call mode presses hook flash to get the first dial tone, then dials an extension number to connect to a second call. During the second call, the user presses a hook flash to get a feature tone and then dials 55 to toggle back to the previous call party.

```
Router(config)# stcapp call-control mode feature
Router(config-stcapp-fmcode)# toggle-between-two-calls 55
Router(config-stcapp-fmcode)# exit
```

Related Commands

Command	Description
conference	Defines FAC in Feature Mode to initiate a three-party conference.
drop-last-conferee	Defines FAC in feature mode to use to drop last active call during a three-party conference.
hangup-last-active-call	Defines FAC in feature mode to drop last active call during a three-party conferencee.
transfer	Defines FAC in feature mode to connect a call to a third party that the phone user dials.

token-root-name

To specify which root or Certificate Authority (CA) certificate the router uses to validate the settlement token in the incoming setup message, use the **token-root-name**command in settlement configurationmode. To reset to the default, use the **no** form of this command.

token-root-name *name*
no token-root-name

Syntax Description

name	Certificate identification name as configured with the **crypto ca identity** *name* command or the **crypto ca trusted-root** *name* command.

Command Default

The terminating gateway uses the CA certificate to validate the settlement token.

Command Modes

Settlement configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on Cisco 2600 series, Cisco 3600 series, Cisco AS5300, and Cisco AS5800.

Examples

The following example defines the **token-root-name** as "sample":

```
token-root-name sample
```

The following example shows new output for the **show settlement** command to display the value of the **token-root-name** command:

```
Settlement Provider 0
        Operation Status = UP
        Type = osp
        Address url = https://1.14.115.100:8444/
        Encryption = all                (default)
        Token Root Name = sample
        Max Concurrent Connections = 20 (default)
        Connection Timeout = 3600 (s)   (default)
        Response Timeout = 1 (s)        (default)
        Retry Delay = 2 (s)             (default)
        Retry Limit = 1                 (default)
        Session Timeout = 86400 (s)     (default)
        Customer Id = 1000
        Device Id = 2000
        Roaming = Disabled              (default)
        Signed Token = On
        Number of Connections = 1
        Number of Transactions = 0
```

Related Commands

Command	Description
crypto ca identity	Declares the Certificate Authority that your router should use.

Command	Description
crypto ca trusted -root	Configures the root certificate that the server uses to sign the settlement tokens.
show settlement	Displays the configuration for all settlement server transactions.

tone busytone

To enable automatic busytone generation in a basic call scenario, use the **tone busytone**command in dial peer voice configuration mode. To disable automatic busytone generation, use the **no** form of this command.

tone busytone remote-onhook
no tone busytone remote-onhook

Syntax Description

remote-onhook	Generates busy tone after remote onhook in basic call mode.

Command Default

Automatic busytone generation after remote disconnect is disabled.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The automatic busytone generation after remote disconnect in basic call mode feature is enabled and disabled per dial peer with the **tone busytone remote-onhook**command. The **tone busytone**command is available to all dial peer services. Each service determines whether to utilize or enable it. For STCAPP, only the Foreign eXchange Subscriber (FXS) loop-start port will enable this service.



Note The **tone busytone** command cannot coexist with thedialtone generation after remote-onhook feature. Because the **tone dialtone**is a default configuration, you must disable the feature using the **no tone dialtone**command before connfiguring the **tone busytone**command.

Use the **show dial-peer voice** command or the **show stcapp device voice** command to verify the feature is enabled.

Examples

The following example shows busytone generation after remote disconnect being configured:

```
Router(config-dial-peer)# tone busytone remote-onhook
```

Related Commands

Command	Description
show dial-peer voice	Displays information for voice dial peers.
tone dialtone	Enable automatic dial tone generation.
show stcapp device voice	Displays configuration information about STCAPP analog voice ports.

tone dialtone

To enable automatic dial-tone generation in basic call mode, use the **tone dialtone**command in dial peer configuration mode. To disable automatic dial-tone generation, use the **no** form of this command.

tone dialtone remote-onhook
no tone dialtone remote-onhook

Syntax Description

remote-onhook	Generates dial tone after remote onhook in basic call mode.

Command Default

Automatic dial-tone generation after remote disconnect is enabled.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(6)XE	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

Use this command to generate immediate dial tone once a remote party disconnects, similar to what the user experiences in a PBX environment. If you disable this feature using the **no** form of this command, the user is required to go on hook or perform a hookflash to generate dial tone after the remote party disconnects in a basic two-part call scenario. This feature is supported on Skinny Client Control Protocol (SCCP) gateway controlled loop-start FXS ports only.

Examples

The following examples show that the automatic Dial Tone Generation After Remote Onhook feature is enabled. Because the dial tone generation after remote onhook feature is enabled by default, it does not display in the show running-config output.

```
Router# show running-config
service stcapp
 dial-peer voice 3001 pots
 port 1/1/1

Router# show dial-peer voice 3001
VoiceEncapPeer3001
 peer type = voice, system default peer = FALSE, information type = voice,
!
!
!
 in bound application associated: 'stcapp'
 dial tone generation after remote-onhook = enabled

Router# show stcapp device voice-port 1/1/1
Port Identifier:  1/1/1
!
Dialtone after remote-onhook feature: activated
```

The following examples show the dial tone generation after remote onhook feature disabled.

```
Router# show running-config
no tone dialtone remote-onhook
dial-peer voice 3002 pots
 service stcapp
 port 1/1/0
```

Related Commands

Command	Description
sccp	Enables SCCP and related applications.
show dial-peer voice	Displays information for voice dial peers.
show stcapp device	Displays configuration information about SCCP Telephony Control Application (STCAPP) analog voice ports.

tone incoming

To activate 2100-Hz answer (ANS) tone detection on either the IP or the PSTN side of the network and to disable the echo suppressor, use the **tone incoming**command in voice-service VoIP configuration mode or VoIP dial-peer configuration mode. To deactivate tone detection and disable the echo suppressor, use the **no** form of this command.

tone incoming [**ip** | **pstn**] {**ans-all auto-control** | **ans disable echo suppressor** | **anspr disable echo suppressor**}
no tone incoming

Syntax Description

ip	(Optional) Specifies tone detection on the IP side of the network.
pstn	(Optional) Specifies tone detection on the PSTN side of the network.
ans auto-control	Detects ANS tone and enables standard actions for modem tones.
ans-all disable echo suppressor	Detects modem answer tones and disables echo suppressor.
anspr disable echo suppressor	Detects /ANS tone and disables echo suppressor.

Command Default

Tone incoming detection is not enabled.

Command Modes

Voice-service VoIP configuration
VoIP dial-peer configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use this command in voice-service VoIP or VoIP dial-peer configuration mode to activate detection of all ANS, ANSam, and ANSpr tones and enable or disable echo canceller control. When this command is issued in voice-service VoIP configuration mode*, all dial peers are globally configured unless a specific dial peer is configured for no tone incoming.*

To deactivate all 2100-Hz ANS, ANSam, and ANSpr tone detection on either the IP or the PSTN side of the network, and enable the echo canceller, use the **no tone incoming** command in voice-service VoIP configuration or VoIP dial-peer configuration mode.

If neither IP nor PSTN is specified, all ANS, ANSam, and ANSpr tones are detected on both sides of the network, and the echo suppressor is disabled in all cases.

The **tone incoming ip ans-all auto-control** command is equivalent to these two commands together:

- **tone incoming ip ans disable echo suppressor**
- **tone incoming ip anspr disable echo suppressor**

The **tone incoming pstn ans-all auto-control** command is equivalent to these two commands together:

- **tone incoming pstn ans disable echo suppressor**

- **tone incoming pstn anspr disable echo suppressor**

The **tone incoming ans-all auto-control** command is equivalent to these four commands together:

- **tone incoming ip ans disable echo suppressor**
- **tone incoming ip anspr disable echo suppressor**
- **tone incoming pstn ans disable echo suppressor**
- **tone incoming pstn anspr disable echo suppressor**

When modem tones from either the IP or PSTN direction are received, the echo canceller can be dynamically disabled to allow modem calls to pass through.

The IP tone detector feature applies only on the following NextPort platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850--and only with SIP and H.323 voice signaling. It does not apply to MGCP in VoIP dial-peer configuration mode.

The gateway must be configured for G.711 codecs for the IP tone detector feature to work (see the "Examples" section).

To display the status of the echo canceller, use the **show port operational status** command.

Examples

The following example configures tone detection of ANS tones in voice-service VoIP configuration mode:

```
Router(conf-voi-serv)# tone incoming ip ans disable echo supressor
```

The following example configures tone detection of all incoming ANS, ANSam, and ANSpr tones on a dial peer:

```
Router(config-dial-peer)# tone incoming ip ans-all auto-control
```

Related Commands

Command	Description
tone incoming system	Sets a dial peer for tone incoming or no tone incoming detection.
show port operational status	Displays the status of the echo canceller.

tone incoming system

To set a dial peer for tone incoming or no tone incoming, use the **tone incoming system** command in VoIP dial-peer configuration mode. To block the voice service VoIP settings for a dial peer, use the **no** form of this command.

tone incoming system
no tone incoming system

Syntax Description

This command has no arguments or keywords.

Command Default

The dial peer is set for tone incoming.

Command Modes

VoIP dial-peer configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use this command in VoIP dial-peer configuration mode to activate or deactivate tone detection and to enable echo canceller control. When modem tones from either the IP or PSTN directions are received. The echo canceller can be dynamically disabled to allow modem calls through. This command is used primarily to allow or to block global voice service VoIP configuration settings.

To block the voice service VoIP settings for a dial peer, use the **no tone incoming system** command.

Examples

The following example shows activating tone detection for a dial peer.

```
Router(config-dial-peer)# tone incoming system
```

The following example shows deactivating tone detection for a dial peer.

```
Router(config-dial-peer)# no tone incoming system
```

Related Commands

Command	Description
tone incoming ans disable echo suppressor	Activates ANS tone detection.
tone incoming anspr disable echo canceller	Activates ANSpr tone detection.
tone incoming ans-all auto-control	Activates ANS, ANSam, and ANSpr tone detection.
show port operational status	Displays the status of the echo canceller.

tone ringback alert-no-PI

To generate automatic ringback for the caller when no Progress Indicator (PI) alert has been received over the H.323 network, use the **tone ringback alert-no-PI**command in dial-peer configurationmode. To disable automatic ringback, use the **no** form of this command.

tone ringback alert-no-PI
no tone ringback alert-no-PI

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, Cisco AS5300, and Cisco AS5800.

Usage Guidelines

Use this command to generate ringback in an H.323 network when the attached device (for example, an ISDN device) cannot.

Examples

The following example activates ringback for a VoIP dial peer numbered 322:

```
Router(config)# dial-peer voice 322 voip
Router(config-dial-peer)# tone ringback alert-no-PI
```

Related Commands

Command	Description
progress_ind	Sets a specific PI in call Setup, Progress, or Connect messages from an H.323 VoIP gateway.

trace (voice service voip)

To configure the VoIP Trace framework in CUBE, use the **trace** command in voice service voip configuration mode. To disable VoIP tracing, use the **no** form of this command.

[no] trace

Command Default

Trace is enabled by default.

Command Modes

Voice Service VoIP configuration mode (conf-voi-serv)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2 Cisco IOS XE Bengaluru 17.4.1a	This command was introduced on Cisco Unified Border Element.

Usage Guidelines

Use the **trace** command to configure the VoIP Trace framework to persistently monitor and troubleshoot SIP calls on CUBE. With **trace** enabled, event logging and debugging of VoIP parameters such as SIP messages, FSM, and Unified Communication flows processed by CUBE are logged.

VoIP tracing is disabled using the command **shutdown** under the **trace** configuration mode. To re-enable VoIP Trace, configure **[no] shutdown** . The **shutdown** command retains the custom **memory-limit** whereas **[no] trace** resets the **memory-limit** to default.

To define a custom limit for the memory allotted for storage of VoIP Trace information in CUBE, configure **memory-limit** *memory* under trace configuration mode. Range is 10–1000 MB. If **memory-limit** isn't configured, the default configuration of **memory-limit platform** is applied. By default, 10% of the total memory available to the IOS processor at the time of configuring the command will be reserved for VoIP Trace data storage.

Examples

The following is a sample configuration for enabling **trace** on Unified Border Element:

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#voice service voip
router(conf-voi-serv)#?
VOICE SERVICE configuration commands:
address-hiding Address hiding (SIP-SIP)
allow-connections Allow call connection types
call-quality Global call quality of service setup
callmonitor Call Monitoring
cause-code Sets the internal cause code for SIP and H323
clid Caller ID option
cpa Enable Call Progress Analysis for voip calls
default Set a command to its defaults
dtmf-interworking Dtmf Interworking
emergency List of Emergency Numbers
exit Exit from voice service configuration mode
fax Global fax commands
fax-relay Global fax relay commands
gcid Enable Global Call Identifcation for voip
h323 Global H.323 configuration commands
ip Voice service voip ip setup
lpcor Voice service voip lpcor setup
```

```
media Global media setting for voip calls
media-address Voice Media IP Address Range
mode Global mode setting for voip calls
modem Global modem commands
no Negate a command or set its defaults
notify send facility indication to application
qsig QSIG
redirect voip call redirect
redundancy-group Associate redundancy-group with voice HA
redundancy-reload Reload control when RG fail
rtcp Configure RTCP report generation
rtp-media-loop Global setting for rtp media loop count
rtp-port Global setting for rtp port range
shutdown Stop VoIP services gracefully without dropping active calls
signaling Global setting for signaling payload handling
sip SIP configuration commands
srtp Allow Secure calls
stun STUN configuration commands
supplementary-service Config supplementary service features
trace Voip Trace configuration
voice enable voice parameters
vpn-group Enter vpn-group mode
vpn-profile Enter vpn-profile mode

router(conf-voi-serv)# trace
```

Related Commands

Command	Description
memory-limit (trace)	Defines the memory limit for storing VoIP Trace information.
shutdown (trace)	Disable the VoIP Trace serviceability framework in CUBE.
show voip trace	Displays the VoIP Trace information for SIP legs on a call received on CUBE

transfer

To define a Feature Access Code (FAC) to access the Call Transfer feature in feature mode on analog phones connected to FXS ports, use the **transfer** command in STC application feature-mode call-control configuration mode. To return the code to its default, use the **no** form of this command.

transfer *keypad-character*
no transfer

Syntax Description

keypad-character	Character string of one to four characters that can be dialed on a telephone keypad (0-9, *, #). Default is #2.

Command Default

The default value is #2.

Command Modes

STC application feature-mode call-control configuration (config-stcapp-fmcode)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

This command changes the value of the FAC for Call Transfer from the default (#2) to the specified value.

If you attempt to configure this command with a value that is already configured for another FAC in feature mode, you receive a message. This message will not prevent you from configuring the feature code. If you configure a duplicate FAC, the system implements the first feature it matches in the order of precedence as determined by the value for each FAC (#1 to #5).

If you attempt to configure this command with a value that precludes or is precluded by another FAC in feature mode, you receive a message. If you configure a FAC to a value that precludes or is precluded by another FAC in feature mode, the system always executes the call feature with the shortest code and ignores the longer code. For example, 1 will always preclude 12 and 123. These messages will not prevent you from configuring the feature code. You must configure a new value for the precluded code in order to enable phone user access to that feature.

Examples

The following example shows how to change the value of the feature code for the Call Transfer feature from the default (#2). With this configuration, a phone user presses hook flash to get the first dial tone, then dials an extension number to connect to a second call. When the second call is established, the user presses hook flash to get a feature tone and then dials 22 to transfer the call; the user hears silence after the call is transferred.

```
Router(config)# stcapp call-control mode feature
Router(config-stcapp-fmcode)# transfer 22
Router(config-stcapp-fmcode)# exit
```

Related Commands

Command	Description
conference	Defines FAC in Feature Mode to initiate a three-party conference.

Command	Description
drop-last-conferee	Defines FAC in feature mode to use to drop last active call during a three-party conference.
hangup-last-active-call	Defines FAC in feature mode to drop last active call during a three-party conferencee.
toggle-between-two-calls	Defines FAC in feature mode to toggle between two active calls.

translate

To apply a translation rule to manipulate dialed digits on an inbound POTS call leg, use the **translate** command in voice-port configuration mode. To remove the translation rule, use the **no** form of this command.

translate {**calling-number** | **called-number**} *name-tag*
no translate {**calling-number** | **called-number**} *name-tag*

Syntax Description

calling -number	Translation rule applies to the inbound calling party number.
called -number	Translation rule applies to the inbound called party number.
name -tag	Tag number by which the rule set is referenced. This is an arbitrarily chosen number. Range is from 1 to 2147483647. There is no default value.

Command Default

No default behavior or values

Command Modes

Voice-port configuration

Command History

Release	Modification
12.0(7)XR1	This command was introduced for VoIP on Cisco AS5300.
12.0(7)XK	This command was implemented for VoIP on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T and implemented for VoIP Cisco AS5300, Cisco 7200, and Cisco 7500.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

A translation rule is a general-purpose digit-manipulation mechanism that performs operations such as automatically adding telephone area and prefix codes to dialed numbers.

Examples

The following example applies translation rule 21 to the POTS inbound calling-party number:

```
translation-rule 21
 rule 1 555.% 1408555 subscriber international
 rule 2 7.% 1408555 abbreviated international
voice-port 0:1
 translate calling-number 21
```

The following example applies translation rule 20 to the POTS inbound called-party number:

```
translation-rule 20
 rule 1 .%555.% 7 any abbreviated
voice-port 0:1
 translate called-number 20
```

Related Commands

Command	Description
numbering-type	Specifies number type for the VoIP or POTS dial peer.
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
show translation-rule	Displays the contents of all the rules that have been configured for a specific translation name.
translate-outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls.
translation-rule	Creates a translation name and enters translation-rule configuration mode.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

translate (translation profiles)

To associate a translation rule with a voice translation profile, use the **translate** command in voice translation-profile configuration mode. To delete the translation rule from the profile, use the **no** form of this command.

translate {**called** | **calling** | **redirect-called** | **redirect-target**} *translation-rule-number*
no translate {**called** | **calling** | **redirect-called** | **redirect-target**} *translation-rule-number*

Syntax Description

called	Associates the translation rule with called numbers.
calling	Associates the translation rule with calling numbers.
redirect -called	Associates the translation rule with redirected called numbers.
redirect-target	Associates the translation rule with transfer-to numbers and call-forwarding final destination numbers.
translation -rule-number	Number of the translation rule to use for the call translation. Valid range is from 1 to 2147483647. There is no default value.

Command Default

No translation rule is associated with the translation profile.

Command Modes

Voice translation-profile configuration (cfg-translation-profile)

Command History

Release	Modification
12.0(7)XR1	This command was introduced on the Cisco AS5300.
12.0(7)XK	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T and implemented on the following platforms: Cisco 1750, Cisco AS5300, Cisco 7200 series, and Cisco 7500 series.
12.1(2)T	This command was implemented on the Cisco MC3810.
12.2(11)T	This command was reconfigured for voice translation-profile configuration mode. The **redirect-called**keyword and *translation-rule-number*argument were added.
12.4(11)XJ	The **redirect-target** keyword was added.
12.4(15)T	The **redirect-target** keyword was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

Use this command as part of a voice translation-profile definition. Enter this command for each translation rule that is part of the profile definition.

Examples

The following example defines voice translation profile "sjmorning" with two translation rules: translation rule 15 for called numbers and translation rule 36 for calling numbers.

```
Router(config)# voice translation-profile sjmorning
Router(cfg-translation-profile)# translate called 15
Router(cfg-translation-profile)# translate calling 36
```

Related Commands

Command	Description
rule (voice translation-rule)	Sets the criteria for the translation-rule.
show voice translation-profile	Displays the configuration of the translation-profile.
translation-profile (dial-peer)	Assigns a translation profile to a dial peer.
translation-profile (source group)	Assigns a translation profile to a source IP group.
translation-profile (trunk group)	Assigns a translation profile to a trunk group.
translation-profile (voice port)	Assigns a translation profile to a voice port.
translation-profile (voice service POTS)	Assigns a translation profile to an NFAS interface.
voice translation-profile	Initiates the translation-profile definition.
voice translation-rule	Initiates the translation-rule definition.

translate-outgoing

To apply a translation rule to manipulate dialed digits on an outbound POTS or VoIP call leg, use the **translate-outgoing command in**dial-peer configuration mode. To disable the translation rule, use the **no** form of this command.

translate-outgoing {**calling-number** | **called-number**} *name-tag*
no translate-outgoing {**calling-number** | **called-number**} *name-tag*

Syntax Description

calling -number	Apply to the outbound calling party number.
called -number	Apply to the outbound called party number.
name -tag	Tag number by which the rule set is referenced. This is an arbitrarily chosen number. Range is 1 to 2147483647. There is no default value.

Command Default

No default behavior or values

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.0(7)XR1	This command was introduced for VoIP on Cisco AS5300.
12.0(7)XK	This command was implemented for VoIP on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(1)T	This command was integrated into Cisco IOS Release 12.2(1)T and implemented for VoIP on the Cisco 1750, Cisco AS5300, Cisco 7200, and Cisco 7500. support for the Cisco MC3810 is not included in this release.
12.1(2)T	This command is supported on the Cisco MC3810 in this release.

Examples

The following example applies translation rule 21 to the VoIP outbound calling number:

```
translation-rule 21
 rule 1 555.% 1408555 subscriber international
 rule 2 7.% 1408555 abbreviated international
 dial-peer voice 100 voip
 translate-outgoing calling-number 21
```

The following example applies translation rule 20 to the VoIP called number:

```
translation-rule 20
 rule 1 .%555.% 7 any abbreviated
dial-peer voice 100 voip
 translate-outgoing called-number 20
```

Related Commands

Command	Description
numbering-type	Specifies number type for the VoIP or POTS dial peer.
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
show translation-rule	Displays the contents of all the rules that have been configured for a specific translation name.
translate	Applies a translation rule to a calling party number or a called party number for incoming calls.
translation-rule	Creates a translation name and enters translation-rule configuration mode.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

translation-profile (dial peer)

To assign a translation profile to a dial peer, use the **translation-profile** command in dial peer configuration mode. To delete the translation profile from the dial peer, use the **no** form of this command.

translation-profile {**incoming** | **outgoing**} *name*
no translation-profile {**incoming** | **outgoing**} *name*

Syntax Description

incoming	Specifies that this translation profile handles incoming calls.
outgoing	Specifies that this translation profile handles outgoing calls.
name	Name of the translation profile.

Command Default

No default behavior or values

Command Modes

Dial peer configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.4(22)T	Support for IPv6 was added.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

Use the **translation-profile** command to assign a predefined translation profile to a dial peer.

Examples

The following example assigns the translation profile named "profile1" to handle translation of outgoing calls for a dial peer:

```
Router(config)# dial-peer voice 111 pots
Router(config-dial-peer)# translation-profile outgoing profile1
```

Related Commands

Command	Description
rule (voice translation-rule)	Sets the criteria for the translation rule.
show voice translation-profile	Displays the configuration of a translation profile.
translate (translation profiles)	Assigns a translation rule to a translation profile.
voice translation-profile	Initiates the translation-profile definition.
voice translation-rule	Initiates the translation-rule definition.

translation-profile (source group)

To assign a translation profile to a source IP group, use the **translation-profile** command in source group configuration mode. To delete the translation profile from the source IP group, use the **no** form of this command.

translation-profile incoming *name*
no translation-profile incoming *name*

Syntax Description

incoming	Specifies that this translation profile handles incoming calls.
name	Name of the translation profile.

Command Default

No default behavior or values

Command Modes

Source group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use the **translation-profile** command to assign a predefined translation profile to a source IP group.

Examples

The following example assigns the translation profile named "chicago" to handle translation of incoming calls for a voice source group:

```
Router(config)# voice source-group alpha
Router(cfg-source-grp)# translation-profile incoming chicago
```

Related Commands

Command	Description
rule (voice translation-rule)	Sets the criteria for the translation rule.
show voice translation-profile	Displays the configuration of a translation profile.
translate (translation profiles)	Assigns a translation rule to a translation profile.
voice translation-profile	Initiates the translation-profile definition.
voice translation-rule	Initiates the translation-rule definition.

translation-profile (trunk group)

To assign a translation profile to a trunk group, use the **translation-profile** command in trunk group configuration mode. To delete the translation profile from the trunk group, use the **no** form of this command.

translation-profile {**incoming** | **outgoing**} *name*
no translation-profile {**incoming** | **outgoing**} *name*

Syntax Description

incoming	Specifies that this translation profile handles incoming calls.
outgoing	Specifies that this translation profile handles outgoing calls.
name	Name of the translation profile.

Command Default

No default behavior or values

Command Modes

Trunk group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use the **translation-profile** command to assign a predefined translation profile to a trunk group.

Examples

The following example assigns the translation profile named "newyork" to handle translation of incoming calls for a trunk group:

```
Router(config)# trunk group 10
Router(config-trunk-group)# translation-profile incoming newyork
```

Related Commands

Command	Description
rule (voice translation-rule)	Sets the criteria for the translation rule.
show voice translation-profile	Displays the configuration of a translation profile.
translate (translation profiles)	Assigns a translation rule to a translation profile.
voice translation-profile	Initiates the translation-profile definition.
voice translation-rule	Initiates the translation-rule definition.

translation-profile (voice port)

To assign a translation profile to a voice port, use the **translation-profile** command in voice port configuration mode. To delete the translation profile from the voice port, use the **no** form of this command.

translation-profile {**incoming** | **outgoing**} *name*
no translation-profile {**incoming** | **outgoing**} *name*

Syntax Description

incoming	Specifies that this translation profile handles incoming calls.
outgoing	Specifies that this translation profile handles outgoing calls.
name	Name of the translation profile.

Command Default

No default behavior or values

Command Modes

Voice port configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use the **translation-profile** command to assign a predefined translation profile to a voice port.

Examples

The following example assigns the translation profile named "chicago" to handle translation of incoming calls and a translation profile named "sanjose" to handle outgoing calls for a voice port:

```
Router(config)# voice-port 1/0/0
Router(config-voiceport)# translation-profile incoming chicago
Router(config-voiceport)# translation-profile outgoing sanjose
```

Related Commands

Command	Description
rule (voice translation-rule)	Sets the criteria for the translation rule.
show voice translation-profile	Displays the configuration of a translation profile.
translate (translation profiles)	Assigns a translation rule to a translation profile.
voice translation-profile	Initiates the translation-profile definition.
voice translation-rule	Initiates the translation-rule definition.

translation-profile (voice service POTS)

To assign a translation profile to a non-facility associated signaling (NFAS) interface, use the **translation-profile** command in voice service POTS configuration mode. To delete the translation profile from the interface, use the **no** form of this command.

translation-profile [**incoming** | **outgoing**] **controller** [**T1** | **E1**] *unit-number name*
no translation-profile [**incoming** | **outgoing**] **controller** [**T1** | **E1**] *unit-number name*

Syntax Description

incoming	Specifies that this translation profile handles incoming calls.
outgoing	Specifies that this translation profile handles outgoing calls.
T1	T1 controller.
E1	E1 controller.
unit-number	Number of the controller unit.
name	Name of the translation profile.

Command Default

No default behavior or values

Command Modes

Voice service POTS configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use the **translation-profile** command to assign a predefined translation profile to an NFAS interface.

Examples

The following example assigns to an NFAS interface the translation profile named "delta1" to outgoing T1 calls on controller slot 3 and translation profile "alpha" to incoming T1 calls on controller slot 2:

```
Router(config)# voice service pots
Router(conf-voi-serv)# translation-profile outgoing controller T1 3 delta1
Router(conf-voi-serv)# translation-profile incoming controller T1 2 alpha
```

Related Commands

Command	Description
rule (voice translation-rule)	Sets the criteria for the translation rule.
show voice translation-profile	Displays the configuration of a translation profile.
translate (translation profiles)	Assigns a translation rule to a translation profile.
voice translation-profile	Initiates the translation-profile definition.

Command	Description
voice translation-rule	Initiates the translation-rule definition.

translation-rule

To create a translation name and enter translation-rule configuration mode to apply rules to the translation name, use the **translation-rule** command in global configuration mode. To disable the translation rule, use the **no** form of this command.

translation-rule *name-tag*
no translation-rule *name-tag*

Syntax Description

name -tag	Tag number by which the rule set is referenced. This is an arbitrarily chosen number. Range is from 1 to 2147483647. There is no default value.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR1	This command was introduced for VoIP on Cisco AS5300.
12.0(7)XK	This command was implemented for the following voice technologies on the following platforms: • VoIP Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 • VoFR Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 • VoATM Cisco 3600 series and Cisco MC3810
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T and implemented for the following voice technology on the following platforms: VoIP (Cisco 1750, Cisco 2600 series, Cisco 3600 series, Cisco AS5300, Cisco 7200 series, and Cisco 7500 series)
12.1(2)T	This command was integrated ino Cisco IOS Release 12.1(2)T for the following voice technologies on the following platforms: • VoIP Cisco MC3810 • VoFR Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 • VoATM Cisco 3600 series and Cisco MC3810
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

This command applies to all translation rules.

Examples

The following example creates translation rule 21 and applies a rule to it:

```
translation-rule 21

   rule 1 555.% 1408555 subscriber international
```

Related Commands

Command	Description
numbering-type	Specifies number type for the VoIP or POTS dial peer.
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
test translation-rule	Tests the execution of the translation rules on a specific name tag.
translate	Applies a translation rule to a calling party number or a called party number for incoming calls.
translate-outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

transport (sip-ua)

To configure the Session Initiation Protocol (SIP) user agent (gateway) for SIP signaling messages on inbound calls through the SIP TCP, Transport Layer Security (TLS) over TCP, or User Datagram Protocol (UDP) socket, use the **transport** command in SIP user agent configuration mode. To block reception of SIP signaling messages on a particular socket, use the **no** form of this command.

transport { **tcp** [**tls** [**v1.0** | **v1.1** | **v1.2** [**minimum**] | **v1.3**]] | **udp** }
no transport { **tcp** [**tls** [**v1.0** | **v1.1** | **v1.2** [**minimum**] | **v1.3**]] | **udp** }
default transport { **tcp** [**tls**] | **udp** }

Syntax Description

tcp	SIP user agent receives SIP messages on TCP port 5060.
tls	(Optional) SIP user agent receives SIP messages on TLS over TCP port 5061. You can configure TLS version 1.0, 1.1, 1.2, or 1.3. Starting from Cisco IOS XE 26.1.1 release, insecure TLS versions and ciphers are not supported in default configurations. However, these insecure configurations are supported in "system mode insecure" operation-mode.
minimum	(Optional) Specifies minimum configured TLS version. The **minimum** keyword can be configured only with TLS version 1.2. This configuration enables TLS versions 1.2 and 1.3.
udp	SIP user agent receives SIP messages on UDP port 5060.

Command Default

TCP, TLS over TCP, and UDP transport protocols are enabled.

Command Modes

SIP user-agent configuration (config-sip-ua)

Command History

Release	Modification
Cisco IOS XE 26.1.1	This command is modified with the removal of insecure TLS versions (1.0, 1.1) and associated ciphers from default configurations. Support for insecure configurations in "system mode insecure" operation-mode.
Cisco IOS XE 17.18.2	Security warnings for usage of legacy TLS and associated weaker ciphers.
Cisco IOS XE 17.14.1a	This command is modified to include the TLS version 1.3 support. In addition, **minimum** keyword configuration support is introduced with TLS version 1.2. Introduced support for the following YANG models: • **transport tcp tls v1.3** • **transport tcp tls v1.2 minimum**
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.
15.6(1)T and 3.17S	This command was modified to include the TLS version 1.2.

Release	Modification
12.4(6)T	The optional TLS keyword was added to the command.
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series routers. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms were not included in this release.
12.2(2)XB1	This command was implemented on Cisco AS5850 platforms.
12.2(2)XA	This command was implemented on Cisco AS5400 and Cisco AS5350 platforms.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300 platforms.

Usage Guidelines

This command controls whether messages reach the SIP service provider interface (SPI). Setting **tcp**, or **tls** over **tcp**, or **udp** as the protocol for the SIP user agents to listen on port 5060.

To block reception of SIP signaling messages on a specific socket, use the **no** form of this command.

To reset this command to the default value, use the **default** form of this command.

Note In the Cisco IOS XE 17.18.2 release, a security warning message appears for configurations using TLS versions below 1.2 and associated weaker ciphers. For secure configurations, we recommend configuring stronger ciphers with TLS version 1.2 or higher.

Note Starting from Cisco IOS XE 26.1.1 release, the insecure TLS versions (1.0, 1.1) and associated ciphers are not supported in default configurations. However, insecure configurations are allowed in "system mode insecure" operation-mode. The following are the insecure ciphers associated with TLS versions (1.0, 1.1):

- DHE_RSA_WITH_AES_128_CBC_SHA
- RSA_WITH_AES_128_CBC_SHA
- RSA_WITH_AES_256_CBC_SHA

Examples

The following example sets the SIP user agent to allow the reception of SIP signaling messages on the UDP socket:

```
sip-ua
 transport udp
```

The following example sets the SIP user agent to allow the reception of SIP signaling messages on the TCP socket:

```
sip-ua
 transport tcp
```

The following example sets the SIP user agent to allow the reception of SIP signaling messages on the TLS over TCP socket:

```
sip-ua
 transport tcp tls
  v1.0  Enable TLS Version 1.0
  v1.1  Enable TLS Version 1.1
  v1.2  Enable TLS Version 1.2
  v1.3  Enable TLS Version 1.3
```

The following example sets the SIP user agent to TLS version 1.2 as minimum, enabling both TLS versions 1.2 and 1.3:

```
sip-ua
 transport tcp tls v1.2 minimum
```

The following example illustrates a security warning message display in Cisco IOS XE 17.18.2 release for configurations using TLS versions below 1.2:

```
Device(config-sip-ua)#transport tcp tls v1.0
 SECURITY WARNING - Module: SIPUA, Command: transport tcp tls v1.0, Reason: Weak tls version,

Remediation: Use stronger tls version to enhance security

Device(config-sip-ua)#do sh run | sec sip-ua
sip-ua
 no remote-party-id
 timers connect 501
 timers dns registrar-cache 60
 transport tcp tls v1.0
 registration spike 100
 connection-reuse
  crypto signaling remote-addr 10.10.10.70 255.255.255.255  trustpoint CUBE-TLS strict-cipher

alias exec tcp show sip-ua connections tcp tls detail
```

The following example illustrates weaker TLS versions (1.0, 1.1) configuration in insecure mode with warning message display, starting from Cisco IOS XE 26.1.1 release:

```
Device# configure terminal
Device(config)# system mode insecure
Device(config)# sip-ua
Device(config-sip-ua)# transport tcp tls v1.1
SECURITY WARNING - Module: SIPUA, Command: transport tcp tls v1.0, Reason: Weak tls version,

Remediation: Use stronger tls version to enhance security
```

The following example illustrates weaker TLS versions (1.0, 1.1) configuration in secure mode with error message display, starting from Cisco IOS XE 26.1.1 release:

```
Device(config-sip-ua)# transport tcp tls v1.1
%Error:Insecure configurations are not permitted in secure mode. To proceed, set the system
 mode to insecure
using the command system mode insecure, and then try again.
Module: SIPUA, Command: transport tcp tls v1.1 , Reason: Weak tls version, Remediation: Use
 stronger tls version
to enhance security
%ERROR: Security policy check failed, configuration can't be applied
```

Related Commands

Command	Description
sip-ua	Enables the SIP user agent configuration commands.

transport switch

To enable switching between UDP and TCP transport mechanisms globally for large Session Initiation Protocol (SIP) messages, use the **transport switch**command in SIP configuration mode. To disable switching between UDP and TCP transport mechanisms globally for large SIP messages, use the **no** form of this command.

transport switch udp tcp
no transport switch udp tcp

Syntax Description

udp	Enables switching the transport mechanism from UDP on the basis of the size of the SIP request being greater than the MTU size.
tcp	Enables switching transport to TCP.

Command Default

Disabled.

Command Modes

SIP configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Switching between transports is provided globally on the router and also on an individual VoIP dial peer.

- Dial-peer mode. You can configure transport for a specific dial peer by using the **voice-class sip transport switch**command. The **voice-class sip transport switch command in** dial-peer configuration mode takes precedence over **the transport switch**command in **global configuration mode.**
- SIP mode. You can configure transport globally by using the **transport switch**command. The **transport switch** command is considered only when there is no matching VoIP dial peer.

In a call forking scenario, if this command is configured, the configuration applies to all forks.

Examples

The following example enables switching of the transport from UDP to TCP:

```
Router(config)# voice service voip
Router(config-voi-srv)# sip
Router(conf-serv-sip)# transport switch udp tcp
```

Related Commands

Command	Description
debug ccsip transport	Enables tracing of the SIP transport handler and the TCP or UDP process.
sip	Enters SIP configuration mode from voice-service VoIP configuration mode.
voice -class sip transport switch	Enables switching between transport mechanisms if the SIP message is larger than 1300 bytes for a specific dial peer.

trunk group (global)

To define or modify the definition of a trunk group and to enter trunk group configuration mode, use the **trunk group**command in global configuration mode. To delete the trunk group, use the **no** form of this command.

trunk group *name*
no trunk group *name*

Syntax Description

name	Name of the trunk group. Valid names contain a maximum of 63 alphanumeric characters.

Command Default

No trunk group is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

Use the **trunk group** command to assign a number or a name to a set of trunk characteristics. The set of characteristics, or *profile* , is assigned to specific trunks as part of the usual trunk configuration steps.

The **trunk group** command initiates the profile definition and switches from global configuration to trunk group configuration mode. Additional commands are available to construct the characteristics of the profile.

Up to 1000 trunk groups can be configured on the gateway provided that the gateway has sufficient memory to store the profiles. If you see the message "Trunk group name could not be added as the threshold has been reached", enter the **debug tgrm**command and check the number of trunk groups or check for insufficient memory.

To associate a trunk group with an interface, use the **trunk-group** (interface) command. A trunk group that was created using the **trunk group** (global) command can be associated with an interface. However, a trunk group need not be defined globally before being associated with an interface. If a trunk group has not been defined globally, it will be created by issuing the **trunk-group** (interface) command.

Examples

The following example creates trunk group 5 and configures the trunk group profile:

```
Router(config)# trunk group 5
Router(config-trunk-group)# carrier-id allcalls
Router(config-trunk-group)# max-calls voice 500 in
Router(config-trunk-group)# hunt-scheme round-robin even up
Router(config-trunk-group)# translation-profile incoming 3
Router(config-trunk-group)# translation-profile outgoing 2
Router(config-trunk-group)# exit
```

The following example creates a trunk group named "mytrunk" and configures the trunk group profile:

```
Router(config)# trunk group mytrunk
Router(config-trunk-group)# carrier-id local
Router(config-trunk-group)# max-calls voice 500
```

```
Router(config-trunk-group)# hunt-scheme least-idle
Router(config-trunk-group)# translation-profile incoming 1
Router(config-trunk-group)# translation-profile outgoing 12
Router(config-trunk-group)# exit
```

Related Commands

Command	Description
carrier-id (trunk group)	Identifies the carrier that owns the trunk group.
description (trunk group)	Permits a description to be associated with a trunk group.
hunt-scheme least-idle	Specifies the least-idle channel search method for incoming and outgoing calls.
hunt-scheme least-used	Specifies the least-used channel search method for incoming and outgoing calls.
hunt-scheme longest-idle	Specifies the longest-idle channel search method for incoming and outgoing calls.
hunt-scheme random	Specifies the random channel search method for incoming and outgoing calls.
hunt-scheme round-robin	Specifies the round-robin channel search method for incoming and outgoing calls.
hunt-scheme sequential	Specifies the sequential channel search method for incoming and outgoing calls.
max-calls	Specifies the number of incoming and outgoing voice and data calls that a trunk group can handle.
show trunk group	Displays the configuration of trunk groups.
translation-profile (trunk group)	Defines call number translation profiles for incoming and outgoing calls.
trunk-group (interface)	Assigns an ISDN PRI or NFAS interface to a trunk group.

trunk-group (CAS custom)

To assign a channel-associated signaling (CAS) trunk to a trunk group, use the **trunk-group**command in CAS custom configuration mode. To delete the CAS trunk from the trunk group, use the **no** form of this command.

trunk-group *name* [*preference-num*]
no trunk-group *name* [*preference-num*]

Syntax Description

name	Name of the trunk group. Maximum length of the trunk group name is 63 alphanumeric characters.
preference -num	(Optional) Priority of the trunk group member in a trunk group. Range is from 1 (highest priority) to 64 (lowest priority).

Command Default

Preference-num is set lower than 64 (internally set to 65)

Command Modes

CAS custom configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use the **trunk-group** command to assign a CAS trunk as a member of a trunk group. This assignment provides the CAS trunk with carrier information, a hunt scheme for finding an available channel for the outgoing call, and translation profiles for number translation.

If more than one CAS trunk is assigned to the same trunk group, the *preference-num* value determines the order in which the trunk group uses the interfaces. A *preference-num* value of 1 is the highest preference so that the trunk is used first; a value of 64 is the lowest preference so that the trunk is used last. If no value is entered for *preference-num*, the software assigns the trunk a preference of 65, which causes that trunk to be used after all other trunks are used.

If two CAS trunks have the same *preference-num*, the trunk that was configured first is used before the other trunk.

A CAS trunk can belong to only one trunk group.

If an interface is removed from the CAS trunk, the interface is removed automatically from the trunk group. A new nonprimary CAS interface is automatically a member of the same trunk group as its primary CAS interface.

Examples

The following example assigns two CAS interfaces to trunk group "westcoast". The preference value for DS0 group 2 is lower than for DS0 group 1; hence DS0 group 2 has a higher priority. Trunk group "westcoast" uses DS0 group 2 first.

```
Router(config)# controller T1 1/0
Router(config-controller)# ds0-group 1 timeslots 1-10 type e&m-fgd
Router(config-controller)# cas-custom 1
```

```
Router(config-controller)# trunk-group westcoast 5
Router(config-controller)# exit
Router(config)# controller T1 1/0
Router(config-controller)# ds0-group 2 timeslots 15-20 type e&m-fgd
Router(config-controller)# cas-custom 2
Router(config-controller)# trunk-group westcoast 3
Router(config-controller)# exit
```

Related Commands

Command	Description
show trunk group	Displays the configuration of a trunk group.

trunkgroup (dial peer)

To assign a dial peer to a trunk group for trunk group label routing, use the **trunkgroup**command in dial-peer configuration mode. To delete the dial peer from the trunk group, use the **no** form of this command.

trunkgroup *name preference-num*
no trunkgroup *name*

Syntax Description

name	Label of the trunk group to use for the call. Valid trunk group names contain a maximum of 63 alphanumeric characters.
preference -num	Preference or priority of the trunk group. Range is from 1 (highest priority) to 64 (lowest priority).

Command Default

Preference-num is set lower than 64 (internally set to 65)

Command Modes

Dial peer configuration (config dial-peer)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2	This command was integrated into the Cisco IOS Release 12.2.
12.2(11)T	The*preference -num* argument was added.

Usage Guidelines

Use the **trunkgroup** command to assign an outgoing dial peer as a member of one or more trunk groups. This assignment provides the dial peer with carrier information, a hunt scheme for finding an available channel for the outgoing call, and translation profiles for number translation.

If the dial peer is a member of more than one trunk group, use the *preference-num* value to set the order in which the trunk groups will be used for the dial peer. A *preference-num* value of 1 is the highest preference so that the trunk group is used first; a value of 64 is the lowest preference so that the trunk group is used last. If no value is entered for *preference-num*, the software assigns the trunk group a preference of 65, which causes that trunk group to be selected after all other trunks are used.

If two trunk groups have the same *preference-num*, the trunk group that was configured first is used before the other trunk group.

Examples

In the following example, dial peer 112 should use the trunk group "east17" and trunk group "north5" for outbound dial peer matching. When selecting a trunk group, "north5" is used first because it has a higher preference than "east17":

```
Router(config)# dial-peer voice 112 pots
Router(config-dial-peer)# trunkgroup east17 3
Router(config-dial-peer)# trunkgroup north5 1
```

Related Commands

Command	Description
debug dialpeer	Initiates dial peer debugging.
show dial-peer voice	Displays the dial peer configuration.
translation-profile (dial peer)	Defines call number translation profiles for incoming and outgoing calls.

trunk-group (interface)

To assign an ISDN PRI or Non-Facility Associated Signaling (NFAS) interface to a trunk group, use the **trunk-group**command in interface configuration mode. To delete the interface from the trunk group, use the **no** form of this command.

trunk-group *name* [*preference-num*]
no trunk-group *name* [*preference-num*]

Syntax Description

name	Name of the trunk group. Valid trunk group names contain a maximum of 63 alphanumeric characters.
preference -num	Priority of the trunk group member in a trunk group. Range is from 1 (highest priority) to 64 (lowest priority).

Command Default

Preference-num is set lower than 64 (internally set to 65)

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(11)T	The trunk-group identification was expanded to include alphanumeric characters using the *name* **argument, and the** *preference-num* argument was added.

Usage Guidelines

Use the **trunk-group** command to configure an ISDN PRI or Non-Facility Associated Signaling (NFAS) interface as a member of a trunk group. This assignment provides the interface with carrier information, a hunt scheme for finding an available channel for the outgoing call, and translation profiles for number translation.

If more than one interface is assigned to the same trunk group, the *preference_num* value determines the order in which the trunk group uses the interfaces. A *preference-num* value of 1 is the highest preference so that the interface is used first; a value of 64 is the lowest preference so that the interface is used last. If no value is entered for *preference-num*, the software assigns the interface a preference of 65, which causes that interface to be selected after all other interfaces are used.

If two interfaces have the same *preference-num*, the interface that was configured first is used before the other interface.

An interface can belong to only one trunk group. Multiple interfaces can belong to the same trunk group.

If an NFAS interface group is assigned as a member of a trunk group, all the subinterfaces belong to that trunk group.

If a subinterface is removed from the NFAS group, the subinterface is removed automatically from the trunk group.

If a new nonprimary NFAS interface is added to the NFAS group, that interface automatically becomes a member of the same trunk group as its primary NFAS interface.

Examples

The following example assigns an ISDN interface to trunk group "eastern" with a preference of 3.

```
Router(config)# interface Serial2:23
Router(config-if)# no ip address
Router(config-if)# isdn switch-type primary-ni
Router(config-if)# isdn T306 30000
Router(config-if)# isdn T310 10000
Router(config-if)# no cdp enable
Router(config-if)# trunk-group eastern 3
Router(config-if)# exit
```

If another interface were assigned to trunk group "eastern" with preference of 1 or 2, the trunk group would use that interface before the one shown above.

Related Commands

Command	Description
show trunk group	Displays the configuration of the trunk group.

trunk-group (voice port)

To assign an analog voice port to a trunk group, use the **trunk-group**command in voice port configuration mode. To delete the trunk group, use the **no** form of this command.

trunk-group *name* [*preference-num*]
no trunk-group *name* [*preference-num*]

Syntax Description

name	Name of the trunk group. Maximum length of the trunk group name is 63 alphanumeric characters.
preference -num	Priority of the trunk group member in a trunk group. Range is from 1 (highest priority) to 64 (lowest priority).

Command Default

Preference-num is set lower than 64 (internally set to 65)

Command Modes

Voice port configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use the **trunk-group** command to configure an analog voice port as a member of a trunk group. This assignment provides the voice port with carrier information, a hunt scheme for finding an available channel for the outgoing call, and translation profiles for number translation.

If more than one voice port is assigned to the same trunk group, the *preference-num* value determines the order by which the trunk group uses the voice ports. A *preference-num* value of 1 is the highest preference so that the voice port is used first; a value of 64 is the lowest preference so that the voice port is used last. If no value is entered for *preference-num*, the software assigns the voice port a preference of 65, which causes that voice port to be selected after all other voice ports are used.

If two voice ports have the same *preference-num*, the voice port that was configured first is used before the other voice port.

A voice port can belong to only one trunk group. Multiple voice ports can belong to the same trunk group.

Examples

The following example assigns voice port 1/0/0 and voice port 1/0/1 to trunk group "north5". Trunk group "north5" uses voice port 1/0/1 before using voice port 1/0/0 because voice port 1/0/1 has preference 1, which is a higher priority than voice port 1/0/0, with preference 2.

```
Router(config)# voice port 1/0/0
Router(config-voiceport)# translation-profile incoming 7
Router(config-voiceport)# translation-profile outgoing 4
Router(config-voiceport)# trunk-group north5 2
Router(config-voiceport)# exit
Router(config)# voice port 1/0/1
Router(config-voiceport)# translation-profile incoming 3
Router(config-voiceport)# translation-profile outgoing 8
```

```
Router(config-voiceport)# trunk-group north5 1
Router(config-voiceport)# exit
```

Related Commands

Command	Description
show trunk group	Displays the configuration of a trunk group.

trunk-group-label (dial peer)

To specify a trunk group as the source or target of a call, use the **trunk-group-label**command in dial peer configuration mode. To delete the trunk group label, use the **no** form of this command.

trunk-group-label {**source** | **target**} *name*
no trunk-group-label {**source** | **target**} *name*

Syntax Description

source	Indicates the trunk group as the source of the incoming call.
target	Indicates the trunk group as the target of the outbound call.
name	Trunk group label. Maximum length of the trunk group label is 127 alphanumeric characters.

Command Default

No default behavior or values

Command Modes

Dial peer configuration (config dial-peer)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

An originating gateway uses the source trunk group label as a matching key to route the call over an inbound dial peer. The terminating gateway uses the target trunk group label to select a dial peer for routing the outbound call over a POTS line.

If a dial peer has a source (or target) carrier ID already defined, then assigning a source (or target) trunk group label to that same dial peer overrides the source (or target) carrier ID. The same is true for the reverse: if a dial peer has a source (or target) trunk group label defined, then assigning a source (or target) carrier ID for that same dial peer overrides the source (or target) trunk group label.

The name of a trunk group label and carrier ID cannot be the same in dial peers.

Examples

The following example shows that dial peer 112 should use trunk group label "north3" for inbound dial peer matching and trunk group label "east17" for outbound dial peer matching:

```
Router(config)# dial-peer voice 112 pots
Router(config-dial-peer)# trunk-group-label source north3
Router(config-dial-peer)# trunk-group-label target east17
```

Related Commands

Command	Description
carrier-id (dial peer)	Specifies the carrier associated with a VoIP call.
show dial-peer voice	Displays configuration information for dial peers.

trunk-group-label (voice source group)

To define a trunk group label in a source IP group, use the **trunk-group-label**command in voice source group configuration mode. To delete the trunk group label, use the **no** form of this command.

trunk-group-label {**source** | **target**} *name*
no trunk-group-label {**source** | **target**} *name*

Syntax Description

source	Indicates the trunk group as the source of the incoming call.
target	Indicates the trunk group as the target of the outbound call.
name	Trunk group label. Maximum length of the trunk group label is 127 alphanumeric characters.

Command Default

No default behavior or values

Command Modes

Voice source group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

A terminating gateway uses the source trunk group label as a search key to find a source IP group for the incoming VoIP call. The gateway uses the target trunk group label to select an outbound dial peer to route the call over a POTS line.

If a source IP group has a source (or target) carrier ID already defined, then assigning a source (or target) trunk group label to that same source IP group overrides the source (or target) carrier ID. The same is true for the reverse: if a source IP group has a source (or target) trunk group label defined, then assigning a source (or target) carrier ID for that same source IP group overrides the source (or target) trunk group label.

The name of a trunk group label and carrier ID of the same type (source or target) cannot be the same in the source IP group.

Examples

The following example shows that source IP group "alpha" uses trunk group "north3" to search for a source IP group for incoming VoIP calls and trunk group "east17" for outbound dial peer matching:

```
Router(config)# voice source-group alpha
Router(cfg-source-grp)# trunk-group-label source north3
Router(cfg-source-grp)# trunk-group-label target east17
```

Related Commands

Command	Description
carrier-id (dial-peer)	Specifies the carrier associated with a VoIP call.
show voice source-group	Displays the configuration for voice source IP groups.

trustpoint (DSP farm profile)

To associate a trustpoint with a DSP farm profile, use the **trustpoint** command in DSP farm profile configuration configuration mode. To remove the association, use the **no** form of this command.

trustpoint *trustpoint-label*
no trustpoint *trustpoint-label*

Syntax Description

trustpoint-label	Label of the trustpoint to be associated with the digital signal processor (DSP) farm profile.

Command Default

No trustpoints are associated with the DSP farm profile

Command Modes

DSP farm profile configuration (config-dspfarm-profile)

Command History

Release	Modification
12.4(11)XW1	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to associate trustpoints with secure DSP farm profiles only. Use the **security** keyword of the **dspfarm profile** command to configure a secure DSP farm profile. If the trustpoint is not already configured, you are prompted to configure the trustpoint.

Examples

The following example associates the trustpoint dspfarm with the DSP farm profile 101:

```
Router(config)# dspfarm profile 101 conference security
Router(config-dspfarm-profile)# trustpoint dspfarm
```

Related Commands

Command	Description
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for digital signal processor (DSP) farm services.

trustpoint (voice class)

To configure a trustpoint, and associate it to a TLS profile, use the **trustpoint** command in voice class configuration mode. To delete the trustpoint, use the **no** form of this command.

trustpoint *trustpoint-name* [**client** *client-trustpoint-name*]
no trustpoint

Syntax Description

trustpoint-name	**trustpoint** *trustpoint-name* —creates a trustpoint to store the devices certificate generated as part of the enrollment process using Cisco IOS public-key infrastructure (PKI) commands.
client *client-trustpoint-name*	(Optional) Associate a client trustpoint. Specify the client trustpoint label.

Command Default

No default behavior or values

Command Modes

Voice class configuration (config-class)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1a	This command was introduced under voice class configuration mode. Introduced support for Yang Model.
Cisco IOS XE 26.1.1	This command was modified to allow provisioning and assigning separate certificates for client and server roles on each SIP trunk in CUBE.

Usage Guidelines

The trustpoint is associated to a TLS profile through the command **voice class tls-profile** *tag*. The *tag* associates the trustpoint configuration to the command **crypto signaling**.

Starting from Cisco IOS XE 26.1.1 release, you can configure client trustpoint along with existing trustpoint configuration under **voice class tls profile**. The client trustpoint is used for TLS client authentication. If client trustpoint is not configured then it'll fallback to common trustpoint .

Examples

The following example illustrates how to create a voice class tls-profile and associate a trustpoint to be used by Cisco UBE to establish a connection with a remote device:

```
Router(config)#voice class tls-profile 2
Router(config-class)#trustpoint CUBETP
```

The following is a sub option to configure client trustpoint along with existing trustpoint config under **voice class tls profile**:

```
Router(config)#voice class tls-profile 1
Router(config-class)#trustpoint  CUBE_TP client Client_TP
```

Related Commands

Command	Description
voice class tls-profile	Provides sub-options to configure the commands that are required for a TLS session.
crypto signaling	Identifies the trustpoint or the **tls-profile** *tag* that is used during the TLS handshake process.

ttl

To set the expiration timer for advertisements, enter the **ttl**command in Annex G configuration mode. To reset to the default, use the no form of this command.

ttl *ttl-value*
no ttl

Syntax Description

ttl -value	Amount of time (in seconds) for which a route from a neighbor is considered valid. Range is from 1 to 2147483647. The default is 1800 (or 30 minutes).

Command Default

1800 seconds (30 minutes)

Command Modes

Annex G configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

The address templates or routes that are static to this Annex G border element (BE) can be advertised to its neighbors. A time-to-live (TTL) value is associated with each of the advertised routes. The TTL value indicates how long the neighbor should consider the routes valid. On expiration of the ttl, the neighbor must query the addressing information again.

Examples

The following example shows a BE with a time-to-live value of 20 seconds.

```
Router(config)# call-router h323-annexg be20
Router(config-annexg)# ttl 20
```

Related Commands

Command	Description
call -router	Enables the Annex G BE configuration commands.
show call -router status	Displays the Annex G BE status.

type (settlement)

To point to the provider type and the specific settlement server, use the **type** command in settlement configuration mode. To disable this command, use the **no** form of this command.

type {**osp** | **uni-osp**}
no type

Syntax Description

osp	Enables the Open Settlement Protocol (OSP) server type.
uni -osp	Enables authentication of VoIP calls to the Public Switched Telephone Network (PSTN) using a single settlement server.

Command Default

osp

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on Cisco 2600 series and Cisco 3600 series, and Cisco AS5300.
12.1(2)T	The uni-osp keyword was introduced.

Usage Guidelines

This command defines the settlement server that is doing the accounting and enables the server to do the accounting.

Examples

The following example enables authentication of VoIP calls to the PSTN using a single settlement server:

```
settlement 0
 type uni-osp
```

Related Commands

Command	Description
connection -timeout	Sets the connection timeout.
customer -id	Sets the customer identification.
device -id	Sets the device identification.
encryption	Specifies the encryption method.
max -connection	Sets the maximum simultaneous connections.
response -timeout	Sets the response timeout.
retry -delay	Sets the retry delay.

Command	Description
retry -limit	Sets the connection retry limit.
session -timeout	Sets the session timeout.
settlement	Enters settlement configuration mode.
show settlement	Displays the configuration for all settlement server transactions.
shutdown/no shutdown	Brings up the settlement provider and then shuts it down.
url	Specifies the Internet service provider (ISP) address.

type (voice)

To specify the E&M interface type, use the **type** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

type {**1** | **2** | **3** | **5**}
no type {**1** | **2** | **3** | **5**}

Syntax Description

1	Indicates the following lead configuration: • E--Output, relay to ground. • M--Input, referenced to ground.
2	Indicates the following lead configuration: • E--Output, relay to SG. • M--Input, referenced to ground. • SB--Feed for M, connected to -48V. • SG--Return for E, galvanically isolated from ground.
3	Indicates the following lead configuration: • E--Output, relay to ground. • M--Input, referenced to ground. • SB--Connected to -48V. • SG--Connected to ground.
5	Indicates the following lead configuration: • E--Output, relay to ground. • M--Input, referenced to -48V.

Command Default

Type 1

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series routers.
11.3(1)MA	This command was implemented on Cisco MC3810.

Usage Guidelines

Use the **type** command to specify the E&M interface for a particular voice port. With **1**, the tie-line equipment generates the E-signal to the PBX type grounding the E-lead. The tie-line equipment detects the M-signal by detecting current flow to ground. If you select **1**, a common ground must exist between the line equipment and the PBX.

With **2**, the interface requires no common ground between the equipment, thereby avoiding ground loop noise problems. The E-signal is generated toward the PBX by connecting it to SG. The M-signal is indicated by the PBX connecting it to SB. While Type 2 interfaces do not require a common ground, they do have the tendency to inject noise into the audio paths because they are asymmetrical with respect to the current flow between devices.



Note E&M Type 4 is not a supported option. However, Type 4 operates similarly to Type 2 except for the M-lead operation. On Type 4, the M-lead states are open/ground, compared to Type 2, which is open/battery. Type 4 can interface with Type 2. To use Type 4 you can set the E&M voice port to Type 2 and perform the necessary M-lead rewiring.

With **3**, the interface operates the same as Type 1 interfaces with respect to the E-signal. The M-signal, however, is indicated by the PBX connecting it to SB on assertion and alternately connecting it to SG during inactivity. If you select **3**, a common ground must be shared between equipment.

With **5**, the Type 5 line equipment indicates E-signal to the PBX by grounding the E-lead. The PBX indicates M-signal by grounding the M-lead. A Type 5 interface is quasi-symmetrical in that while the line is up, current flow is more or less equal between the PBX and the line equipment, but noise injection is a problem.

Examples

The following example selects Type 3 as the interface type for the voice port:

```
voice-port 1/0/0
 type 3
```



U

- uc wsapi, on page 220
- uc secure-wsapi, on page 221
- unbundle vfc, on page 222
- update-callerid, on page 223
- url, on page 224
- url (dial peer), on page 226
- url (SIP), on page 227
- usage-indication, on page 229
- use-proxy, on page 230
- user-id, on page 233

uc wsapi

To configure the nonsecure Cisco Unified Communication IOS services environment for a specific application, use the **uc wsapi** command. To remove the configuration, use **no** form of this command.

uc wsapi
no uc wsapi

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
15.2(2)T	This command was introduced.
Cisco IOS XE Everest 16.6.1	This command extended support for configuring Cisco Unified Communication IOS services environment using HTTPS connection.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use **uc wsapi**command to enter the Cisco Unified Communication IOS services configuration environment in nonsecure mode.

Note If you intend to move from secure mode to nonsecure mode, remove the existing **uc secure-wsapi** configuration and reconfigure in nonsecure mode.

Examples

The following example enters the Cisco Unified Communication IOS services configuration:

```
Router(config)# uc wsapi
Router(config-uc-wsapi)#
```

Related Commands

Command	Description
provider	Enables a provider service.

uc secure-wsapi

To configure secure Cisco Unified Communication IOS services environment for a specific application, use the **uc secure-wsapi** command. To remove the configuration, use **no** form of this command.

uc secure-wsapi
no uc secure-wsapi

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.
Cisco IOS XE Cupertino 17.7.1	Introduced support for YANG models.

Usage Guidelines

Use **uc secure-wsapi** command to enter the Cisco Unified Communication IOS services configuration environment in secure mode.

Note If you intend to move from nonsecure mode to secure mode, remove the existing **uc wsapi** configuration and reconfigure in secure mode.

The following example enters the Cisco Unified Communication IOS services configuration in secure mode:

```
Router(config)# uc secure-wsapi
Router(config-uc-wsapi)#
```

Related Commands

Command	Description
provider	Enables a provider service.

unbundle vfc

To unbundle DSPWare from the VCWare and configure the default file and capability lists with default values, use the **unbundle vfc** command in privileged EXEC mode.

unbundle [**high-complexity** | **medium-complexity**] **vfc** *slot-number*

Syntax Description

high -complexity	(Optional) High-complexity firmware set.
medium -complexity	(Optional) Medium-complexity firmware set.
slot -number	Voice feature card (VFC) slot number.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco AS5300.
12.0(2)XH	The **high-complexity** and **medium-complexity** keywords were added.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

VFCs come with a single bundled image, VCWare, stored in VFC Flash memory. Use this command to unbundle this bundled image into separate files, which are then written to Flash memory. When VCWare is unbundled, it automatically adds DSPWare to Flash memory, creates both the capability and default file lists, and populates these lists with the default files for that version of VCWare. The default file list includes the files to be used to boot up the system. The capability list defines the available voice codecs for H.323 capability negotiation. These files are used during initial card configuration and for subsequent firmware upgrades.

Before unbundling a VFC software image that you have just copied over to VFC Flash, use the **clear vfc**command. Unbundling a DSP firmware set rewrites the default-file and capabilities lists. After unbundling, you must reload the router for any changes to take effect.

Examples

The following example unbundles the high-complexity firmware set into slot 2:

```
Router# unbundle high-complexity vfc 2
```

Related Commands

Command	Description
clear vfc	Resets the VFC.
copy flash vfc	Copies a new version of VCWare from the Cisco AS5300 motherboard to VFC Flash memory.
copy tftp vfc	Copies a new version of VCWare from a TFTP server to VFC Flash memory.

update-callerid

To enable sending updates for callerid, use the **udpate-callerid** command in the Session Initiation Protocol (SIP) configuration mode. To disable this configuration, use the **no** form of this command.

udpate-callerid
no udpate-callerid

Syntax Description

This command has no keywords or arguments.

Command Default

Enabled by default.

Command Modes

Session Initiation Protocol (SIP) configuration mode (conf-voi-serv).

Voice class tenant configuration mode.

Command History

Release	Modification
15.4(1)T Cisco IOS XE 3.11S	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

By default, update-callerid configuration is enabled at global level and CUBE sends an UPDATE message during call transfer handling on CUBE. If you do not need to send callerid UPDATE, disable this configuration at global level. If specific trunks require callerid UPDATE to be sent, it can be enabled at tenant level.

Examples

The following example shows how to enable udpate-callerid using the **udpate-callerid** command:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# udpate-callerid
Device(conf-serv-sip)# end
```

Related Commands

Command	Description

url

To configure the Internet service provider (ISP) address, use the **url** command in settlement configuration mode. To disable the address, use the **no** form of this command.

url *url-address*
no url *url-address*

Syntax Description

url-address	URL address. A valid URL address is as follows: http://*fully qualified domain nam* e[:*port*]/[*URL*]

Command Default

No default behavior or values

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on Cisco 2600 series and Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(11)T	The settlement configuration for this command was modified. The settlement provider must be shut down before the **url** command is entered.

Usage Guidelines

You can configure the address type multiple times. If you configure multiple URLs for the settlement server, the gateway attempts to send the request to each URL in the order in which you configured these addresses.

If the first URL is unsuccessful, the gateway tries the next URL. If the first URL becomes available, the gateway does not switch back until it loops through the list of URLs, for example:

url http://example1.com

url http://example2.com

url http://example3.com

If http://example1.com fails, the gateway sends the request to http://example2.com. If http://example1.com comes back online, the gateway continues to send requests to http://example2.com. Later on, if http://example2 is down, the gateway sends requests to http://example3.com.

When http://servicepoint3.com is down the gateway routes its requests back to http://example1.com.

Examples

The following example shows four URLs configured for the settlement server:

```
settlement 0
 url http://1.2.3.4/
 url http://1.2.3.4:80/
 url https://1.2.3.4:4444/
 url https://example.com:443/
```

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
customer-id	Sets the customer identification.
device-id	Sets the device identification.
encryption	Specifies the encryption method.
max-connection	Sets the maximum simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.
session-timeout	Sets the session timeout.
settlement	Enters settlement configuration mode.
show settlement	Displays the configuration for all settlement server transactions.
shutdown	Brings up the settlement provider.
no shutdown	Shuts down the settlement provider.
type	Specifies the provider type.

url (dial peer)

To specify the URL of a text file that has E.164 patterns configured on a destination E.164 pattern map, use the **url** command in dial-peer configuration mode. To remove the URL of the text file, use the **no** form of this command.

url *url*
no url *url*

Syntax Description

url	The URL of an internally or an externally stored text file that has been used on an E.164 pattern map.

Command Default

The URL is not specified for a text file that is configured on an E.164 pattern map.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Examples

The following example shows how to specify the URL of a text file configured on an E.164 pattern map:

```
Device(config)# dial-peer voice 123 voip system
Device(config-dial-peer)# url http://http-host/config-files/destination-pattern-map.cfg
```

Related Commands

Command	Description
destination e164-pattern-map	Links an E.164 pattern map to a dial peer.
e164	Configures an E.164 pattern entry on a destination E.164 pattern map.
show voice class e164-pattern-map	Displays details of the configuration of a voice class E.164 pattern map.
voice class e164-pattern-map load	Loads a destination E.164 pattern map specified by a text file.

url (SIP)

To configure URLs to either the Session Initiation Protocol (SIP), SIP secure (SIPS), or telephone (TEL) format for your VoIP SIP calls, use the **url** command in SIP configuration mode voice class tenant configuration mode. To reset to the default, use the **no** form of this command.

url {**sip** | **sips** | **system** |**tel** [**phone-context**]}
no url

Syntax Description

sip	Generates URLs in SIP format for VoIP calls.
sips	Generates URLs in SIPS format for VoIP calls.
system	Specifies that the URLs use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.
tel	Generates URLs in TEL format for VoIP calls.
phone-context	(Optional) Appends the phone-context parameter to the TEL URL.

Command Default

SIP URLs

Command Modes

SIP configuration (conf-serv-sip).

Voice class tenant configuration (config-class).

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.
12.4(6)T	The **sips** keyword was added.
12.4(22)YB	The **phone-context** keyword was added.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

This command affects only user-agent clients (UACs), because it causes the use of a SIP, SIPS, or TEL URL in the request line of outgoing SIP INVITE requests. SIP URLs indicate the originator, recipient, and destination of the SIP request; TEL URLs indicate voice call connections.

The **voice-class sip url**command takes precedence over the **url** command configured in SIP global configuration mode. However, if the **voice-class sip url** command is configured with the **system** keyword, the gateway uses what was globally configured with the **url** command.

Enter SIP configuration mode after entering voice-service VoIP configuration mode, as shown in the "Examples" section.

Examples

The following example generates URLs in SIP format:

```
voice service voip
sip
 url sip
```

The following example generates URLs in SIPS format:

```
voice service voip
sip
 url sips
```

The following example generates URLs in the voice class tenant configuration mode:

```
Router(config-class)# url system
```

The following example generates URLs in TEL format:

```
voice service voip
sip
 url tel
```

The following example generates URLs in TEL format and appends the phone-context parameter:

```
voice service voip
sip
 url tel phone-context
```

Related Commands

Command	Description
sip	Enters SIP configuration mode from voice-service VoIP configuration mode.
voice -class sip url	Generates URLs in the SIP, SIPS, or TEL format.

usage-indication

To enter the Annex G neighbor usage mode used to configure optional usage indicators, use the **usage indication** command in Annex G neighbor configuration mode. To return to the default setting, use the **no** form of this command.

usage-indication
no usage-indication

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Annex G neighbor

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use the **usage-indication**command to enter the mode to set usage indication characteristics. Repeat this command for each border element neighbor that you configure.

Note The no shutdown command must be used to enable each service relationship.

Examples

The following example shows how to enter the Annex G neighbor usage mode:

```
doc-rtr3(config-nxg-neigh-usg)#
usage-indication
```

Related Commands

Command	Description
access-policy	Requires that a neighbor be explicitly configured.
inbound ttl	Sets the inbound time-to-live value.
outbound retry-interval	Defines the retry period for attempting to establish the outbound relationship between border elements.
retry interval	Defines the time between delivery attempts.
retry window	Defines for how long a border element will attempt delivery.
shutdown	Enables or disables the border element.

use-proxy

To enable proxy communications for calls between local and remote zones or the H.225 Annex G border element, use the **use-proxy** command in gatekeeper configuration mode. To remove either a proxy configuration entry for a remote zone or the H.225 Annex G border element, to disable proxy communications between local and remote zones or H.225 Annex G border element, use the **no** form of this command.

use-proxy *local-zone-name* {**default** | **h323-annexg** | **remote-zone** *remote-zone-name*} {**inbound-to** | **outbound-from**} {**gateway** | **terminal**}
no use-proxy *local-zone-name* {**default** | **h323-annexg** | **remote-zone** *remote-zone-name*} [{**inbound-to** | **outbound-from**} {**gateway** | **terminal**}]

Syntax Description

local -zone-name	Name or zone name of the gatekeeper, which is usually the fully domain-qualified host name of the gatekeeper.
default	Default proxy policy for all calls that are not defined by a **use-proxy** command with the **remote-zone** keyword or **h323-annexg**keyword.
h323-annexg	Proxy policy for calls to or from the H.225 Annex G border element co-located with the gatekeeper.
remote -zone *remote-zone-name*	Proxy policy for calls to or from a specific remote gatekeeper or zone.
inbound -to	Proxy policy as it applies to calls that are inbound to the local zone from a remote zone. Each **use-proxy** command defines the policy for only one direction.
outbound -from	Proxy policy as it applies to calls that are outbound from the local zone to a remote zone. Each **use-proxy** command defines the policy for only one direction.
gateway	Type of local device to which the policy applies. The **gateway** option applies the policy only to local gateways.
terminal	Type of local device to which the policy applies. The **terminal** option applies the policy only to local terminals.

Command Default

The local zone uses proxy for both inbound and outbound calls to and from the local H.323 terminals only. Proxy is not used for both inbound and outbound calls to and from local gateways. For releases prior to Cisco IOS Release 12.3(7)T, both inbound and outbound calls using the H.225 Annex G border element do not use the proxy.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.0(5)T	This command was introduced on the Cisco AS5300.

Release	Modification
12.1(5)XM2	The command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.3(7)T	The **h323-annexg** keyword was added.

Usage Guidelines

This command replaces the **zone access** command used in previous versions of the gatekeeper. When a previous version of a gatekeeper is upgraded, any **zone access** commands are translated to **use-proxy**commands. You can use the **show gatekeeper zone status** command to see the gatekeeper proxy configuration.

If the domain name is cisco.com, the gatekeeper name might be gk1.cisco.com. However, if the gatekeeper is controlling multiple zones, the name of the gatekeeper for each zone should be a unique string.

Examples

In the following example, the local zone sj.xyz.com is configured to use a proxy for inbound calls from remote zones tokyo.xyz.com and milan.xyz.com to gateways in its local zone. The sj.xyz.com zone is also configured to use a proxy for outbound calls from gateways in its local zone to remote zones tokyo.xyz.com and milan.xyz.com.

```
use-proxy sj.xyz.com remote-zone tokyo.xyz.com inbound-to gateway
use-proxy sj.xyz.com remote-zone tokyo.xyz.com outbound-from gateway
use-proxy sj.xyz.com remote-zone milan.xyz.com inbound-to gateway
use-proxy sj.xyz.com remote-zone milan.xyz.com outbound-from gateway
```

Because the default mode disables proxy communications for all gateway calls, only the gateway calls listed above can use the proxy.

In the following example, the local zone sj.xyz.com uses a proxy for only those calls that are outbound from H.323 terminals in its local zone to the specified remote zone germany.xyz.com:

```
no use-proxy sj.xyz.com default outbound-from terminal
use-proxy sj.xyz.com remote-zone germany.xyz.com outbound-from terminal
```



Note Any calls inbound to H.323 terminals in the local zone sj.xyz.com from the remote zone germany.xyz.com use the proxy because the default applies.

The following example removes one or more proxy statements for the remote zone germany.xyz.com from the proxy configuration list:

```
no use-proxy sj.xyz.com remote-zone germany.xyz.com
```

This command removes all special proxy configurations for the remote zone germany.xyz.com. After you enter a command like this, all calls between the local zone (sj.xyz.com) and germany.xyz.com are processed according to the defaults defined by any **use-proxy** commands that use the **default** option.

To prohibit proxy use for inbound calls to H.323 terminals in a local zone from a specified remote zone, enter a command similar to the following:

```
no use-proxy sj.xyz.com remote-zone germany.xyz.com inbound-to terminal
```

This command overrides the default and disables proxy use for inbound calls from remote zone germany.xyz.com to all H.323 terminals in the local zone sj.xyz.com.

In the following example, the local zone sj.xyz.com is configured to use a proxy for inbound calls and outbound calls that use the H.225 Annex G border element co-located with the gatekeeper:

```
use-proxy sj.xyz.com h323-annexg inbound-to gateway
use-proxy sj.xyz.com h323-annexg outbound-from gateway
```

In the following example, the local zone sj.xyz.com is configured not to use a proxy for inbound calls and outbound calls that use the H.225 Annex G border element co-located with the gatekeeper:

```
no use-proxy sj.xyz.com h323-annexg inbound-to terminal
no use-proxy sj.xyz.com h323-annexg outbound-from terminal
```

The following example removes one or more proxy statements for the H.225 Annex G border element from the proxy configuration list:

```
no use-proxy sj.xyz.com h323-annexg
```

Related Commands

Command	Description
show gatekeeper zone status	Displays the status of zones related to a gatekeeper.

user-id

To match a call based on the user-id field in the Session Initiation Protocol (SIP) uniform resource identifier (URI), use the **user-id**command in voice URI class configuration mode. To remove the match pattern, use the **no** form of this command.

user-id *username-pattern*
no user-id

Syntax Description

username-pattern	Cisco IOS regular expression pattern to match against the user-id field in a SIP URI. Can be up to 32 characters.

Command Default

No default behavior or values

Command Modes

Voice URI class configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- You can use this command only in a voice class for SIP URIs.
- You cannot use this command if you use the **pattern** command in the voice class. The **pattern** command matches on the entire URI, whereas this command matches only a specific field.

Examples

The following example defines a voice class that matches on the user-id field in a SIP URI:

```
voice class uri r100 sip
 user-id abc123
```

Related Commands

Command	Description
destination uri	Specifies the voice class used to match the dial peer to the destination URI for an outgoing call.
host	Matches a call based on the host field in a SIP URI.
incoming uri	Specifies the voice class used to match a VoIP dial peer to the URI of an incoming call.
pattern	Matches a call based on the entire SIP or TEL URI.
phone context	Filters out URIs that do not contain a phone-context field that matches the configured pattern.
voice class uri	Creates or modifies a voice class for matching dial peers to calls containing a SIP or TEL URI.

Command	Description
voice class uri sip preference	Sets a preference for selecting voice classes for a SIP URI.



vad (dial peer) through voice-class sip encap clear-channel

- vad (dial peer), on page 238
- vad (SPA-DSP), on page 240
- vbd-playout-delay, on page 242
- vbr-rt, on page 244
- vcci, on page 246
- video codec (dial peer), on page 247
- video codec (voice class), on page 249
- video screening, on page 251
- violation, on page 252
- violation (media profile), on page 254
- vmwi, on page 256
- vofr, on page 257
- voice, on page 260
- voicecap configure, on page 261
- voicecap entry, on page 262
- voice call capacity mir, on page 264
- voice call capacity reporting, on page 266
- voice call capacity stw, on page 268
- voice call capacity timer interval, on page 270
- voice call convert-discpi-to-prog, on page 271
- voice call csr data-points, on page 273
- voice call csr recording interval, on page 274
- voice call csr reporting interval, on page 275
- voice call debug, on page 276
- voice call disc-pi-off, on page 279
- voice call rate monitor, on page 280
- voice call send-alert, on page 281
- voice call trap deviation, on page 282
- voice call trigger hwm, on page 283
- voice call trigger lwm, on page 285
- voice call trigger percent-change, on page 287

- voice-card, on page 289
- voice cause-code, on page 291
- voice class aaa, on page 292
- voice class busyout, on page 294
- voice class called number, on page 296
- voice class cause-code, on page 298
- voice class codec, on page 299
- voice class custom-cptone, on page 301
- voice class dscp-profile, on page 302
- voice class dualtone, on page 303
- voice class dualtone-detect-params, on page 305
- voice class e164-pattern-map, on page 306
- voice-class dpg, on page 307
- voice class e164-pattern-map load, on page 309
- voice class e164-translation, on page 310
- voice class h323, on page 311
- voice class media, on page 312
- voice class permanent, on page 313
- voice class resource-group, on page 315
- voice class route-string, on page 316
- voice class server-group, on page 317
- voice class sip-copylist, on page 319
- voice class sip-hdr-passthrulist, on page 320
- voice class sip-profiles, on page 321
- voice class srtp-crypto, on page 322
- voice class tenant, on page 324
- voice class tls-profile, on page 325
- voice class tls-cipher, on page 327
- voice class tone-signal, on page 328
- voice class uri, on page 330
- voice class uri sip preference, on page 332
- voice-class aaa (dial peer), on page 334
- voice-class called-number (dial peer), on page 335
- voice-class called-number-pool, on page 336
- voice-class codec (dial peer), on page 337
- voice-class h323 (dial peer), on page 339
- voice-class permanent (dial-peer), on page 340
- voice-class permanent (voice-port), on page 342
- voice-class sip anat, on page 344
- voice-class sip asserted-id, on page 345
- voice-class sip associate registered-number, on page 347
- voice-class sip asymmetric payload, on page 348
- voice-class sip audio forced, on page 349
- voice-class sip authenticate redirecting-number, on page 350
- voice-class sip bind, on page 352
- voice-class sip block, on page 353

- voice-class sip call-route, on page 356
- voice-class sip calltype-video, on page 358
- voice-class sip content sdp version increment, on page 359
- voice-class sip copy-list, on page 360
- voice-class sip e911, on page 361
- voice-class sip-event-list, on page 362
- voice-class sip early-media update block, on page 363
- voice-class sip encap clear-channel, on page 364

vad (dial peer)

To enable voice activity detection (VAD) for calls using a specific dial peer, use the **vad** command in dial-peer configuration mode. To disable VAD, use the **no** form of this command.

vad [**aggressive**]
no vad [**aggressive**]

Syntax Description

aggressive	Reduces noise threshold from -78 to -62 dBm. Available only when session protocol multicast is configured.

Command Default

VAD is enabled

Aggressive VAD is enabled in multicast dial peers

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(4)T	This command was implemented as a dial-peer command on Cisco MC3810 (in prior releases, the **vad**command was available only as a voice-port command).
12.2(11)T	The **aggressive** keyword was added.
Cisco IOS XE Bengaluru 17.6.1a	Introduced support for YANG models.

Usage Guidelines

Use thiscommand to enable voice activity detection. With VAD, voice data packets fall into three categories: speech, silence, and unknown. Speech and unknown packets are sent over the network; silence packets are discarded. The sound quality is slightly degraded with VAD, but the connection monopolizes much less bandwidth. If you use the **no** form of this command, VAD is disabled and voice data is continuously sent to the IP backbone. When configuring voice gateways to handle fax calls, VAD should be disabled at both ends of the IP network because it can interfere with the successful reception of fax traffic.

When the **aggressive** keyword is used, the VAD noise threshold is reduced from -78 to -62 dBm. Noise that falls below the -62 dBm threshold is considered to be silence and is not sent over the network. Additionally, unknown packets are considered to be silence and are discarded.

Examples

The following example enables VAD for a Voice over IP (VoIP) dial peer, starting from global configuration mode:

```
dial-peer voice 200 voip
 vad
```

Related Commands

Command	Description
comfort-noise	Generates background noise to fill silent gaps during calls if VAD is activated.
dial-peer voice	Enters dial-peer configuration mode, defines the type of dial peer, and defines the tag number associated with a dial peer.
vad (voice-port)	Enables VAD for the calls using a particular voice port.

vad (SPA-DSP)

To enable or disable voice activity detection (vad) settings configured locally irrespective of the external vad settings, use the **vad**command in config dspfarm profile mode.

vad {**on** | **off**} **override**

Syntax Description

on	Enables the local vad settings irrespective of the external vad settings.
off	Disables the local vad settins irrespective of the external vad settings.
override	Overrides the external vad settings with local vad configuration details.

Command Default

By default, VAD is enabled.

Command Modes

DSP Farm Profile Configuration Mode (config-dspfarm-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Use this command to enable voice activity detection locally irrespective of external VAD settings. With VAD, voice data packets fall into three categories: speech, silence, and unknown. Speech and unknown packets are sent over the network; silence packets are discarded. The sound quality is slightly degraded with VAD, but the connection monopolizes much less bandwidth. If you disable VAD, voice data is continuously sent to the IP backbone.

Examples

The following example enables VAD and overrides external vad settings with local vad settings:

```
Router(config)# dspfarm profile 1
Router(config-dspfarm-profile)# vad on override
Router(config-dspfarm-profile)# do show running-config
!!!
dspfarm profile 1 transcode
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 maximum sessions 588
 associate application SBC
 vad on override
!
```

The following example disables local vad settings and overrides external vad setting configuration:

```
Router(config)# dspfarm profile 1
Router(config-dspfarm-profile)# vad off override
Router(config-dspfarm-profile)# do show running-config
!!!
dspfarm profile 1 transcode
 codec g711ulaw
```

```
 codec g711alaw
 codec g729ar8
 codec g729abr8
 maximum sessions 588
 associate application SBC
 vad off override
!
```

Related Commands

Command	Description
dsp services dspfarm	Enables the DSP-farm services.
dspfarm profile	Enters the DSP farm profile configuration mode, and defines a profile for the DSP farm services.
show dspfarm (SPA-DSP)	Displays DSP farm service information, such as operational status and DSP resource allocation for transcoding.

vbd-playout-delay

To configure the voice-band-detection playout-delay buffer on a Cisco router, use the **vbd-playout-delay command in**voice service session configuration mode. To disable the buffer, use the no form of this command.

vbd-playout-delay {**maximum** *milliseconds* | **minimum** *milliseconds* | **mode** {**fixed** [**no-timestamps**] | **passthrough**} | **nominal** *milliseconds*}
no vbd-playout-delay

Syntax Description

maximum	Sets the maximum playout buffer delay, in milliseconds (ms). Range: 40 to 1000. Default: 1000.
milliseconds	Delay time, in milliseconds (ms).
minimum	Sets the minimum playout buffer delay, in ms. Range: 10 to 40. Default: 40.
mode	Configures voice-band-detection playout buffer adaptation mode.
fixed	Sets the jitter buffer to a constant delay.
no-timestamps	(Optional) Fixes the jitter buffer at a constant delay without time stamps.
passthrough	Sets the jitter buffer passthrough mode for clock compensation.
nominal	Sets the nominal playout buffer delay, in ms. Range:10 to 1000. Default: 60.

Command Default

The voice-band-detection playout-delay buffer is disabled.

Command Modes

Voice service session configuration (conf-voi-serv-sess)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(24)T	This command was modified. • The minimum time range value was changed from 4 to 1700 ms to a range of 10 to 40 ms. The default value 4 was increased to 40 ms. • The maximum time value was decreased from 1700 to 1000 ms and the default of 200 was increased to 1000 ms. • The nominal time range value was changed from 0 to 1500 ms to a range of 10 to 1000 ms. The default value of 100 was decreased to 60 ms.
12.4(24)T6	This command was modified. The **no-timestamps** keyword was added and **passthrough** keyword usage guidelines were clarified.

Usage Guidelines

Use thiscommand to set the playout jitter buffer. When a voice band is detected, the call uses the G.711 codec, and the playout delay values that you set are picked up. The original voice-call parameters are restored after

the fax or modem call is completed. The **no-timestamps** keyword sets the jitter buffer at a constant delay without reading time stamps.



Note The **passthough** keyword is a special mode used to handle clock drifting properly. We recommend this keyword only when instructed by your Cisco representative.

Examples

The following example configures ATM adaptation layer 2 (AAL2) voice-band-detection playout-delay adaptation mode and sets the mode to fixed:

```
voice service voatm
 session protocol aal2
  vbd-playout-delay mode fixed
```

The following example configures AAL2 voice-band-detection playout-delay adaptation mode and sets the mode at a constant delay without timestamps:

```
voice service voatm
 session protocol aal2
  vbd-playout-delay mode fixed no-timestamps
```

The following example sets the nominal AAL2 voice-band-detection playout-delay buffer to 12 ms:

```
voice service voatm
 session protocol aal2
  vbd-playout-delay nominal 12
```

The following example sets the AAL2 voice-band-detection playout-buffer delay to a maximum of 55 ms:

```
voice service voatm
 session protocol aal2
  vbd-playout-delay maximum 55
```

The following example sets the AAL2 voice-band-detection playout-buffer delay to a minimum of 22 ms:

```
voice service voatm
 session protocol aal2
  vbd-playout-delay minimum 22
```

The following sample output shows the vdb-playout-delay being verified in the running configuration output:

```
Router(conf-voi-serv-sess)#do show run | sec voice service voatm
voice service voatm
 !
 session protocol aal2
  vbd-playout-delay minimum 22
```

Related Commands

Command	Description
voice-service	Specifies the voice encapsulation type and enters voice service configuration mode.

vbr-rt

To configure the real-time variable bit rate (VBR) for VoATM voice connections, use the **vbr-rt** command in the appropriate configuration mode. To disable VBR for voice connections, use the **no** form of this command.

vbr-rt *peak-rate average-rate burst*
no vbr-rt

Syntax Description

peak-rate	Peak information rate (PIR) for the voice connection, in kilobytes per second (kbps). If it does not exceed your carrier's line rate, set it to the line rate. Range is from 56 to 10000.
average-rate	Average information rate (AIR) for the voice connection, in kbps.
burst	Burst size, in number of cells. Range is from 0 to 65536.

Command Default

No real-time VBR settings are configured

Command Modes

ATM Bundle-vc configuration for ATM VC bundle members
ATM PVP configuration for an ATM PVP
Interface-ATM-VC configuration for an ATM permanent virtual connection (PVC) or switched virtual circuit (SVC)
VC-class configuration for a virtual circuit (VC) class

Command History

Release	Modification
12.0	This command was introduced on the Cisco MC3810.
12.1(5)XM	This command was implemented on Cisco 3600 series routers and modified to support Simple Gateway Control Protocol (SGCP) and Media Gateway Control Protocol (MGCP).
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.
Cisco IOS XE Release 2.3	This command was made available in ATM PVP configuration mode.

Usage Guidelines

This command configures traffic shaping between voice and data PVCs. Traffic shaping is required so that the carrier does not discard calls. To configure voice and data traffic shaping, you must configure the peak, average, and burst options for voice traffic. Configure the burst value if the PVC will carry bursty traffic. Peak, average, and burst values are needed so that the PVC can effectively handle the bandwidth for the number of voice calls.

Calculate the minimum peak, average, and burst values for the number of voice calls as follows:

Peak Value

Peak value = (2 x the maximum number of calls) x 16K = _____

Average Value

Calculate according to the maximum number of calls that the PVC will carry times the bandwidth per call. The following formulas give you the average rate in kbps:

- For VoIP:
  - G.711 with 40- or 80-byte sample size:

Average value = max calls x 128K = _____

- • G.726 with 40-byte sample size:

Average value = max calls x 85K = _____

- • G.729a with 10-byte sample size:

Average value = max calls x 85K = _____

- For VoATM adaptation layer 2 (VoAAL2):
  - G.711 with 40-byte sample size:

Average value = max calls x 85K = _____

- • G.726 with 40-byte sample size:

Average value = max calls x 43K = _____

- • G.729a with 10-byte sample size:

Average value = max calls x 43K = _____

If voice activity detection (VAD) is enabled, bandwidth usage is reduced by as much as 12 percent with the maximum number of calls in progress. With fewer calls in progress, bandwidth savings are less.

Burst Value

Set the burst size as large as possible, and never less than the minimum burst size. Guidelines are as follows:

- Minimum burst size = 4 x number of voice calls = _____
- Maximum burst size = maximum allowed by the carrier = _____

When you configure data PVCs that will be traffic shaped with voice PVCs, use AAL5snap encapsulation and calculate the overhead as 1.13 times the voice rate.

Examples

The following example configures the traffic-shaping rate for ATM PVC 20. Peak, average, and burst rates are calculated based on a maximum of 20 calls on the PVC.

```
pvc 20
 encapsulation aal5mux voice
 vbr-rt 640 320 80
```

Related Commands

Command	Description
encapsulation aal5	Configures the AAL and encapsulation type for an ATM PVC, SVC, or VC class.

vcci

To identify a permanent virtual circuit (PVC) to the call agent, use the **vcci** command in ATM virtual circuit (VC) configuration mode. To restore the default value, use the **no**form of this command.

vcci *pvc-identifier*
no vcci

Syntax Description

pvc-identifier	Identifier for the PVC. Range is from 0 to 32767. There is no default value.

Command Default

No default behavior or values

Command Modes

ATM virtual circuit configuration mode

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

The *pvc-identifier argument*is a unique 15-bit value for each PVC. The call agent sets up a call with the gateway by specifying the PVC using the *pvc-identifier*.

Examples

The following example shows how to assign a PVC identifier:

```
Router(config-if-atm-vc)# vcci 5278
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
pvc	Creates an ATM PVC for voice traffic.

video codec (dial peer)

To assign a video codec to a VoIP dial peer, use the **video codec** command in dial peer configuration mode. To remove a video codec, use the **no** form of this command.

video codec { **h261** | **h263** | **h263** + | **h264** | **mpeg4** | **scip** }
no video codec

Syntax Description

h261	Video Codec H.261
h263	Video Codec H.263
h263+	Video Codec H.263+
h264	Video Codec H.264
mpeg4	Video Codec MPEG-4 ISO/ISE 14496-2
scip	Video Codec SCIP (This feature is available in 'preview' mode)

Command Default

No video codec is configured.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE 17.16.1a	This command was modified to include **SCIP** video codec type. **Note** This feature is available in 'preview' mode as it includes limited functionality or incomplete software dependencies.

Usage Guidelines

Use the **video codec** command to configure a video codec for a VoIP dial peer. If no video codec is configured, the default is transparent codec operation between the endpoints.

Examples

The following example shows configuration for video codec H.263+ on VoIP dial peer 30:

```
dial-peer voice 30 voip
 video codec h263+
```

The following example shows configuration for video codec SCIP on VoIP dial peer 30:

```
dial-peer voice 30 voip
 video codec scip
```

Related Commands

Command	Description
video codec (voice-class)	Specifies a video codec for a voice class.

video codec (voice class)

To specify a video codec for a voice class, use the **video codec** command in voice class configuration mode. To remove the video codec, use the **no** form of this command.

video codec { **h261** | **h263** | **h263 +** | **h264** | **mpeg4** | **scip** }
no video codec { **h261** | **h263** | **h263 +** | **h264** | **mpeg4** | **scip** }

Syntax Description

h261	Apply this preference to video codec H.261
h263	Apply this preference to video codec H.263
h263+	Apply this preference to video codec H.263+
h264	Apply this preference to video codec H.264
mpeg4	Video Codec MPEG-4 ISO/IES 14496-2
scip	Video Codec SCIP (This feature is available in 'preview' mode)

Command Default

No video codec is configured.

Command Modes

voice class configuration (config-class)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.
Cisco IOS XE 17.16.1a	This command was modified to support **SCIP** video codec type. **Note** This feature is available in 'preview' mode as it includes limited functionality or incomplete software dependencies.

Usage Guidelines

Use the **video codec** command to specify one or more video codecs for a voice class.

Examples

The following example shows configuration of two audio codec preferences and three video codec preferences for voice class codec 10:

```
voice class codec 10
 codec preference 1 g711alaw
 codec preference 2 g722
 video codec h261
 video codec h263
 video codec h264
 video codec mpeg4
```

The following example shows configuration of SCIP video codec for voice class codec 1:

```
voice class codec 1
 video codec scip
```

Related Commands

Command	Description
video codec (dial peer)	Specifies a video codec for a VoIP dial peer.

video screening

To enable transcoding and transsizing between two call legs when configuring SIP, use the **video screening** command in voice service SIP configuration mode or voice class tenant configuration mode. To disable transcoding and transsizing, use **no** form of this command.

video screening system
no video screening system

Syntax Description

system	Specifies that transcoding and transsizing use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

Video screening is disabled.

Command Modes

Voice service SIP configuration.

Voice class tenant configuration (config-class)

Command History

Release	Modification
15.1(4)M	The command was introduced.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.

Usage Guidelines

Use this command to enable conversion of video streams if there is a mismatch between two call legs.

Examples

The following example enters the voice-card configuration mode and enables video screening:

```
Router(config)# voice service voip
Router(config-voicecard)# sip
Router((conf-serv-sip)# video screening
```

The following example enters the voice-card configuration mode and enables video screening in voice class tenant configuration mode:

```
Router(conf-class)# video screening system
```

Related Commands

Command	Description
codec profile	Defines the video capabilities needed for video endpoints.
video codec	Assigns a video codec to a VoIP dial peer.

violation

To specify the action that needs to be performed on any violation in the Differentiated Services Code Point (DSCP) policy, use the **violation** command in voice class configuration mode. To disable the configuration, use the **no** form of this command.

violation *number* **action** {**disconnect** | **ignore**} [**no-syslog**]
no violation *number* **action** {**disconnect** | **ignore**} [**no-syslog**]

Syntax Description

number	Number of violations after which the required action needs to be taken. The range is from 1 to 200000. The default value is 20.
action	Specifies that an action must be performed after the specified number of violations.
disconnect	Disconnects the call after the specified number of violations is exceeded.
ignore	Specifies that no action should be taken after the specified number of violations is exceeded.
no-syslog	(Optional) Specifies not to print messages to the system log when violations occur.

Command Default

No actions are specified against any violation.

Command Modes

Voice class configuration (config-class)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

You can use the **violation** command to specify the action that needs to be performed on any violation in the DSCP policy. A system log is created by default. You can configure the **no-syslog** keyword to disable the Cisco Unified Border Element (Cisco UBE) from generating system logs on DSCP policy violation.

Configure a high value for DSCP violations. If you configure a low value such as 5, action will be performed on the call after every five violations and system logs will be generated frequently.

The “100 - Invalid information element contents [Q.850]” message is displayed in the system log when a call is disconnected because of a DSCP policy violation. The cause for disconnecting the call is propagated only to the call leg causing the violation. For example, if the outgoing call leg of a Session Initiation Protocol (SIP)-to-SIP call violates the DSCP policy and the number of violations exceeds the configured number, this call is disconnected with the cause of 100 (Invalid information element contents [Q.850]) to the outgoing call leg and cause 16 (Normal Call Cleaning) to the incoming call leg.

Examples

The following example shows how to configure a router to print to the system log and disconnect the call if a call exceeds 20,000 violations:

```
Router> enable
Router# configure terminal
Router(config)# voice class dscp-profile 1
Router(config-class)# violation 20000 action disconnect
```

Related Commands

Command	Description
dscp media	Specifies the RPH to DSCP mapping.
voice class dscp-profile	Configures the DSCP profile.

violation (media profile)

To specify the action that needs to be performed on any violation in the media bandwidth policy, use the **violation** command in media profile configuration mode. To disable the configuration, use the **no** form of this command.

violation *number* **action** {**disconnect** | **drop** | **ignore**} [**no-syslog**]
no violation *number* **action** {**disconnect** | **drop** | **ignore**} [**no-syslog**]

Syntax Description

number	Number of violations after which the required action needs to be taken. The range is from 1 to 200000. The default value is 20.
action	Specifies that an action must be performed after the specified number of violations.
disconnect	Disconnects the call after the specified number of violations is exceeded.
drop	Drops the call after the specified number of violations is exceeded.
ignore	Specifies that no action should be taken after the specified number of violations is exceeded.
no-syslog	(Optional) Specifies not to print messages to the system log when violations occur.

Command Default

No actions are specified against any violation.

Command Modes

Media profile configuration (cfg-mediaprofile)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

You can use the **violation** command to specify the action that needs to be performed on any violation in the media bandwidth policy. A system log is created by default. You can configure the **no-syslog** keyword to disable the Cisco Unified Border Element (Cisco UBE) from generating system logs on DSCP policy violation.

Configure a high value for DSCP violations. If you configure a low value such as 5, action will be performed on the call after every five violations and system logs will be generated frequently.

Examples

The following example shows how to configure a router to print the system log and disconnect the call if a call exceeds 20,000 violations:

```
Router> enable
Router# configure terminal
Router(config)# media profile police 1
Router(cfg-mediaprofile)# violation 20000 action drop
```

Related Commands

Command	Description
media profile police	Configures the media policing profile.
overhead	Configures the overhead bandwidth percentage above the negotiated bandwidth.

vmwi

To enable DC voltage or FSK visual message-waiting indictator (VMWI) on a Cisco VG224 onboard analog FXS voice port, use the **vmwi** command in voice-port configuration mode. To reset VMWI to default, use the **no** form of this command.

vmwi {**dc-voltage** | **fsk**}
no vmwi

Syntax Description

dc-voltage	DC voltage VMWI is enabled on this FXS port.
fsk	FSK VMWI is enabled on this FXS port. Default.

Command Default

FSK VMWI is enabled.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

This command with the **dc-voltage** keyword enables the message-waiting lamp to flash on an analog phone that requires DC voltage to activate a visual indicator.

This command with the **fsk** keyword enables the message-waiting lamp to flash on an analog phone that requires an FSK message to activate a visual indicator.

DC Voltage VMWI is supported for the SCCP telephony control (STC) application only. For all other applications, such as MGCP, FSK will be used even if you configure the **vmwi dc-voltage** command on the voice gateway.

Examples

The example shows how to enable DC Voltage VMWI on port 2/0 on a Cisco VG224.

```
Router(config)#voice-port 2/0
Router(config-voiceport)#vmwi dc-voltage
Router(config-voiceport)#end
```

Related Commands

Command	Description
stcapp	Enables basic SCCP call-control features for FXS analog ports on Cisco IOS voice gateways

vofr

To enable Voice over Frame Relay (VoFR) on a specific data-link connection identifier (DLCI) and to configure specific subchannels on that DLCI, use the **vofr** command in frame relay DLCI configuration mode. To disable VoFR on a specific DLCI, use the **no** form of this command.

Switched Calls
vofr [**data** *cid*] [**call-control** [*cid*]]
no vofr [**data** *cid*] [**call-control** [*cid*]]

Switched Calls to Cisco MC3810 Multiservice Concentrators Running Cisco IOS Releases Release Before 12.0(7)XK and Release 12.1(2)T
vofr [**cisco**]
no vofr [**cisco**]

Cisco-Trunk Permanent Calls
vofr data *cid* **call-control** *cid*
no vofr data *cid* **call-control** *cid*

FRF.11 Trunk Calls
vofr [**data** *cid*] [**call-control** *cid*]
no vofr [**data** *cid*] [**call-control** *cid*]

Syntax Description

data	(Required for Cisco-trunk permanent calls. Optional for switched calls.) Selects a subchannel (CID) for data other than the default subchannel, which is 4.
cid	(Optional) Specifies the subchannel to be used for data. Range is from 4 to 255. The default is 4. If **data** is specified, enter a valid CID.
call-control	(Optional) Reserves a subchannel for call-control signaling.
cisco	(Optional) Cisco proprietary voice encapsulation for VoFR with data is carried on CID 4 and call-control on CID 5.
cid	(Optional) Specifies the subchannel to be used for call-control signaling. Valid range is from 4 to 255. The default is 5. If **call-control** is specified and a CID is not entered, the default CID is used.

Command Default

Disabled

Command Modes

Frame relay DLCI configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series routers and Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.

Release	Modification
12.0(7)XK	The use of the **cisco** option was modified. Beginning in this release, use the **cisco** option only when configuring connections to Cisco MC3810 running Cisco IOS Releases before 12.0(7)XK and 12.1(2)T.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

The table below lists the different options of the **vofr** command and which combination of options is used beginning in Cisco IOS Release 12.0(7)XK and Release 12.1(2)T.

Table 2: Combinations of the vofr Command

Type of Call	Command Combination to Use
Switched call (user dialed or auto-ringdown) to other routers supporting VoFR	**vofr** [**data** *cid*] [**call-control** [*cid*]][1]
Cisco-trunk permanent call (private-line) to other routers supporting VoFR	**vofr** **data** *cid* **call-control** *cid*
FRF.11 trunk call (private-line) to other routers supporting VoFR	**vofr** [**data** *cid*] [**call-control** *cid*][2]

1 The recommended form of this command to use is vofr data 4 call-control 5 .
2 For FRF.11 trunk calls, the call-control option is not required. It is required only if you mix FRF.11 trunk calls with other types of voice calls on the same PVC.

Examples

The following example, beginning in global configuration mode, shows how to enable VoFR on serial interface 1/1, DLCI 100. The example configures CID 4 for data; no call-control CID is defined.

```
interface serial 1/1
 frame-relay interface-dlci 100
 vofr
```

To configure CID 4 for data and CID 5 for call-control (both defaults), enter the following command:

```
vofr call-control
```

To configure CID 10 for data and CID 15 for call-control, enter the following command:

```
vofr data 10 call-control 15
```

To configure CID 4 for data and CID 15 for call-control, enter the following command:

```
vofr call-control 15
```

To configure CID 10 for data and CID 5 for call-control, enter the following command:

```
vofr data 10 call-control
```

To configure CID 10 for data with no call-control, enter the following command:

```
vofr data 10
```

Related Commands

Command	Description
class	Assigns a VC class to a PVC.
frame-relay interface-dlci	Assigns a DLCI to a specified Frame Relay subinterface.

voice

To enable voice resource pool services for resource pool management, use the **voice** command in service profile configuration mode. To disable voice services, use the **no** form of this command.

voice
no voice

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Service profile configuration mode

Command History

Release	Modification
12.2(2)XA	This command was introduced on the Cisco AS5350 and AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following example shows that voice service is available and enables voice resource pool service using the **voice** command in service profile configuration mode:

```
Router(config)# resource-pool profile service voip
Router(config-service-profile)# ?
  Service Profile Configuration Commands:
  default   Set a command to its defaults
  exit      Exit from resource-manager configuration mode
  help      Description of the interactive help system
  modem     Configure modem service parameters
  no        Negate a command or set in its defaults
  voice     Configure voice service parameters
Router(config-service-profile)# voice
```

Related Commands

Command	Description
resource-pool enable	Enables resource pool management.
resource-pool profile service voip	Defines the VoIP service profile for resource pool management.

voicecap configure

To apply a voicecap on NextPort platforms, use the **voicecap configure**command in voice-port configuration mode. To remove a voicecap, use the **no** form of this command.

voicecap configure *name*
no voicecap configure *name*

Syntax Description

name	Designates which voicecaps to use on this voice port.

Command Default

No default values or behavior

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The character value for the *name* argument must be identical to the value entered when you created the voicecap using the **voicecap entry** command.

Examples

The following example configures a voicecap with the name qualityERL:

```
Router> enable
Router# configure terminal
Router(config)# voicecap entry qualityERL v270=120
Router(config)# voice-port 3/0:D
Router(config-voiceport)# voicecap configure qualityERL
```

Related Commands

Command	Description
voicecap entry	Creates a voicecap on NextPort platforms.

voicecap entry

To create a voicecap, use the **voicecap entry** command in global configuration mode. To disable a voicecap, use the **no** form of this command.

voicecap entry [*name string*]
no voicecap entry [*name string*]

Syntax Description

name string	(Optional) A word and a string of characters that uniquely identify a voicecap. • The *name* argument specifies a unique identifier for a voicecap. • The *string* argument specifies one or more voicecap register entries, similar to a modemcap. Each entry is of the form **v***index* =*value* , where *index* refers to a specific V register, and *value* designates the value for that V register.

Command Default

No voice caps can be applied to configure firmware.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.4(4)XC	This command was modified to include GSMAMR-NB codec capability.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

This command configures firmware through voicecap strings. This command allows you to assign values to specific registers. Voicecaps are applied to specific voice ports at system startup.

The voicecap values can be entered in a DSP-recognizable format called *raw format* . They can also be entered in *standard format* , which allows you to use commonly accessible values, such as decibels.

Starting with Cisco IOS Release 12.4(4)XC, this command can be used to configure GSMAMR-NB codecs on Cisco AS5350XM and Cisco AS5400XM platforms. The register values for GSMAMR-NB are shown in the table below.

Table 3: GSMAMR-NB Register Values

V-Reg #	Default	Description	Register Values and Additional Notes
0	0	Sets how Adaptive Multi-Rate (AMR) responds to an incoming codec mode request (CMR) that is not a member of the mode set.	0 = Drop the packet with the bad CMR. 1 = Ignore the CMR (do not change rates) but process the rest of the packet data normally. 2 = Change the rate to the highest rate in the mode set lower than the rate requested by the CMR.

V-Reg #	Default	Description	Register Values and Additional Notes
1	0	Sets how AMR handles packets with a frame type (AMR rate) that is not a member of the mode set.	0 = Drop the packet with the bad frame-type. 1 = Attempt to decode the packet.

Examples

The following example creates a voicecap string for a GSMAMR-NB codec named gsmamrnb-ctrl with V register 0 set to 1:

```
Router> enable
Router# configure terminal

Router(config)# voicecap entry gsmamrnb-ctrl v0=1
```

Related Commands

Command	Description
voicecap configure	Applies a voicecap to the specified voice ports.

voice call capacity mir

To set the value for the minimum interval between reporting (MIR), use the voice call capacity mir command in global configuration mode. To turn off these attributes, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **capacity mir seconds**
no voice call {**carrier** | **trunk-group** | **prefix**} **capacity mir**

Syntax Description

carrier	Carrier code address family
trunk-group	Trunk group address family
prefix	E.164 prefix
value	Minimum interval, in seconds, with a range of 1 to 3600 seconds and a default of 10. This value cannot be set higher than the time configured for the capacity update interval.

Command Default

10 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Because the available circuit (AC) attribute of a destination is very dynamic, reporting of this attribute should be handled carefully. AC should be reported as frequently as possible so that the location server has better information about the resources. However, the location server should not be overwhelmed with too many updates.

All of the AC reporting, called the interesting point of AC, is performed when the specified event happens within the minimum interval between reporting (MIR) time since last reporting. This command sets the amount of time used for the interval to control the number of interesting points that are reported so not to overwhelm the location server with too many AC updates.

The seconds argument cannot be set higher than the time configured for the capacity update interval.

Examples

The following example shows the minimum interval between reporting for the carrier address family set to 25 seconds:

```
Router(config)# voice call carrier capacity mir 25
```

Related Commands

Command	Description
capacity update interval (dial peer)	Changes the capacity update for prefixes associated with a dial peer.
capacity update interval (trunk group)	Change the capacity update for carriers or trunk groups.

Command	Description
voice call capacity stw	Set the value for STW.

voice call capacity reporting

To turn on the reporting of maxima (first derivative) or inflection (second derivative) points in available capacity, use the voice call capacity reporting command in global configuration mode. To turn off the reporting, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **capacity reporting** {**maxima** | **inflection**}
no voice call {**carrier** | **trunk-group** | **prefix**} **capacity reporting** {**maxima** | **inflection**}

Syntax Description

carrier	Carrier code address family.
trunk-group	Trunk group address family.
prefix	E.164 prefix.
maxima	Maxima (first derivative) point in available capacity.
inflection	Inflection (second derivative) point in available capacity.

Command Default

The capacity reporting function is turned off.

Command Modes

Global configuration.

Command History

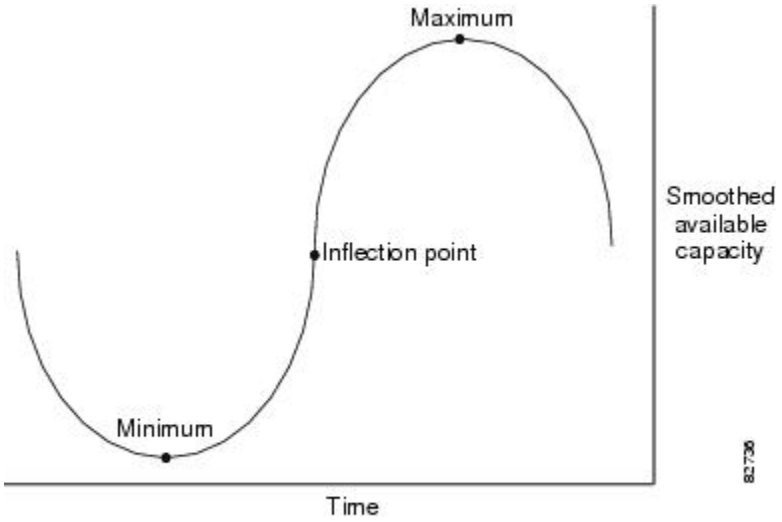
Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The smoothed curve of the available circuits (AC) has maxima, minima, and inflection points. When the curve has reached these points, this represents a change in the call rate.

Maximum, minimum and inflection points are illustrated in the figure below.

Figure 5: Maximum, Minimum, and Inflection Points for Available Capacity



Examples

The following example shows the reporting of the available capacity inflection point on the trunk group is turned on:

```
Router(config)# voice call trunk-group capacity reporting inflection
```

Related Commands

Command	Description
voice call capacity mir	Sets the values for the minimum interval between reporting (MIR) and smoothing transition time for weight (STW).
voice call capacity timer interval	Sets the periodic interval for reporting capacity from carrier, trunk group, or prefix databases
voice call trigger hwm	Sets the value for percentage change, low water mark and high water mark in the available capacity in the trunk group or prefix databases.

voice call capacity stw

To set the value for smoothing transition time for weight (STW), use the voice call capacity stw command in global configuration mode. To turn off these attributes, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **capacity stw seconds**
no voice call {**carrier** | **trunk-group** | **prefix**} **capacity stw**

Syntax Description

carrier	Carrier code address family
trunk-group	Trunk group address family
prefix	E.164 prefix
seconds	Transitions time can be from 0 to 60 seconds with a default of 10.

Command Default

10 seconds.

Command Modes

Global configuration.

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Because the available circuit (AC) attribute of a destination is very dynamic, reporting of this attribute should be handled carefully. AC should be reported as frequently as possible so that the location server has better information about the resources. However, the location server should not be overwhelmed with too many updates.

A smoothing algorithm is applied to the quantity of AC being reported. This algorithm eliminates reporting of noise. The degree of smoothing can be configured with the voice call capacity stw command. This command sets the smoothing transition time for weight, which is the time it takes for current smoothed value of AC to come half way between the current smoothed value and the current instantaneous value of AC. Lower stw values speed the smoothed value of AC as it approaches the instantaneous value of AC. When stw is set to 0, the smoothed value is always equal to the instantaneous value of AC.

Examples

The following example shows the smoothing time for weight for the carrier address family set to 25 seconds:

```
Router(config)# voice call carrier capacity stw 25
```

Related Commands

Command	Description
capacity update interval (dial peer)	Changes the capacity update for prefixes associated with a dial peer.
capacity update interval (trunk group)	Change the capacity update for carriers or trunk groups.

Command	Description
voice call capacity mir	Set the value for MIR.

voice call capacity timer interval

To set the periodic interval for reporting capacity from carrier, trunk group, or prefix databases, use the voice call capacity timer interval command in global configuration mode. To turn off the interval, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **capacity timer interval seconds**
no voice call {**carrier** | **trunk-group** | **prefix**} **capacity timer interval seconds**

Syntax Description

carrier	Carrier code address family
trunk-group	Trunk group address family
prefix	E.164 prefix
seconds	Value from 10 to 3600 seconds.

Command Default

25 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

For the reporting interval, a periodic timer called the capacity update timer handles updates of available circuit (AC) information and can be configured using the voice call capacity timer interval command. For example, if AC has changed since the last reporting, the AC is again reported when the capacity update timer expires.

Examples

The following example sets the timer interval for the prefixes set at 15 seconds:

```
Router(config)# voice call prefix capacity timer interval 15
```

Related Commands

Command	Description
voice call capacity mir	Sets the values for the MIR and STW.
voice call capacity reporting	Turns on the reporting of maxima (first derivative) or inflection (second derivative) points in available capacity.
voice call trigger hwm	Sets the value for percentage change, low water mark and high water mark in the available capacity in the trunk group or prefix databases.

voice call convert-discpi-to-prog

To convert a disconnect message with a progress indicator (PI) to a progress message, use the voice call convert-discpi-to-prog command in global configuration mode. To return to the default condition, use the **no** form of this command.

voice call convert-discpi-to-prog [**tunnel-IEs** | **always** [**tunnel-IEs**]]
no voice call convert-discpi-to-prog

Syntax Description

tunnel-IEs	(Optional) Information elements (IEs) are carried in the progress message.
always	(Optional) Converts disconnect message with a PI to a progress message in both preconnected and connected states.

Command Default

A disconnect message with a PI is not converted to a progress message.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)	This command was introduced.
12.3(6)	The **tunnel-1Es** keyword was added.
12.3(4)XQ	The **always** keyword with the **tunnel-IEs keyword**were added.
12.3(8)T	The **always** keyword with the **tunnel-IEs keyword**were added.
12.3(9)	The **always** keyword with the **tunnel-1Es keyword**were added.

Usage Guidelines

The **voice call convert-discpi-to-prog** command turns an ISDN disconnect message into a progress message. If you use the **tunnel-IEs**keyword, the information elements are not dropped when the disconnect message is converted to a progress message.

Examples

The following example changes a disconnect with PI to a progress message containing information elements (IEs):

```
voice call convert-discpi-to-prog tunnel-IEs
```

The following example changes a disconnect with PI to a progress message in the preconnected and connected states:

```
voice call convert-discpi-to-prog always
```

Related Commands

Command	Description
disc_pi_off	Enables an H.323 gateway to disconnect a call when it receives a disconnect message with a PI.

voice call csr data-points

To set the number of call success rate (CSR) data points, use the voice call csr data-points command in global configuration mode. To disable the setting of the CSR data points, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **csr data-points value**
no voice call {**carrier** | **trunk-group** | **prefix**} **csr data-points value**

Syntax Description

carrier	Carrier code address family
trunk-group	Trunk group address family
prefix	E.164 prefix
value	Value from 10 to 50 data points. Default is 30 data points.

Command Default

30 data points

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples

The following example sets the CSR data points for trunk groups at 10:

```
Router(config)# voice call trunk-group csr data-points 10
```

Related Commands

Command	Description
voice call csr recording interval	Sets the recording interval for the CSR.
voice call csr reporting interval	Sets the reporting interval for the CSR.

voice call csr recording interval

To set the recording interval for call success rates (CSR), use the voice call csr recording interval command in global configuration mode. To disable the CSR recording interval, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **csr recording interval** *minutes*
no voice call {**carrier** | **trunk-group** | **prefix**} **csr recording interval** *minutes*

Syntax Description

carrier	Carrier code address family.
trunk-group	Trunk group address family.
prefix	E.164 prefix.
minutes	Value from 10 to 1000 minutes with a default of 60.

Command Default

60 minutes

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples

The following example sets the CSR recording interval for prefixes at 30 minutes:

```
Router(config)# voice call carrier csr recording interval 30
```

Related Commands

Command	Description
voice call csr data-points	Sets the number of call success rate (CSR) data points.
voice call csr reporting interval	Sets the reporting interval for CSR.

voice call csr reporting interval

To set the reporting interval for call success rate (CSR), use the voice call csr reporting interval command in global configuration mode. To disable the CSR recording interval, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **csr reporting interval seconds**
no voice call {**carrier** | **trunk-group** | **prefix**} **csr reporting interval seconds**

Syntax Description

carrier	Carrier code address family.
trunk-group	Trunk group address family.
prefix	E.164 prefix.
seconds	Value from 10 to 10000 seconds with a default of 25.

Command Default

25 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples

The following example sets the CSR reporting interval for trunk groups at 40 seconds:

```
Router(config)# voice call carrier csr reporting interval 40
```

Related Commands

Command	Description
voice call csr data-points	Sets the number of CSR data points.
voice call csr recording interval	Sets the recording interval for CSR.

voice call debug

To debug a voice call, use the **voice call debug** command in global configuration mode. To disable the **short-header** setting and return tothe **full-guid** setting, use the **no** form of this command.

{**voice call debug full-guid** | **short-header**}
{**no voice call debug full-guid** | **short-header**}

Syntax Description

full-guid	Displays the GUID in a 16-byte header. **Note** When the no version of this command is input with the full-guid keyword, the short 6-byte version displays. This is the default.
short-header	Displays the CallEntry ID in the header without displaying the GUID or module-specific parameters.

Command Default

The short 6-byte header displays.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	The new debug header was added to the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660 series, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850, and Cisco MC3810.
12.2(15)T	The header-only keyword was replaced by the short-header keyword.

Usage Guidelines

Despite its nontraditional syntax (trailing rather than preceding "debug"), this is a normal **debug** command.

You can control the contents of the standardized header. Display options for the header are as follows:

- Short 6-byte GUID
- Full 16-byte GUID
- Short header which contains only the CallEntry ID

The format of the GUID headers is as follows: //CallEntryID/GUID/Module-Dependent-List/Function-name:.

The format of the short header is as follows: //CallEntryID/Function-name:.

When the voice call debug short-header command is entered, the header displays with no GUID or module-specific parameters. When the no voice call debug short-header command is entered, the header, the 6-byte GUID, and module-dependent parameter output displays. The default option is displaying the 6-byte GUID trace.

Note Using the no form of this command does not turn off debugging.

Examples

The following is sample output when the full-guid keyword is specified:

```
Router# voice call debug full-guid
!
00:05:12: //1/0E2C8A90-BC00-11D5-8002-DACCFDCEF87D/VTSP:(0:D):0:0:4385/vtsp_insert_cdb:
00:05:12: //-1/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/CCAPI/cc_incr_if_call_volume: 00:05:12:
 //1/0E2C8A90-BC00-11D5-8002-DACCFDCEF87D/VTSP:(0:D):0:0:4385/vtsp_open_voice_and_set_params:
00:05:12:
//1/0E2C8A90-BC00-11D5-8002-DACCFDCEF87D/VTSP:(0:D):0:0:4385/vtsp_modem_proto_from_cdb:
00:05:12: //1/0E2C8A90-BC00-11D5-8002-DACCFDCEF87D/VTSP:(0:D):0:0:4385/set_playout_cdb:
00:05:12:
//1/0E2C8A90-BC00-11D5-8002-DACCFDCEF87D/VTSP:(0:D):0:0:4385/vtsp_dsp_echo_canceller_control:
```

Note The "//-1/" output indicates that CallEntryID for the CCAPI module is not available.

The table below describes significant fields shown in the display.

Table 4: voice call debug full-guid Field Descriptions

Field	Description
VTSP:(0:D):0:0:4385	VTSP module, port name, channel number, DSP slot, and DSP channel number.
vtsp_insert_cdb	Function name.
CCAPI	CCAPI module.

The following is sample output when the short-header keyword is specified:

```
Router(config)# voice call debug short-header
!
00:05:12: //1/vtsp_insert_cdb:
00:05:12: //-1/cc_incr_if_call_volume:
00:05:12: //1/vtsp_open_voice_and_set_params:
00:05:12: //1/vtsp_modem_proto_from_cdb:
00:05:12: //1/set_playout_cdb:
00:05:12: //1/vtsp_dsp_echo_canceller_control:
```

Note The "//-1/" output indicates that CallEntryID for CCAPI is not available.

Related Commands

Command	Description
debug rtsp api	Displays debug output for the RTSP client API.
debug rtsp client session	Displays debug output for the RTSP client data.

Command	Description
debug rtsp error	Displays error message for RTSP data.
debug rtsp pmh	Displays debug messages for the PMH.
debug rtsp socket	Displays debug output for the RTSP client socket data.
debug voip ccapi error	Traces error logs in the CCAPI.
debug voip ccapi inout	Traces the execution path through the CCAPI.
debug voip ivr all	Displays all IVR messages.
debug voip ivr applib	Displays IVR API libraries being processed.
debug voip ivr callsetup	Displays IVR call setup being processed.
debug voip ivr digitcollect	Displays IVR digits collected during the call.
debug voip ivr dynamic	Displays IVR dynamic prompt play debug.
debug voip ivr error	Displays IVR errors.
debug voip ivr script	Displays IVR script debug.
debug voip ivr settlement	Displays IVR settlement activities.
debug voip ivr states	Displays IVR states.
debug voip ivr tclcommands	Displays the TCL commands used in the script.
debug voip rawmsg	Displays the raw VoIP message.
debug vtsp all	Enables **debug vtsp session**, **debug vtsp error**, and **debug vtsp dsp**.
debug vtsp dsp	Displays messages from the DSP.
debug vtsp error	Displays processing errors in the VTSP.
debug vtsp event	Displays the state of the gateway and the call events.
debug vtsp port	Limits VTSP debug output to a specific voice port.
debug vtsp rtp	Displays the voice telephony RTP packet debugging.
debug vtsp send-nse	Triggers the VTSP software module to send a triple redundant NSE.
debug vtsp session	Traces how the router interacts with the DSP.
debug vtsp stats	Debugs periodic statistical information sent and received from the DSP
debug vtsp vofr subframe	Displays the first 10 bytes of selected VoFR subframes for the interface.
debug vtsp tone	Displays the types of tones generated by the VoIP gateway.

voice call disc-pi-off

To enable the gateway to treat a disconnect message with progress indicator (PI) like a standard disconnect without a PI, use the **voice call disc-pi-off**command in global configuration mode. To reset to the default, use the **no** form of this command.

voice call disc-pi-off
no voice call disc-pi-off

Syntax Description

This command has no keywords or arguments.

Command Default

Gateway disconnects incoming call leg when it receives a disconnect message with PI.

Command Modes

Global configuration

Command History

Release	Modification
12.3(5)	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

Use this command if the gateway is connected to a switch that sends a release immediately after it receives a Disconnect with PI. To properly handle the call, the switch should open a backward voice path and keep the call active. Otherwise the rotary dial peer feature does not work because the incoming call leg is disconnected. Using this command enables the gateway to handle a disconnect with PI like a regular disconnect message so that you can use the rotary dial peer feature.

Examples

The following example enables the gateway to properly handle a disconnect with PI:

```
voice call disc-pi-off
```

Related Commands

Command	Description
disc_pi_off	Enables an H.323 gateway to disconnect a call when it receives a disconnect message with a PI.
voice call convert-discpi-to-prog	Converts a disconnect message with a PI to a progress message.

voice call rate monitor

To enable voice call rate monitoring, use the **voice call rate monitor** command in voice service configuration mode. To disable voice call monitoring, use the **no** form of this command.

voice call rate monitor
no voice call rate monitor

Syntax Description

This command has no arguments or keywords.

Command Default

Voice call monitoring is disabled.

Command Modes

Voice service configuration (conf-voi-serv)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

You can use the **voice call rate monitor** command to enable the call monitoring functionality for a duration of 60 seconds.

Examples

The following example shows how to enable voice call rate monitoring on a Cisco Unified Border Element (Cisco UBE):

```
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# voice call rate monitor
```

Related Commands

Command	Description
show voice call rate	Displays the voice call rate information.

voice call send-alert

To enable the terminating gateway to send an alert message instead of a progress message after it receives a call setup message, use the **voice call send-alert command in**global configuration mode. To reset to the default, use the **no** form of this command.

voice call send-alert
no voice call send-alert

Syntax Description

This command has no arguments or keywords.

Command Default

The terminating gateway sends a progress message after it receives a call Setup message.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)XI4	This command was introduced.
12.1(5)T	This command was not supported in this release.
12.1(5.3)T	This command was integrated into Cisco IOS Release 12.1(5.3)T.
12.2(1)	This command was integrated into Cisco IOS Release 12.2.

Usage Guidelines

In Cisco IOS Release 12.1(3)XI and later, the terminating gateway sends a Progress message with a progress indicator (PI) after it receives a Setup message. Previously, the gateway responded with an Alert message after receiving a call. In some cases, if the terminating switch does not forward the progress message to the originating gateway, the originating gateway does not cut-through the voice path until a Connect is received and the caller does not hear a ringback tone. In these cases, you can use the **voice call send-alert** command to make the gateway backward compatible with releases earlier than Cisco IOS Release 12.1(3)XI. If you configure the **voice call send-alert** command, the terminating gateway sends an Alert message after it receives a Setup message from the originating gateway.

To complete calls from a PRI to an FXS interface, configure the **voice call send-alert** command on the FXS device.

Examples

The following example configures the gateway to send an Alert message:

```
voice call send-alert
```

Related Commands

Command	Description
progress_ind	Sets a specific PI in call Setup, Progress, or Connect messages from an H.323 VoIP gateway.

voice call trap deviation

To configure the percentage deviation for voice call trap parameters, use the **voice call trap deviation** command in global configuration mode. To disable the configured percentage deviation, use the **no** form of this command.

voice call trap deviation *percent* [**vad**]
no voice call trap deviation *percent* [**vad**]

Syntax Description

percent	The percentage deviation for trapping calls. The range of acceptable values is 1 to 100. The default is 49.
vad	(Optional) Specifies the deviation for calls with voice activity detection (VAD) turned on.

Command Default

This command is enabled by default, and the deviation for trapping calls is set to 49 percent.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(12)	This command was introduced in a release earlier than Cisco IOS Release 12.4(12).
15.0(1)M	The **no** form of this command was modified.

Usage Guidelines

Prior to Release 15.0(1)M, if a non-default *percent* value was configured, it could be disabled by entering the **no voice call trap deviation** *percent*command, even if the *percent* value was not the configured value. For example, if the **voice call trap deviation 30** command was configured, the **no voice call trap deviation 40**command disabled the initial command.

Beginning in Release 15.0(1)M, the *percent* value in the **no** form of the command must match the configured non-default value. For example, if the **voice call trap deviation 30** command is configured, the only way to disable it is to enter the **no voice call trap deviation 30**command. If the **no voice call trap deviation 40** command is entered, the command-line interface displays this message: "Please enter correct deviation."

Examples

The following example shows how to set the deviation value for trapping calls to 30 percent:

```
Router(config)# voice call trap deviation 30 vad
```

voice call trigger hwm

To set the value for high water mark in the available capacity in the trunk group or prefix databases, use the voice call trigger hwm command in global configuration mode. To disable the trigger point, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **trigger hwm percent**
no voice call {**carrier** | **trunk-group** | **prefix**} **trigger hwm percent**

Syntax Description

carrier	Carrier code address family
trunk-group	Trunk group address family
prefix	E.164 prefix
percent	Value can be 50 to 100 percent with a default of 80. If set to 100, this trigger will be turned off.

Command Default

80 percent

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Available circuits are reported when the value of AC goes above a threshold, called the high water mark. This can be configured with the voice call trigger hwm command. When the hwm option is selected and the value is set to 100, no update is sent due to high water mark.

Examples

The following example sets the trigger for available capacity on trunk groups to send at a high water mark of 75%:

```
Router(config)# voice call trunk-group trigger hwm 75
```

Related Commands

Command	Description
voice call capacity mir	Sets the values for the minimum interval between reporting (MIR) and smoothing transition time for weight (STW).
voice call capacity reporting	Turns on the reporting of maxima (first derivative) or inflection (second derivative) points in available capacity.
voice call capacity timer interval	Sets the periodic interval for reporting capacity from carrier, trunk group, or prefix databases
voice call trigger lwm	Sets the value for low water mark in the available capacity for carrier, trunk group, or prefix databases

Command	Description
voice call trigger percent-change	Sets the value for percentage change in the available capacity for carrier, trunk group, or prefix databases

voice call trigger lwm

To set the value for low water mark in the available capacity in the trunk group or prefix databases, use the voice call trigger lwm command in global configuration mode. To disable the trigger point, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **trigger lwm percent**
no voice call {**carrier** | **trunk-group** | **prefix**} **trigger lwm percent**

Syntax Description

carrier	Carrier code address family
trunk-group	Trunk group address family
prefix	E.164 prefix
percent	Value can be 0 to 30 percent with a default of 10. If set to 0, this trigger will be turned off.

Command Default

10 percent

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Available circuits are reported when the value of AC falls below a threshold, called the low water mark. When the lwm option is selected and the value is set to 0, no update is sent due to low water mark.

Examples

The following example sets the trigger for available capacity for E.164 prefixes to send at a low water mark of 25%:

```
Router(config)# voice call prefix trigger lwm 25
```

Related Commands

Command	Description
voice call capacity mir	Sets the values for the minimum interval between reporting (MIR) and smoothing transition time for weight (STW).
voice call capacity reporting	Turns on the reporting of maxima (first derivative) or inflection (second derivative) points in available capacity.
voice call capacity timer interval	Sets the periodic interval for reporting capacity from carrier, trunk group, or prefix databases.
voice call trigger hwm	Sets the value for high water mark in the available capacity for carrier, trunk group, or prefix databases.

Command	Description
voice call trigger percent-change	Sets the value for percentage change in the available capacity for carrier, trunk group, or prefix databases.

voice call trigger percent-change

To set the value for percentage change, low water mark and high water mark in the available capacity in the trunk group or prefix databases, use the voice call trigger command in global configuration mode. To disable the trigger point, use the **no** form of this command.

voice call {**carrier** | **trunk-group** | **prefix**} **trigger percent-change percent**
no voice call {**carrier** | **trunk-group** | **prefix**} **trigger percent-change percent**

Syntax Description

carrier	Carrier code address family
trunk-group	Trunk group address family
prefix	E.164 prefix
percent	If percent-change is selected, value can be 0 to 100 percent with a default of 30. If set to 0, this trigger will be turned off. If lwm is selected, value can be 0 to 30 percent with a default of 10. If set to 0, this trigger will be turned off. If hwm is select, value can be 50 to 100 percent with a default of 80. If set to 100, this trigger will be turned off.

Command Default

30 percent

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Available circuits are reported when the absolute percent change is above a threshold. When the percent-change option is selected and the value is set to 0, no update for percent change is sent

Examples

The following example sets the trigger for available capacity on the carrier codes to send at a percentage change of 15%:

```
Router(config)# voice call carrier trigger percent-change 15
```

Related Commands

Command	Description
voice call capacity mir	Sets the values for the minimum interval between reporting (MIR) and smoothing transition time for weight (STW).
voice call capacity reporting	Turns on the reporting of maxima (first derivative) or inflection (second derivative) points in available capacity.

Command	Description
voice call capacity timer interval	Sets the periodic interval for reporting capacity from carrier, trunk group, or prefix databases
voice call trigger hwm	Sets the value for high water mark in the available capacity for carrier, trunk group, or prefix databases
voice call trigger lwm	Sets the value for low water mark in the available capacity for carrier, trunk group, or prefix databases

voice-card

To enter voice-card configuration mode and configure a voice card, use the **voice-card** command in global configuration mode. There is no **no** form of this command.

voice-card *slot*

Syntax Description

slot	Slot number for the card to be configured. The following platform-specific numbering schemes apply:
	• Cisco 2600 series and Cisco 2600XM:
	  • 0 is the Advanced Integration Module (AIM) slot in the router chassis.
	  • 1 is the network module slot in the router chassis.
	• Cisco 3600 series:
	  • A value from 1 to 6 identifies a network module slot in the router chassis.
	• Cisco 3660:
	  • 7 is AIM slot 0 in the router chassis.
	  • 8 is AIM slot 1.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XK	The command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.0(7)XK	This command was implemented on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)XB	Values for the *slot* argument were updated to include AIMs.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(13)T	This command was supported in Cisco IOS Release 12.2(13)T and implemented on the Cisco 1700 series, Cisco 2600XM, Cisco 3700 series, Cisco 7200 series, Cisco 7500 series, Cisco ICS7750, Cisco MC3810, and Cisco VG200.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

Voice-card configuration mode is used for commands that configure the use of digital signal processing (DSP) resources, such as codec complexity and DSPs. DSP resources can be found in digital T1/E1 packet voice trunk network modules on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.

Codec complexity is configured in voice-card configuration mode and has the following platform-specific usage guidelines:

- On Cisco 2600 series, Cisco 2600XM, Cisco 3660, Cisco 3725, and Cisco 3745, the *slot* argument corresponds to the physical chassis slot of the network module that has DSP resources to be configured.

DSP resource sharing is also configured in voice-card configuration mode. On the Cisco 2600 series, Cisco 2600XM, Cisco 3660, Cisco 3725, and Cisco 3745 under specific circumstances, configuration of the **dspfarm** command enters DSP resources on a network module or AIM into a DSP resource pool. Those DSP resources are then available to process voice traffic on a different network module or voice/WAN interface card (VWIC). See the dspfarm (voice-card) command reference for more information about DSP resource sharing.



Note When running high-complexity images, the system can only process up to 16 voice channels. Those 16 time slots need to be within a contiguous range (timeslot maximum (TSmax) minus timeslot minimum (TSmin) is less than or equal to 16, where TSmax and TSmin are the maximum DS0 and minimum DS0 configured for voice).

This command does not have a no form.

Examples

The following example enters voice-card configuration mode to configure resources on the network module in slot 1:

```
voice-card 1
```

The following example shows how to enter voice-card configuration mode and load high-complexity DSP firmware on voice-card 0. The dspfarm command enters the DSP resources on the AIM specified in the **voice-card** command into the DSP resource pool.

```
voice-card 0
 codec complexity high
 dspfarm
```

Related Commands

Command	Description
codec complexity	Matches the DSP complexity packaging to the codecs to be supported.
dspfarm (voice-card)	Adds the specified voice card to those participating in a DSP resource pool.

voice cause-code

To set the internal Q850 cause code mapping for voice and to enter voice cause configuration mode, use the **voice cause-code**command in global configuration mode. To disable the internal Q850 cause code mapping for voice, use the **no** form of this command.

voice cause-code
no voice cause-code

Syntax Description

This command has no arguments or keywords.

Command Default

Internal Q850 cause code mapping for voice is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Examples

The following example shows how to set the cause code mapping for voice:

```
Router> enable
Router# configure terminal
Router(config)# voice cause-code
```

Related Commands

Command	Description
voice class codec	Assigns an identification tag number for a codec voice class.

voice class aaa

To enable dial-peer-based VoIP AAA configurations, use the **voice class aaa** command in global configuration mode. To disable dial-peer-based VoIP AAA configurations, use the **no** form of this command.

voice class aaa *tag*
no voice class aaa *tag*

Syntax Description

tag	A number used to identify voice class AAA. The range is from 1 to 10000. There is no default value.

Command Default

No default behaviors or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

The **voice class aaa** configuration command sets up a voice service class that allows you to perform dial-peer-based AAA configurations.

The command activates voice class AAA configuration mode. Commands that are configured in voice class AAA configuration mode are listed in the "Related Commands" section.

Examples

The following example shows AAA configurations in voice class AAA configuration mode. The number assigned to the tag is 1.

```
voice class aaa 1
 authentication method dp
 authorization method dp
 accounting method dp
in-bound
 accounting template temp-dp
```

The following example shows accounting configurations in voice class AAA configuration mode:

```
voice class aaa 2
 accounting method dp-out out-bound
 accounting template temp-dp out-bound
```

Related Commands

Command	Description
accounting suppress	Disables accounting that is automatically generated by the service provider module for a specific dial peer.
authentication method	Specifies an authentication method for calls coming into the defined dial peer.
authorization method	Specifies an authorization method for calls coming into the defined dial peer.

Command	Description
method	Specifies an accounting method for calls coming into the defined dial peer.
voice-class aaa	Applies properties defined in the voice class to a specific dial peer.

voice class busyout

To create a voice class for local voice busyout functions, use the **voice class busyout command in**global configuration mode. To delete the voice class, use the **no** form of this command.

voice class busyout *tag*
no voice class busyout *tag*

Syntax Description

tag	Unique identification number assigned to one voice class. Range is 1 to 10000.

Command Default

No voice class is configured for busyout functions.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.

Usage Guidelines

You can apply a busyout voice class to multiple voice ports. You can assign only one busyout voice class to a voice port. If a second busyout voice class is assigned to a voice port, the second voice class replaces the one previously assigned.

If you assign a busyout voice class to a voice port, you may not assign separate busyout commands directly to the voice port, such as **busyout monitor serial**, **busyout monitor ethernet**, or **busyout monitor probe**.

Examples

The following example configures busyout voice class 20, in which the connections to two remote interfaces are monitored by a response time reporter (RTR) probe with a G.711ulaw profile, and voice ports are busied out whenever both links have a packet loss exceeding 10 percent and a packet delay time exceeding 2 seconds:

```
voice class busyout 20
 busyout monitor probe 171.165.202.128 g711u loss 10 delay 2000
 busyout monitor probe 171.165.202.129 g711u loss 10 delay 2000
```

The following example configures busyout voice class 30, in which voice ports are busied out when serial ports 0/0, 1/0, 2/0, and 3/0 go out of service.

```
voice class busyout 30
 busyout monitor serial 0/0
 busyout monitor serial 1/0
 busyout monitor serial 2/0
 busyout monitor serial 3/0
```

Related Commands

Command	Description
busyout monitor ethernet	Configures a voice port to monitor a local Ethernet interface for events that would trigger a voice-port busyout.

Command	Description
busyout monitor probe	Configures a voice port to enter the busyout state if an RTR probe signal returned from a remote, IP-addressable interface crosses a specified delay or loss threshold.
busyout monitor serial	Configures a voice port to monitor a serial interface for events that would trigger a voice-port busyout.
show voice busyout	Displays information about the voice busyout state.

voice class called number

To define a voice class called number or range of numbers, use the **voice class called number**command in global configuration mode. To remove a voice class called number, use the **no** form of this command.

voice class called number {**inbound** | **outbound** | **pool**} *tag*
no voice class called number

Syntax Description

inbound	Inbound voice class called number.
outbound	Outbound voice class called number.
pool	Voice class called number pool.
tag	Digits that identify a specific inbound or outbound voice class called number or voice class called number pool.

Command Default

No voice class called number is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command to define one or more static voice class called numbers for inbound and outbound POTS dial peers or a dynamic voice class called number pool. The indexes for a voice class called number are defined with the **index** (voice class) command.



Note Enter the **voice class called number** command in global configuration mode without hyphens. Enter the **voice-class called-number** command in dial-peer configuration mode with hyphens.

Examples

The following example shows configuration for an outbound voice class called number:

```
voice class called number outbound 30
 index 1 5550100
 index 2 5550101
 index 3 5550102
 index 4 5550103
```

The following example shows configuration for a voice class called number pool:

```
voice class called number pool 1
 index 1 5550100 - 5550199
```

Related Commands

Command	Description
show voice class called-number	Displays a specific voice class called number.
voice-class called-number (dial-peer)	Assigns a previously defined voice class called number to an inbound or outbound POTS dial peer.

voice class cause-code

To configure cause code list parameters for a voice class and to enter cause code configuration mode, use the **voice class cause-code**command in global configuration mode. To disable the cause code list parameters configuration for a voice class, use the **no** form of this command.

voice class cause-code *number*
no voice class cause-code *number*

Syntax Description

number	Numeric tag that specifies the voice class cause code. The range is from 1 to 64.

Command Default

The cause code list parameters are not defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to configure cause code list parameters for voice class 5:

```
Router> enable
Router# configure terminal
Router(config)# voice class cause-code 5
```

Related Commands

Command	Description
voice class codec	Assigns an identification tag number for a codec voice class.

voice class codec

To enter voice-class configuration mode and assign an identification tag number for a codec voice class, use the voice class codec command in global configuration mode. To delete a codec voice class, use the **no** form of this command.

voice class codec *tag*
no voice class codec *tag*

Syntax Description

tag	Unique number that you assign to the voice class. Range is 1–10000. There is no default.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(2)XH	This command was introduced on the Cisco AS5300.
12.0(7)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.0(7)XK	This command was implemented on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.
Cisco IOS XE Dublin 17.10.1a	Introduced support for the following YANG models in **codec preference** configuration: • **g729br8 [bytes <10-244>]** • **gsmamr-nb [encap | modes | packetization-period]** Introduced support for the following YANG model in **video codec** configuration: • **video codec [h261 | mpeg4]**

Usage Guidelines

This command only creates the voice class for codec selection preference and assigns an identification tag. Use the **codec preference** command to specify the parameters of the voice class, and use the **voice-class codec** dial-peer command to apply the voice class to a VoIP dial peer.

Note

- The **voice class codec**command in global configuration mode is entered without a hyphen. The **voice-class codec**command in dial-peer configuration mode is entered with a hyphen.
- **transparent** is not available under voice class codec in YANG. However, you can configure **codec transparent** directly under dial-peer.

Examples

The following example shows how to enter voice-class configuration mode and assign a voice class tag number starting from global configuration mode:

```
voice class codec 10
```

After you enter voice-class configuration mode for codecs, use the **codec preference** command to specify the parameters of the voice class.

The following example creates preference list 99, which can be applied to any dial peer:

```
voice class codec 99
 codec preference 1 g711alaw
 codec preference 2 g711ulaw bytes 80
 codec preference 3 g723ar53
 codec preference 4 g723ar63 bytes 144
 codec preference 5 g723r53
 codec preference 6 g723r63 bytes 120
 codec preference 7 g726r16
 codec preference 8 g726r24
 codec preference 9 g726r32 bytes 80
 codec preference 10 g728
 codec preference 11 g729br8
 codec preference 12 g729r8 bytes 50
codec preference 13 gsmamr-nb
```

Related Commands

Command	Description
codec preference	Specifies a list of preferred codecs to use on a dial peer.
test voice port detector	Defines the order of preference in which network dial peers select codecs.
voice-class codec (dial peer)	Assigns a previously configured codec selection preference list to a dial peer.

voice class custom-cptone

To create a voice class for defining custom call-progress tones to be detected, use the **voice class custom-cptone command in**global configuration mode. To delete the voice class, use the **no** form of this command.

voice class custom-cptone *cptone-name*
no voice class custom-cptone *cptone-name*

Syntax Description

cptone-name	Descriptive identifier for this class of custom call-progress tones that associates this set of custom call-progress tones with voice ports.

Command Default

No voice class of custom call-progress tones is created.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600, Cisco 3600, and Cisco MC3810 platforms.
12.2(2)T	This command was implemented on Cisco 1750 access routers and integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines

After you create a voice class, you need to define custom call-progress tones for this voice class using the **dualtone** command.

Examples

The following example creates a voice class named country-x.

```
voice class custom-cptone country-x
```

The following example deletes the voice class named country-x.

```
no voice class custom-cptone country-x
```

Related Commands

Command	Description
dualtone	Defines the tone and cadence for a custom call-progress tone.
supervisory custom-cptone	Associates a class of custom call-progress tones with a voice port.
voice class dualtone-detect-params	Modifies the boundaries and limits for call-progress tones.

voice class dscp-profile

To configure the differentiated services code point (DSCP) profile, use the **voice class dscp-profile** command in global configuration mode. To disable the configuration, use the **no** form of this command.

voice class dscp-profile *tag*
no voice class dscp-profile *tag*

Syntax Description

tag	Voice class DSCP tag. The range is from 1 to 10000.

Command Default

A DSCP profile is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

You can use the **voice class dscp-profile** command to configure the DSCP profile and then configure DSCP policing and enter voice class configuration mode.

Examples

The following example shows how to configure a DSCP profile and enter voice class configuration mode:

```
Router> enable
Router# configure terminal
Router(config)# voice class dscp-profile 1
Router(config-class)# end
```

Related Commands

Command	Description
dscp media	Specifies the RPH to DSCP mapping.

voice class dualtone

To create a voice class for Foreign Exchange Office (FXO) supervisory disconnect tone detection parameters, use the **voice class dualtone**command in global configuration mode. To delete the voice class, use the **no** form of this command.

voice class dualtone *tag*
no voice class dualtone *tag*

Syntax Description

tag	Unique identification number assigned to one voice class. Range is from 1 to 10000.

Command Default

No voice class is configured for tone detection parameters.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and the Cisco MC3810.

Usage Guidelines

Use this command first to create the voice class. Then use the **supervisory disconnect dualtone voice-class**command to assign the voice class to a voice port.

A voice class can define any number of tones to be detected. You need to define a matching tone for each supervisory disconnect tone expected from a PBX or from the public switched telephone network (PSTN).

Examples

The following example configures voice class dualtone 70, which defines one tone with two frequency components, and does not configure a cadence list:

```
voice class dualtone 100
 freq-pair 1 350 440
 freq-max-deviation 10
 freq-max-power 6
 freq-min-power 25
 freq-power-twist 15
 freq-max-delay 16
 cadence-min-on-time 50
 cadence-max-off-time 400
 cadence-variation 8
 exit
```

The following example configures voice class dualtone 100, which defines one tone with two frequency components, and configures a cadence list:

```
voice class dualtone 100
 freq-pair 1 350 440
 freq-pair 2 480 850
 freq-max-deviation 10
 freq-max-power 6
 freq-min-power 25
 freq-power-twist 15
 freq-max-delay 16
```

```
 cadence-min-on-time 50
 cadence-max-off-time 400
 cadence-list 1 100 100 300 300
 cadence-variation 8
 exit
```

The following example configures voice class dualtone 90, which defines three tones, each with two frequency components, and configures two cadence lists:

```
voice class dualtone 90
 freq-pair 1 350 440
 freq-pair 2 480 850
 freq-pair 3 1000 1250
 freq-max-deviation 10
 freq-max-power 6
 freq-min-power 25
 freq-power-twist 15
 freq-max-delay 16
 cadence-min-on-time 50
 cadence-max-off-time 500
 cadence-list 1 100 100 300 300 100 200
 cadence-list 2 100 200 100 400
 cadence-variation 8
 exit
```

Related Commands

Command	Description
supervisory disconnect dualtone voice-class	Assigns a previously configured voice class for FXO supervisory disconnect tone to a voice port.

voice class dualtone-detect-params

To create a voice class for defining a set of tolerance limits for the frequency, power, and cadence parameters of the tones to be detected, use the **voice class dualtone-detect-params command in**global configuration mode. To delete the voice class, use the **no** form of this command.

voice class dualtone-detect-params *tag*
no voice class dualtone-detect-params *tag*

Syntax Description

tag	Unique tag identification number assigned to a voice class. Range is from 1 to 10000.

Command Default

No voice class is configured for defining answer-supervision tolerance limits.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was implemented on Cisco 1750 routers and integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines

Use this command to create a voice class in which you can define maximum and minimum call-progress tone tolerance parameters that you can apply to any voice port. These parameters further define the call-progress tones defined by the **voice class custom-cptone** command. Use the **supervisory dualtone-detect-params**command to apply these tolerance parameters to a voice port.

Examples

The following example creates voice class 70, in which you can specify modified boundaries and limits for call-progress tone detection.

```
voice class dualtone-detect-params 70
freq-max-deviation 25
freq-max-power -5
freq-min-power -20
freq-power-twist 10
freq-max-delay 50
cadence-variation 80
exit
```

Related Commands

Command	Description
supervisory dualtone-detect-params	Assigns the boundary and detection tolerance parameters defined by the **voice class dualtone-detect-params**command to a voice port.
voice class custom-cptone	Creates a voice class for defining custom call-progress tones.

voice class e164-pattern-map

To create an E.164 pattern map that specifies multiple destination E.164 patterns in a dial peer, use the **voice class e164-pattern map** command in global configuration mode. To remove an E.164 pattern map from a dial peer, use the **no** form of this command.

voice class e164-pattern-map *tag*
no voice class e164-pattern-map

Syntax Description

tag	A number assigned to a voice class E.164 pattern map. The range is from 1 to 10000.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(4)M	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Examples

The following example shows how to create an E.164 pattern map that specifies multiple destination E.164 patterns in a dial peer:

```
Device(config)# voice class e164-pattern-map 2543
```

Related Commands

Command	Description
show voice class e164-pattern-map	Displays the configuration of E.164 pattern maps.
voice class e164-pattern-map load	Loads a destination E.164 pattern map that is specified by a text file on a dial peer.

voice-class dpg

To create a dial-peer group for grouping multiple outbound dial peers, use the **voice class dpg** command in global configuration mode.

voice class dpg *dial-peer-group-id*

Syntax Description

dial-peer-group-id	Assigns a tag for a particular dial-peer group. The range is 1-10000.

Command Default

Disabled by default.

Command Modes

Global configuration voice class (config).

Command History

Release	Modification
Cisco IOS 15.4(1)T Cisco IOS XE 3.11S	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

You can group up to 20 outbound (H.323, SIP or POTS) dial peers into a dial-peer group and configure this dial-peer group as the destination of an inbound dial peer. Once an incoming call is matched by an inbound dial peer with an active destination dial-peer group, dial peers from this group are used to route the incoming call. No other outbound dial-peer provisioning to select outbound dial peers is used.

A preference can be defined for each dial peer in a dial-peer group. This preference is used to decide the order of selection of dial peers from the group for the setup of an outgoing call.

You can also specify various dial-peer hunt mechanisms using the existing dial-peer hunt command. For more information, refer to Configure Outbound Dial-Peer Group as an Inbound Dial-Peer Destination.

Examples

```
Router(config)#voice class dpg ?
  <1-10000>  Voice class dialpeer group tag

Router(config)#voice class dpg 1
Router(config-class)#dial-pee
Router(config-class)#dial-peer ?
  <1-1073741823>  Voice dial-peer tag

Router(config-class)#dial-peer 1 ?
  preference  Preference order of this dialpeer in a group
  <cr>        <cr>

Router(config-class)#dial-peer 1 pre
Router(config-class)#dial-peer 1 preference ?
  <0-10>  Preference order

Router(config-class)#dial-peer 1 preference 9
Router(config-class)#
```

Related Commands

Command	Description
dial-peer voice	To define a dial peer.
destination -pattern	To configure a destination pattern.

voice class e164-pattern-map load

To load a destination E.164 pattern map that is specified by a text file on a dial peer, use the **voice class e164-pattern-map load** command in privileged EXEC mode.

voice class e164-pattern-map load *tag*

Syntax Description

tag	A number that is assigned to the destination E.164 pattern map. The range is from 1 to 10000.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

After creating an E.164 pattern map, you can add destination E.164 pattern entries to the E.164 pattern map and store all the information on the voice gateway or create the E.164 pattern entries in a text file and store the file on the internally or externally supported file system.

Examples

The following example shows how to reload a particular destination E.164 pattern map on a dial peer:

```
Device# voice class e164-pattern-map load 2543
```

Related Commands

Command	Description
show voice class e164-pattern-map	Displays the configuration of E.164 pattern maps.
voice class e164-pattern-map	Creates an E.164 pattern map to specify multiple destination E.164 patterns in a dial peer.

voice class e164-translation

To translate the phone number of the call source into E.164 format, as per the translation rules, use the **voice class e164-translation** command in global configuration mode.

voice class e164-translation *tag*

Syntax Description

tag	The range is from 1 to 10000.

Command Modes

Global configuration (config)

Command History

Release	Modification
IOS XE Fuji Release 16.8.1	This command was introduced.

Example

The following example translates the input call number with tag 1 into E.164 format.

```
Router(config)# voice class e164-translation 1
Router(config-class)#url ftp://test:test123@8.0.0.200/test_e164.cfg
Router(config-class)#^Z
```

Related Commands

voice class e164-pattern-map	Creates an E.164 pattern map to specify multiple destination E.164 patterns in dial peer.
voice class e164-pattern-map load	Loads a destination E.164 pattern map that is specified by a text file on a dial peer.

voice class h323

To create an H.323 voice class that is independent of a dial peer and can be used on multiple dial peers, use the voice class h323 command in global configuration mode. To remove the voice class, use the no form of this command.

voice class h323 tag
no voice class h323

Syntax Description

tag	Unique number to identify the voice class. Range is from 1 to 10000. There is no default value.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	This command was introduced on the Cisco 1700, Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco AS5300, Cisco uBR910, and Cisco uBR924.

Usage Guidelines

The **voice class h323** command in global configuration mode does not include a hyphen. The **voice-class h323** command in dial-peer configuration mode includes a hyphen.

Examples

The following example demonstrates how a voice class is created and applied to an individual dial peer. Voice class 4 contains a command to disable the capability to detect Cisco CallManager systems in the network (this command is used by Cisco CallManager Express 3.1 and later versions). The example then uses the **voice-class h323**command to apply voice class 4 to dial peer 36.

```
Router(config)# voice class h323 4
Router(config-class)# no telephony-service ccm-compatible
Router(config-class)# exit
Router(config)# dial-peer voice 36 voip
Router(config-dial-peer)# destination-pattern 555....
Router(config-dial-peer)# session target ipv4:10.5.6.7

Router(config-dial-peer)# voice-class h323 4
```

Related Commands

Command	Description
voice-class h323	Assigns an H.323 voice class to a VoIP dial peer.

voice class media

To configure the media control parameters for voice, use the **voice class media**command in global configuration mode. To disable the media control parameters for voice, use the **no** form of this command.

voice class media *number*
no voice class media *number*

Syntax Description

number	Numeric tag that specifies the voice class media. The range is from 1 to 10000.

Command Default

The media control parameters for voice are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Examples

The following example shows how to configure media control parameters for voice:

```
Router> enable
Router# configure terminal
Router(config)# voice class media 5
```

Related Commands

Command	Description
voice class codec	Assigns an identification tag number for a codec voice class.

voice class permanent

To create a voice class for a Cisco trunk or FRF.11 trunk, use the **voice class permanent** command in global configuration mode. To delete the voice class, use the **no** form of this command.

voice class permanent *tag*
no voice class permanent *tag*

Syntax Description

tag	Unique number that you assign to the voice class. Range is from 1 to 10000.

Command Default

No voice class is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

The **voice class permanent** command can be used for Voice over Frame Relay (VoFR), Voice over ATM (VoATM), and Voice over IP (VoIP) trunks.

The **voice class permanent**command in global configuration mode is entered without a hyphen. The **voice-class permanent**command in dial-peer and voice-port configuration modes is entered with a hyphen.

Examples

The following example shows how to create a permanent voice class starting from global configuration mode:

```
voice class permanent 10
 signal keepalive 3
 exit
```

Related Commands

Command	Description
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Configures the ABCD bit pattern for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal timing oos	Configures the signal timing parameter for the OOS state of a call.
signal-type	Sets the signaling type for a network dial peer.

Command	Description
voice-class permanent	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a network dial peer.

voice class resource-group

To enter voice-class configuration mode and assign an identification tag number for a resource group, use the **voice class resource-group**command in global configuration mode. To delete a resource group, use the **no** form of this command.

voice class resource-group *tag*
no voice class resource-group *tag*

Syntax Description

tag	Unique tag to identify the resource. The range is from 1 to 5.

Command Default

No resource groups are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Use the **voice class resource-group** command to configure parameters along with the threshold values to be monitored for resource groups. When you use the **voice class resource-group** command, the router enters voice-class configuration mode. You can then group the resources to be monitored and configure parameters such as .

Examples

The following example shows how to enter voice-class configuration mode and assign identification tag number 5 for a resource group:

```
Router> enable
Router# configure terminal
Router(config)# voice class resource-group 5
```

Related Commands

Command	Description
debug rai	Enables debugging for Resource Allocation Indication (RAI).
periodic-report interval	Configures periodic reporting parameters for gateway resource entities.
rai target	Configures the SIP RAI mechanism.
resource (voice)	Configures parameters for monitoring resources.
show voice class resource-group	Displays the resource group configuration information for a specific resource group or all resource groups.

voice class route-string

To assign a unique identifier tag to a route string, use the **voice class route-string** command in global configuration mode. To remove the route string, use the **no** form for this command.

voice class route-string *tag*
no voice class route-string *tag*

Syntax Description

tag	Unique tag to identify the route string. The range is from 1 to 10000.

Command Default

An identifier tag for the route string is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S.

Usage Guidelines

Use the **voice class route-string** command to assign a unique identification tag to the route string. You can use this command to enter voice class configuration mode to configure a route string pattern.

Example

The following example shows how to assign identification tag 2 for a route string:

```
Device> enable
Device# configure terminal
Device(config)# voice class route-string 2
Device(config-class)# pattern london.uk.eu
```

voice class server-group

To enter voice-class configuration mode and configure server groups (groups of IPv4 and IPv6 addresses) which can be referenced from an outbound SIP dial peer, use the **voice class server-group** command in global configuration mode. To delete a server group, use the **no** form of this command.

voice class server-group *server-group-id*
no voice class server-group *server-group-id*

server-group-id	Unique server group ID to identify the server group. You can configure up to five servers per server group.

Command Default

No server groups are created.

Command Modes

Global configuration (config)

Release	Modification
Cisco IOS XE Release 3.11S 15.4(1)T	The following commands were introduced or modified: **voice class server-group**, **description**, **ipv4 port preference**, **ipv6 port preference**, **hunt-scheme**, **show voice class server-group**, **shutdown (Server Group)**.
Cisco IOS XE Bengaluru 17.4.1a	The following command is introduced under **voice class server-group**. **huntstop** *rule-tag* **resp-code** *from_resp_code* to *to_resp_code*.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use the **voice class server-group** command to group IPv4 and IPv6 addresses of servers and configure it as in an outbound SIP dial-peer. When you use the **voice class server-group** command, the router enters voice-class configuration mode. You can then group the servers and associate them with a SIP outbound dial peer.

The following example shows how to enter voice-class configuration mode and assign server group id for a server group:

```
Router> enable
Router# configure terminal
Router(config)# voice class server-group 2
```

After configuring a voice class server-group, you can configure a server IP address along with an optional port number and preference, as part of this server group along with an optional port number and preference order. You can also configure description, hunt-scheme, and huntstop. You can use the shutdown command to make the server group inactive.

```
Device(config)# voice class server-group 2
Device(config-class)# ipv4 10.1.1.1 preference 1
Device(config-class)# ipv4 10.1.1.2 preference 2
Device(config-class)# ipv4 10.1.1.3 preference 3
Device(config-class)# description It has 3 entries
Device(config-class)# hunt-scheme round-robin
```

```
Device(config-class)# huntstop 1 resp-code 400 to 599
Device(config-class)# exit
```

Related Commands

Command	Description
description	Provides a description for the server group.
hunt-scheme	Defines a hunt method for the order of selection of target server IP addresses (from the IP addresses configured for this server group) for the setting up of outgoing calls.
shutdown (Server Group)	To make the server group inactive.
show voice class server-group	Displays the configurations for all configured server groups or a specified server group.

voice class sip-copylist

To configure a list of entities to be sent to the peer call leg, use the **voice class sip-copylist** command in global configuration mode. To disable the configuration, use the **no** form of this command.

voice class sip-copylist *tag*
no voice class sip-copylist *tag*

Syntax Description

tag	Voice class Session Initiation Protocol (SIP) copylist tag. The range is from 1 to 10000.

Command Default

No header is sent to the peer call leg.

Command Modes

Global configuration (config).

Voice class tenant configuration (config-class).

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use the **voice class sip-copylist** command to configure Cisco Unified Border Element (UBE) to pass an unsupported parameter present in a mandatory header from one call leg to another of Cisco UBE. You can copy the inbound message headers into variables and pass the headers to the outbound call leg.

Examples

The following example shows how to configure a SIP list to be sent to the peer call leg:

```
Router(config)# voice class sip-copylist 5
```

Related Commands

Command	Description
sip-header	Specifies the SIP header to be sent to the peer call leg.

voice class sip-hdr-passthrulist

To configure a list of headers to pass-through, use the **voice class sip-hdr-passthrulist** command in global configuration mode. To remove the header pass-through, use the **no** form of this command.

voice class sip-hdr-passthrulist *tag*
no voice class sip-hdr-passthrulist *tag*

Syntax Description

tag	Unique tag to identify the header. The range is from 1 to 1000.

Command Default

None

Command Modes

Global configuration (config)

Voice class tenant configuration (config-class)

Command History

Release	Modification
15.3(3)M	This command was introduced.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use the **voice class sip-hdr-passthrulist** command to configure a list of headers to be passed-through the route string. You can use this command to enter the voice class configuration mode to configure route-string header pass-through.

Example

The following example shows how to configure header pass-through with the unique identification tag 2:

```
Device> enable
Device# configure terminal
Device(config)# voice class sip-hdr-passthrulist 2
Device(config-class)# passthru-hdr x-cisco-dest-route-string
Device(config-class)# passthru-hdr Supported
Device(config-class)# passthru-hdr Subject
```

voice class sip-profiles

To configure Session Initiation Protocol (SIP) profiles for a voice class, use the **voice class sip-profiles**command in global configuration mode. To disable the SIP profiles for a voice class, use the **no** form of this command.

voice class sip-profiles *number*
no voice class sip-profiles *number*

Syntax Description

number	Numeric tag that specifies the voice class SIP profile. The range is from 1 to 10000.

Command Default

SIP profiles for a voice class are not configured.

Command Modes

Global configuration (config).

Voice class tenant configuration (config-class).

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Note The rule option **[before]** is not available in sip-profile YANG configuration.

voice class sip-profile <tag>

rule [before]

Examples

The following example shows how to specify SIP profile 2 for a voice class:

```
Router> enable
Router# configure terminal
Router(config)# voice class sip-profiles 2
```

Related Commands

Command	Description
voice class codec	Assigns an identification tag number for a codec voice class.

voice class srtp-crypto

To enter voice class configuration mode and assign an identification tag for srtp-crypto voice class, use the **voice class srtp-crypto** command in global configuration mode. To delete **srtp-crypto voice class**, use the **no** form of this command.

voice class srtp-crypto *tag*
no voice class srtp-crypto *tag*

Syntax Description

tag	Unique number that you assign to the srtp-crypto voice class. Range is 1–10000. There is no default.

Command Default

No default behavior or values.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1b	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.
Cisco IOS XE Dublin 17.10.1a	The YANG model for this command can now be configured under **voice register pool**.

Usage Guidelines

This command only creates the voice class for srtp-crypto preference selection and assigns an identification tag. Use the **crypto** command under voice class srtp-crypto submode to select the ordered list of preferred cipher-suites.

Deleting srtp-crypto voice class using **no voice class srtp-crypto** *tag* command removes the srtp-crypto tag (same tag) if configured in global, tenant, and dial-peer configuration mode.

Example

```
Device> enable
Device# configure terminal
Device(config)# voice class srtp-crypto 100
```

Related Commands

Command	Description
srtp-crypto	Assigns a previously configured crypto-suite selection preference list globally or to a voice class tenant.
crypto	Specifies the preference for an SRTP cipher-suite that will be offered by Cisco Unified Border Element (CUBE) in the SDP in offer and answer.
show sip-ua calls	Displays active user agent client (UAC) and user agent server (UAS) information on Session Initiation Protocol (SIP) calls.

Command	Description
show sip-ua srtp	Displays Session Initiation Protocol (SIP) user-agent (UA) Secure Real-time Transport Protocol (SRTP) information.

voice class tenant

To enter voice class tenant configuration mode and to allow tenants to configure their own global configurations for a specific voice class, use the **voice class tenant** command in global configuration mode. To disable the tenant configurations for a voice class, use the **no** form of this command.

voice class tenant *tag*
no voice class tenant *tag*

Syntax Description

tag	A number used to identify voice class tenant. The range is from 1 to 10000. There is no default value.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.6(2)T and IOS XE Denali 16.3.1	This command was introduced.
Cisco IOS XE Bengaluru 17.4.1a	Introduced support for YANG models.

Usage Guidelines

The **voice class tenant** command sets up a voice service class that allows tenants to configure their own sip-specific configurations.

Examples

The following example shows how to configure tenants for a voice class:

```
Device(config)# voice class tenant 1
Device (config-class)# ?
aaa – sip-ua AAA related configuration
anat – Allow alternative network address types IPV4 and IPV6
asserted-id – Configure SIP-UA privacy identity settings
……
……
Video – video related function
Warn-header – SIP related config for SIP. SIP warning-header global config
Device (config-voi-tenant)# end
```

voice class tls-profile

To enable voice class configuration mode, and assign an identification tag for a TLS profile, use the command **voice class tls-profile** in global cofiguration mode. To remove a tls-profile, use the **no** form of this command.

voice class tls-profile *tag*

no voice class tls-profile *tag*

Syntax Description

tag	A number used to identify voice class TLS profile. The range is 1-10000. There is no default value.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1a	This command was introduced.

Usage Guidelines

The command **voice class tls-profile** enables voice class configuration mode on the router and provides you sub-options to configure commands required for a TLS session. This command allows you to configure under voice class, the options that can be configured at the global level via sip-ua.

The *tag* associates all the voice class configurations that are made through the command **voice class tls-profile** *tag* to the command **crypto signaling**. Following is the **crypto signaling** command with **tls-profile** *tag*:

crypto signaling {**remote-addr** *ip address subnet mask* | **default**} **tls-profile** *tag*

For more information on the updates to the command **crypto signaling**, see crypto signaling.

Examples

The following example configures the **voice class tls-profile** with *tag* '2' and enables voice class cofiguration mode:

```
Router(config)#voice class tls-profile 2
Router(config-class)#
```

The following section provides details of the sub-commands that can be configured under the command **voice class tls-profile** *tag*.

The following example configures CUBE to use the **trustpoint** *trustpoint-name* keyword and argument when it establishes or accepts the TLS connection with a remote device:

```
Router(config-class)#trustpoint CUBETP
```

The following example configures client verification trustpoint:

```
Router(config-class)#client-vtp TPname
```

The following example indicates the description for the TLS profile group:

```
Router(config-class)#description tlsgroupname
```

The following example configures the specific size of elliptic curves to be used for a TLS session:

```
Router(config-class)#cipher ecdsa-cipher curve-size 384
```

The following example configures CUBE to perform server identity validation through Common Name (CN) and Subject Alternate Name (SAN) fields in the server certificate:

```
Router(config-class)#cn-san-validate server
```

The following example enables Server Name Indication (SNI) required during the initial TLS handshake process:

```
Router(config-class)#sni send
```

Related Commands

Command	Description
trustpoint	Creates a trustpoint to store the devices certificate that is generated as part of the enrollment process using Cisco IOS public-key infrastructure (PKI) commands.
description	Provides a description for the TLS profile group.
client-vtp	Assigns a client verification trustpoint.
cipher	Configures cipher setting.
cn-san	Enables server identity validation through Common Name (CN) and Subject Alternate Name (SAN) fields in the server certificate during client-side SIP /TLS connections
sni send	Enables TLS Server Name Indication (SNI) during the initial TLS handshake process.
crypto signaling	Identifies the trustpoint or the **tls-profile** *tag* that is used during the TLS handshake process.

voice class tls-cipher

To configure an ordered set of TLS cipher suites, use **voice class tls-cipher** command. To disable this command or revert to default, use the **no** form of this command.

voice class tls-cipher *tag*
no voice class tls-cipher *tag*

tag	Specifies the voice class tls-cipher tag.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Release	Modification
Cisco IOS XE Cupertino 17.8.1a	This command was introduced.

Usage Guidelines

The **voice class tls-cipher** command enables voice class configuration mode on the router, allowing you to configure an ordered list of TLS cipher suites:

Examples

```
Router(config)#voice class tls-cipher 123

Router(config-class)# cipher ?
    <1-10>  Set the preference order for the cipher-suite (1 = Highest)

Router(config-class)#cipher 1 ?

AES128_GCM_SHA256              supported in TLS 1.3
AES256_GCM_SHA384              supported in TLS 1.3
CHACHA20_POLY1305_SHA256       supported in TLS 1.3
DHE_RSA_AES128_GCM_SHA256      supported in TLS 1.2
DHE_RSA_AES256_GCM_SHA384      supported in TLS 1.2
DHE_RSA_WITH_AES_128_CBC_SHA   supported in TLS 1.2 & below
DHE_RSA_WITH_AES_256_CBC_SHA   supported in TLS 1.2 & below
ECDHE_ECDSA_AES128_GCM_SHA256  supported in TLS 1.2
ECDHE_ECDSA_AES256_GCM_SHA384  supported in TLS 1.2
ECDHE_RSA_AES128_GCM_SHA256    supported in TLS 1.2
ECDHE_RSA_AES256_GCM_SHA384    supported in TLS 1.2
RSA_WITH_AES_128_CBC_SHA       supported in TLS 1.2 & below
RSA_WITH_AES_256_CBC_SHA       supported in TLS 1.2 & below

Router(config-class)# cipher 1 ECDHE_RSA_AES256_GCM_SHA384 ?
<cr>   <cr>
Router(config-class)#
```

voice class tone-signal

To enter voice-class configuration mode and create a tone-signal voice class, use the **voice class tone-signal** command in global configuration mode. To delete a tone-signal voice class, use the **no** form of this command.

voice class tone-signal *tag*
no voice class tone-signal *tag*

Syntax Description

tag	Label that uniquely identifies the voice class. Can be up to 32 alphanumeric characters.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

Use the **voice class tone-signal** command to define wakeup, frequency selection, and guard tones to be played out before and during the voice packets for a specific voice port. Use the **inject guard-tone**, **inject pause**, and **inject tone** commands to define the tone signaling in this class. You can configure up to ten tones in a tone-signal voice class.

To avoid voice loss at the receiving end of an LMR system, the maximum of the sum of the durations of the injected tones and pauses in the voice class should not exceed 1500 milliseconds. You must also use the **timing delay-voice tdm** command to configure a delay for the voice packet equal to the sum of the durations of all the injected tones and pauses.

Note that the hyphenation in this command differs from the hyphenation used in a similar command, **voice-class tone-signal**, which is used in voice-port configuration mode.

Examples

The following example shows how to create a tone-signal voice class starting from global configuration mode:

```
voice class tone-signal mytones
 inject tone 1 1950 3 150
 inject tone 2 2000 0 60
 inject pause 3 60
 inject tone 4 2175 3 150
 inject tone 5 1000 0 50
```

Related Commands

Command	Description
inject guard-tone	Plays out a guard tone with the voice packet.
inject pause	Specifies a pause between injected tones.

Command	Description
inject tone	Specifies a wakeup or frequency selection tone to be played out before the voice packet.
timing delay-voice tdm	Specifies the delay before a voice packet is played out.
voice-class tone-signal	Assigns a previously configured tone-signal voice class to a voice port.

voice class uri

To create or modify a voice class for matching dial peers to a Session Initiation Protocol (SIP) or telephone (TEL) uniform resource identifier (URI), use the **voice class uri**command in global configuration mode. To remove the voice class, use the **no** form of this command.

voice class uri *tag* {**sip** | **tel**}
no voice class uri *tag*

Syntax Description

tag	Label that uniquely identifies the voice class. Can be up to 32 alphanumeric characters.
sip	Voice class for SIP URIs.
tel	Voice class for TEL URIs.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

- This command takes you to voice URI class configuration mode, where you configure the match characteristics for a URI. The commands that you enter in this mode define the set of rules by which the URI in a call is matched to a dial peer.
- To reference this voice class for incoming calls, use the **incoming uri** command in the inbound dial peer. To reference this voice class for outgoing calls, use the **destination uri** command in the outbound dial peer.
- Using the **no voice class uri** command removes the voice class from any dial peer where it is configured with the **destination uri** or **incoming uri** commands.

Examples

The following example defines a voice class for SIP URIs:

```
voice class uri r100 sip
 user-id abc123
 host server1
 phone context 408
```

The following example defines a voice class for TEL URIs:

```
voice class uri r101 tel
 phone number ^408
 phone context 408
```

Related Commands

Command	Description
debug voice uri	Displays debugging messages related to URI voice classes.
destination uri	Specifies the voice class used to match the dial peer to the destination URI for an outgoing call.
host	Matches a call based on the host field in a SIP URI.
incoming uri	Specifies the voice class used to match a VoIP dial peer to the URI of an incoming call.
pattern	Matches a call based on the entire SIP or TEL URI.
phone context	Filters out URIs that do not contain a phone-context field that matches the configured pattern.
phone number	Matches a call based on the phone number field in a TEL URI.
show dialplan incall uri	Displays which dial peer is matched for a specific URI in an incoming call.
show dialplan uri	Displays which outbound dial peer is matched for a specific destination URI.
user-id	Matches a call based on the user-id field in the SIP URI.

voice class uri sip preference

To set the preference for selecting a voice class for Session Initiation Protocol (SIP) uniform resource identifiers (URIs), use the **voice class uri sip preference**command in global configuration mode. To reset to the default, use the **no** form of this command.

voice class uri sip preference {**user-id** | **host**}
no voice class uri sip preference

Syntax Description

user-id	User-id field is given preference.
host	Host field is given preference.

Command Default

Host field

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- Use this command to resolve ties when more than one voice class is matched for a SIP URI. The default is to match on the host field of the URI.
- This command applies globally to all URI voice classes for SIP.

Examples

The following example defines the preference as the user-id for a SIP voice class:

```
voice class uri sip preference user-id
```

Related Commands

Command	Description
debug voice uri	Displays debugging messages related to URI voice classes.
destination uri	Specifies the voice class used to match the dial peer to the destination URI for an outgoing call.
host	Matches a call based on the host field in a SIP URI.
incoming uri	Specifies the voice class used to match a VoIP dial peer to the URI of an incoming call.
user-id	Matches a call based on the user-id field in the SIP URI.
show dialplan incall uri	Displays which dial peer is matched for a specific URI in an incoming call.
show dialplan uri	Displays which outbound dial peer is matched for a specific destination URI.

Command	Description
voice class uri	Creates or modifies a voice class for matching dial peers to a SIP or TEL URI.

voice-class aaa (dial peer)

To apply properties defined in the voice class to a dial peer, use the **voice-class aaa**command in dial-peer configuration mode. This command does not have a **no** form.

voice-class aaa *tag*

Syntax Description

tag	A number to identify the voice class. Range is from 1 to 10000. There is no default.

Command Default

No default behaviors or values

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

Properties that are configured in voice class AAA configuration mode can be applied to a dial peer by using this command.

Examples

The following example shows redirecting AAA requests using Digital Number Identification Service (DNIS). You define a voice class to specify the AAA methods and then use this command.

```
voice class aaa 1
  authentication method kz
  authorization method kz
  accounting method kz
!
dial-peer voice 100 voip
  incoming called-number 50..
  session target ipv4:1.5.31.201
  voice-class aaa 1
```

Related Commands

Command	Description
voice class aaa	Enables dial-peer-based VoIP AAA configurations.

voice-class called-number (dial peer)

To assign a previously defined voice class called number to an inbound or outbound POTS dial peer, use the **voice-class called-number**command in dial peer configuration mode. To remove a voice class called number from the dial peer, use the **no** form of this command.

voice-class called-number [**inbound** | **outbound**] *tag*
no voice-class called-number

Syntax Description

inbound	Assigns an inbound voice class called number to the dial peer.
outbound	Assigns an outbound voice class called number to the dial peer.
tag	Digits that identify a specific voice class called number.

Command Default

No voice class called number is configured on the dial peer.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command to assign a previously defined voice class called number to a dial peer for a static H.320 secondary call dial plan. Use the **inbound** keyword for inbound POTS dial peers, and the **outbound** keyword for outbound POTS dial peers.

Note The **voice class called number** command in global configuration mode is entered without hyphens. The **voice-class called-number** command in dial peer configuration mode is entered with hyphens.

Examples

The following example shows configuration for an outbound voice class called number outbound on POTS dial peer 22:

```
dial-peer voice 22 pots
 voice-class called-number inbound 300
```

Related Commands

Command	Description
voice class called number	Defines a voice class called number or range of numbers for H.320 calls.
voice-class called-number-pool	Defines a pool of dynamic voice class called numbers for a voice port.

voice-class called-number-pool

To assign a previously defined voice class called number pool to a voice port, use the **voice-class called-number-pool** command in voice class configuration mode. To remove a voice class called number pool from the voice port, use the **no** form of this command.

voice-class called-number-pool *tag*
no voice-class called-number-pool

Syntax Description

tag	Digits that identify a specific voice class called number pool.

Command Default

No voice class called number pool is assigned to the voice port.

Command Modes

Voice class configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command to assign a voice class called number pool to a voice port for a dynamic H.320 secondary call dial plan.

Examples

The following example shows configuration for voice class called number pool 100 on voice port 1/0/0:

```
voice-port 1/0/0
 voice-class called-number-pool 100
```

Related Commands

Command	Description
voice class called number	Defines a voice class called number or range of numbers for H.320 calls.
voice-class called-number (dial peer)	Defines a called number or range of called numbers for a POTS dial peer.

voice-class codec (dial peer)

To assign a previously configured codec selection preference list (codec voice class) to a VoIP dial peer, enter the **voice-class codec** command in dial-peer configuration mode. To remove the codec preference assignment from the dial peer, use the **no** form of this command.

voice-class codec *tag* [**offer-all**]
no voice-class codec

Syntax Description

tag	Unique number assigned to the voice class. The range is from 1 to 10000. • This tag number maps to the tag number created using the **voice class codec**command available in global configuration mode.
offer-all	(Optional) Adds all the configured codecs from the voice class codec to the outgoing offer from the Cisco Unified Border Element (Cisco UBE).

Command Default

Dial peers have no codec voice class assigned.

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
12.0(2)XH	This command was introduced in Cisco IOS Release 12.0(2)XH and implemented on the Cisco AS5300 series routers.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T and implemented on the Cisco 2600 series and the Cisco 3600 series.
12.0(7)XK	This command was integrated into Cisco IOS Release 12.0(7)XK and implemented on the Cisco MC3810.
15.1(2)T	This command was modified. The **offer-all** keyword was added.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

You can assign one voice class to each VoIP dial peer. If you assign another voice class to a dial peer, the last voice class assigned replaces the previous voice class.



Note The **voice-class codec** command in dial-peer configuration mode is entered with a hyphen. The **voice class codec** command in global configuration mode is entered without a hyphen.

Examples

The following example shows how to assign a previously configured codec voice class to a dial peer:

```
Router# configure terminal

Router(config)# dial-peer voice 100 voip
Router(config-dial-peer)# voice-class codec 10 offer-all
```

Related Commands

Command	Description
show dial-peer voice	Displays the configuration for all dial peers configured on the router.
test voice port detector	Defines the order of preference in which network dial peers select codecs.
voice class codec	Enters voice-class configuration mode and assigns an identification tag number for a codec voice class.

voice-class h323 (dial peer)

To assign an H.323 voice class to a VoIP dial peer, use the voice-class h323 command in dial-peer configuration mode. To remove the voice class from the dial peer, use the **no** form of this command.

voice-class h323 *tag*
no voice-class h323 *tag*

Syntax Description

tag	Unique number to identify the voice class. Range is from 1 to 10000.

Command Default

The dial peer does not use an H.323 voice class.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

The voice class that you assign to the dial peer must be configured using the voice class h323 in global configuration mode.

You can assign one voice class to each VoIP dial peer. If you assign another voice class to a dial peer, the last voice class assigned replaces the previous voice class.

The voice-class h323 command in dial-peer configuration mode includes a hyphen and in global configuration mode does not include a hyphen.

Examples

The following example demonstrates how a voice class is created and applied to an individual dial peer. Voice class 4 contains a command to disable the capability to detect Cisco CallManager systems in the network (this command is used by Cisco CallManager Express 3.1 and later versions). The example then uses the **voice-class h323**command to apply voice class 4 to dial peer 36.

```
Router(config)# voice class h323 4
Router(config-class)# no telephony-service ccm-compatible
Router(config-class)# exit
Router(config)# dial-peer voice 36 voip
Router(config-dial-peer)# destination-pattern 555....
Router(config-dial-peer)# session target ipv4:10.5.6.7

Router(config-dial-peer)# voice-class h323 4
```

Related Commands

Command	Description
show dial-peer voice	Displays the configuration for all dial peers configured on the router.
voice class h323	Enters voice-class configuration mode and assigns an identification tag number for an H.323 voice class.

voice-class permanent (dial-peer)

To assign a previously configured voice class for a Cisco trunk or FRF.11 trunk to a network dial peer, use the **voice-class permanent** command in dial-peer configuration mode. To remove the voice-class assignment from the network dial peer, use the **no** form of this command.

voice-class permanent *tag*
no voice-class permanent *tag*

Syntax Description

tag	Unique number assigned to the voice class. The *tag* number maps to the tag number created using the **voice class permanent** global configuration command. Range is from 1 to 10000.

Command Default

Network dial peers have no voice class assigned.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

You can assign one voice class to any given network dial peer. If you assign another voice class to a dial peer, the last voice class assigned replaces the previous voice class.

You cannot assign a voice class to a plain old telephone service (POTS) dial peer.

The **voice-class permanent**command in dial-peer configuration mode is entered with a hyphen. The **voice class permanent**command in global configuration mode is entered without a hyphen.

Examples

The following example assigns a previously configured voice class to a Voice over Frame Relay (VoFR) network dial peer:

```
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Configures the ABCD bit pattern for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal timing oos	Configures the signal timing parameter for the OOS state of a call.

Command	Description
signal-type	Sets the signaling type for a network dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.

voice-class permanent (voice-port)

To assign a previously configured voice class for a Cisco trunk or FRF.11 trunk to a voice port, use the **voice-class permanent** command in voice-port configuration mode. To remove the voice-class assignment from the voice port, use the **no** form of this command.

voice-class permanent *tag*
no voice-class permanent *tag*

Syntax Description

tag	Unique number assigned to the voice class. The *tag* number maps to the tag number created using the **voice class permanent** global configuration command. Range is 1 to 10000.

Command Default

Voice ports have no voice class assigned.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented as a voice-port configuration command on Cisco 2600 series and Cisco 3600 series routers.

Usage Guidelines

You can assign one voice class to any given voice port. If you assign another voice class to a voice port, the last voice class assigned replaces the previous voice class.

The **voice-class permanent**command in voice-port configuration mode is entered with a hyphen. The **voice class permanent**command in global configuration mode is entered without a hyphen.

Examples

The following example assigns a previously configured voice class to voice port 1/1/0:

```
voice-port 1/1/0
 voice-class permanent 10
```

Related Commands

Command	Description
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Configures the ABCD bit pattern for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal timing oos	Configures the signal timing parameter for the OOS state of a call.
signal-type	Sets the signaling type for a network dial peer.

Command	Description
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.

voice-class sip anat

To enable Alternative Network Address Types (ANAT) on a Session Initiation Protocol (SIP) trunk, use the **voice-class sip anat** command in SIP configuration or dial peer configuration mode. To disable ANAT on SIP trunks, use the **no** form of this command.

voice-class sip anat [**system**]
no voice-class sip anat [**system**]

Syntax Description

system	(Optional) Configures ANAT globally.

Command Default

ANAT is enabled on SIP trunks.

Command Modes

SIP configuration (conf-serv-sip)
Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

Both the Cisco IOS SIP gateway and Cisco Unified Border Element are required to support the Session Description Protocol (SDP) ANAT semantics. The **bind** command allows the use of ANAT semantics in outbound SDP. SDP ANAT semantics are intended to address scenarios that involve different network address families (for example, different IPv4 versions). Media lines grouped using ANAT semantics provide alternative network addresses of different families for a single logical media stream. The entity creating a session description with an ANAT group must be ready to receive or send media over any of the grouped "m" lines.

By default, ANAT is enabled on SIP trunks. However, if the SIP gateway is configured in IPv4-only mode or IPv6-only mode, the gateway will not use ANAT semantics in its SDP offer.

The **system** keyword configures ANAT on all network dial peers, including the local dial peer. Using the **voice-class sip anat** command without the **system** keyword enables ANAT only for the local dial peer.

Examples

The following example globally enables ANAT on a SIP trunk:

```
Router(config-serv-sip)# voice-class sip anat system
```

The following example enables ANAT on a specified dial peer:

```
Router(config-dial-peer)# voice-class sip anat
```

Related Commands

Command	Description
bind	Binds the source address for signaling and media packets to the IPv4 or IPv6 address of a specific interface.

voice-class sip asserted-id

To enable support for the dial-peer-based asserted ID header in incoming Session Initiation Protocol (SIP) requests or response messages, and to send asserted ID privacy information in outgoing SIP requests or response messages, use the **voice-class sip asserted-id** command in dial-peer configuration mode. To disable the support for the asserted ID header, use the **no** form of this command.

voice-class sip asserted-id {**pai** | **ppi** | **system**}
no voice-class sip asserted-id

Syntax Description

pai	(Optional) Enables the P-Asserted-Identity (PAI) privacy header in incoming and outgoing SIP requests or response messages.
ppi	(Optional) Enables the P-Preferred-Identity (PPI) privacy header in incoming SIP requests and outgoing SIP requests or response messages.
system	(Optional) Uses global-level configuration settings to configure the dial peer.

Command Default

The privacy information is sent using the Remote-Party-ID (RPID) header or the FROM header.

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(3)T	This command was modified. Support for incoming calls was added.

Usage Guidelines

If you choose the **pai** keyword or the **ppi** keyword for incoming messages, the gateway builds the PAI or the PPI header, respectively, into the common SIP stack, thereby sending the call data using the PAI or the PPI header. For outgoing messages, the privacy information is sent on the PAI or PPI header. The **pai** keyword or the **ppi** keyword has priority over the Remote-Party-ID (RPID) header, and removes the RPID/FROM header from the outbound message, even if the router is configured to use the RPID header at the global level.

Examples

The following example shows how to enable support for the PPI header:

```
Router> enable
Router# configure terminal
Router(config)# dial peer voice 1
Router(conf-voi-serv)# voice-class sip asserted-id ppi
```

Related Commands

Command	Description
asserted-id	Enables support for the asserted ID header in incoming and outgoing SIP requests or response messages at the global level.
calling-info pstn-to-sip	Specifies calling information treatment for PSTN-to-SIP calls.

Command	Description
privacy	Sets privacy in support of RFC 3323.

voice-class sip associate registered-number

To associate the preloaded route and outbound proxy details to the registered number in the dail peer configuration mode, use the **voice-class sip associate registered-number**command in dial peer configuration mode. To remove the association, use the **no** form of this command.

voice-class sip associate registered-number *number* [**system**]
no voice-class sip associate registered-number

Syntax Description

number	Registered number. The number must be between 4 and 32.
system	(Optional) Configures the association globally.

Command Default

The preloaded route and outbound proxy details are not associated by default.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **voice-class sip associate registered-number**command takes precedence over the **associate registered-number**command in voice service VOIP SIP configuration mode. However, if the **voice-class sip associate registered-number** command is used with the **system** keyword, the gateway uses the settings configured globally by the **associate registered-number**command.

Examples

The following example shows how to associate a registered number on dial peer.

```
Router> enable

Router# configure
 terminal
Router(config)# dial-peer voice 2611 voip
Router(config-dial-peer)# voice-class sip associate registered-number 20
```

Related Commands

Command	Description
associate registered- number	Associates the preloaded route and outbound proxy details with the registered number in voice service VoIP SIP configuration mode.

voice-class sip asymmetric payload

To configure dynamic Session Initiation Protocol (SIP) asymmetric payload support on a dial peer, use the **voice-class sip asymmetric payload**command in dial peer configuration mode. To disable the configuration, use the **no** form of this command.

voice-class sip asymmetric payload {**dtmf** | **dynamic-codecs** | **full** | **system**}
no voice-class sip asymmetric payload

Syntax Description

dtmf	Provides asymmetric support only for dual-tone multi-frequency (DTMF) payloads.
dynamic-codecs	Provides asymmetric support only for dynamic codec payloads.
full	Provides asymmetric support both for DTMF and dynamic codec payloads.
system	(Optional) Specifies that the asymmetric payload uses the global value.

Command Default

Disabled (dynamic SIP asymmetric payload support is not enabled).

Command Modes

Dial peer (config-dial-peer)

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS Release IOS XE 3.1S

Usage Guidelines

For the Cisco UBE the SIP asymmetric payload-type is supported for audio/video codecs, DTMF, and NSE. Hence, **dtmf** and **dynamic-codecs** keywords are internally mapped to the **full** keyword to provide asymmetric payload-type support for audio/video codecs , DTMF, and NSE.

Examples

The following example shows how to configure dynamic SIP asymmetric payload support:

```
Router# configure terminal

Router(config)# dial-peer voice 77 voip

Router(config-dial-peer)# voice-class sip asymmetric payload full
```

Related Commands

Command	Description
dial-peer voice	Defines a particular dial peer, specifies the method of voice encapsulation, and enters dial peer configuration mode.

voice-class sip audio forced

To allow only audio and image (for T.38 Fax) media types, and drop all other media types (such as video and application), use the **voice-class sip audio forced** command in dial-peer configuration mode. To disable, use **no** form of this command.

voice-class sip audio forced [system]
no voice-class sip audio forced

Syntax Description

system	(Optional) Uses the global configuration settings to allow only audio and image (for T.38 Fax) media types.

Command Default

Support for audio forced at dial-peer level uses the global configuration level settings.

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
Cisco IOS 15.6(2)T	This command was introduced.
Cisco IOS XE Denali 16.3.1	This command was integrated into Cisco IOS XE Denali 16.3.1.

Usage Guidelines

Use **voice-class sip audio forced** command on the dial-peer when a particular remote end does not support receiving any video or application m-lines in SDP.

Example

```
Router> enable
 Router# configure terminal
 Router(config)# dial-peer voice 1 voip
 Router(config-dial-peer)# voice-class sip audio forced
```

voice-class sip authenticate redirecting-number

To supersede global settings and enable a dial peer on a Cisco IOS voice gateway to authenticate and pass Session Initiation Protocol (SIP) credentials based on the redirecting number of forwarded calls, use the **voice-class sip authenticate redirecting-number** command in dial peer voice configuration mode. To supersede global settings and specify that a dial peer uses only the calling number of forwarded calls, use the **no** form of this command. To return a dial peer to the default setting so that the dial peer uses the global setting, use the **default** form of this command.

voice-class sip authenticate redirecting-number [**system**]
no voice-class sip authenticate redirecting-number
default voice-class sip authenticate redirecting-number

Syntax Description

system	(Optional) Specifies that the dial peer use whatever setting is configured at the global (voice service SIP) command level (default).

Command Default

The dial peer uses the global setting. If the global setting is not specifically configured, the dial peer uses only the calling number of a forwarded call for SIP credentials even when the redirecting number is available for that call.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

When an INVITE message sent out by the gateway is challenged, it must respond with the appropriate SIP credentials before the call is established. The default global behavior for the gateway is to authenticate and pass SIP credentials based on the calling number and all dial peers on a gateway default to the global setting. However, for forwarded calls, it is sometimes more appropriate to use the redirecting number and this can be specified at either the global or dial peer level (configuring behavior for a specific dial peer supersedes the global setting).

Use the **voice-class sip authenticate redirecting-number** command in dial peer voice configuration mode to supersede global settings and enable a dial peer to authenticate and pass SIP credentials based on the redirecting number when available. Use the **no** form of this command to supersede global settings and force a dial peer to authenticate and pass SIP credentials based only on the calling number of forwarded calls. Use the **default** form of this command to configure the dial peer to use the global setting.

The redirecting number is present only in the headers of forwarded calls. When the **voice-class sip authenticate redirecting-number** command is disabled or the redirecting number is not available, the dial peer passes SIP credentials that are based on the calling number of the forwarded call. This is also the behavior on dial peers that are configured to use the global setting and the global setting is disabled (default). To enable the global setting (which is used as the default setting for all dial peers on the gateway), use the **authenticate redirecting-number** command in voice service SIP configuration mode.

Examples

The following example shows how to enable dial peer 2 to authenticate and pass SIP credentials based on the redirecting number (if available) of a forwarded call when a SIP INVITE message is challenged:

```
Router> enable

Router# configure
 terminal
Router(config)# dial-peer voice 2 voip

Router(config-dial-peer)# voice-class sip authenticate redirecting-number
```

The following example shows how to force dial peer 2 to authenticate and pass only the calling number of a call even when the global setting is enabled and a redirecting number is available for a call:

```
Router> enable
Router# configure
 terminal
Router(config)# dial-peer voice 2 voip
Router(config-dial-peer)# no voice-class sip authenticate redirecting-number
```

The following two examples show different ways of setting dial peer 2 to the default setting so that it authenticates and passes either the redirecting or calling number of a call based on the global (system) setting for the gateway:

```
Router> enable
Router# configure
 terminal
Router(config)# dial-peer voice 2 voip
Router(config-dial-peer)# default voice-class sip authenticate redirecting-number
Router> enable
Router# configure
 terminal
Router(config)# dial-peer voice 2 voip
Router(config-dial-peer)# voice-class sip authenticate redirecting-number system
```

Related Commands

Command	Description
authenticate redirecting-number	Enables a Cisco IOS voice gateway to authenticate and pass SIP credentials based on the redirecting number when available instead of the calling number of a forwarded call.

voice-class sip bind

To bind the source address of a specific interface for a dial-peer on a Session Initiation Protocol (SIP) trunk, use the **voice-class sip bind** command in dial peer voice configuration mode. To disable bind at the dial-peer level or restore the bind to the global level, use the **no** form of this command.

voice-class sip bind { **control** | **media** | **all** } **source-interface** *interface-id* [**ipv6-address** *ipv6-address*]
no voice-class sip bind { **control** | **media** | **all** }

Syntax Description

control	Binds Session Initiation Protocol (SIP) signaling packets.
media	Binds only media packets.
all	Binds SIP signaling and media packets.
source interface *interface-id*	Specifies an interface as the source address of SIP packets.
ipv6-address *ipv6-address*	(Optional) Configures the IPv6 address of the interface.

Command Default

Bind is disabled.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Amsterdam 17.3.1a	Introduced support for YANG models.

Usage Guidelines

Use the **voice-class sip bind** command in dial peer voice configuration mode to bind the source address for signaling and media packets to the IP address of an interface on Cisco IOS voice gateway.

You can configure multiple IPv6 addresses for an interface and select one address using the ipv6-address keyword.

Examples

The following example shows how to configure SIP bind command:

```
Router(config)# dial-peer voice 101 voip
Router(config-dial-peer)# session protocol sipv2
Router(config-dial-peer)# voice-class sip bind control source-interface GigabitEthernet0/0
 ipv6-address 2001:0DB8:0:1::1
Router(config-dial-peer)# voice-class sip bind media source-interface GigabitEthernet0/0
Router(config-dial-peer)# voice-class sip bind all source-interface GigabitEthernet0/0
```

voice-class sip block

To configure an individual dial peer on a Cisco IOS voice gateway or Cisco Unified Border Element (Cisco UBE) to drop (not pass) specific incoming Session Initiation Protocol (SIP) provisional response messages, use the **voice-class sip block** command in dial peer voice configuration mode. To disable a configuration to drop incoming SIP provisional response messages on an individual dial peer, use the **no** form of this command.

voice-class sip block {**180** | **181** | **183**} [**sdp** {**absent** | **present**} | **system**]
no voice-class sip block {**180** | **181** | **183**}

Syntax Description

180	Specifies that incoming SIP 180 Ringing messages should be dropped (not passed to the other leg).
181	Specifies that incoming SIP 181 Call is Being Forwarded messages should be dropped (not passed to the other leg).
183	Specifies that incoming SIP 183 Session in Progress messages should be dropped (not passed to the other leg).
sdp	(Optional) Specifies that either the presence or absence of Session Description Protocol (SDP) information in the received response determines when the dropping of specified incoming SIP messages takes place.
absent	Configures the SDP option so that specified incoming SIP messages are dropped only if SDP is absent from the received provisional response.
present	Configures the SDP option so that specified incoming SIP messages are dropped only if SDP is present in the received provisional response.
system	Configures the dial peer to use global configuration settings for dropping incoming SIP provisional response messages.

Command Default

Defaults to the global configuration setting, which, when not specifically configured, means incoming SIP 180, 181, and 183 provisional responses are forwarded.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)YB	This command was introduced. Only SIP 180 and SIP 183 messages are supported on Cisco UBEs.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.0(1)XA	This command was modified. Support was added for SIP 181 messages on the Cisco IOS SIP gateway, SIP-SIP Cisco UBEs, and the SIP trunk of Cisco Unified Communications Manager Express (Cisco Unified CME).
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Release	Modification
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

Use the **voice-class sip block** command in dial peer voice configuration mode to configure a specific dial peer on a Cisco IOS voice gateway or Cisco UBE to override global settings and drop specified SIP provisional response messages. Additionally, you can use the **sdp** keyword to further control when the specified SIP message is dropped based on either the absence or presence of SDP information.

You can also use the **system** keyword to configure a specific dial peer to use global configuration settings for dropping incoming SIP provisional response messages. To configure global settings on a Cisco IOS voice gateway or Cisco UBE, use the **block** command in voice service SIP configuration mode. To disable configurations for dropping specified incoming SIP messages on an individual dial peer, use the **no voice-class sip block** command in dial peer voice configuration mode.

Note This command is supported only on outbound dial peers--it is nonoperational if configured on inbound dial peers. You should configure this command on the outbound SIP leg that sends out the initial INVITE message. Additionally, this feature applies only to SIP-to-SIP calls and will have no effect on H.323-to-SIP calls.

Examples

The following example shows how to configure dial peer 1 to override any global configurations and drop specified incoming SIP provisional response messages regardless whether SDP is present:

```
Router> enable
Router# configure
 terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip block 181
```

The following example shows how to configure dial peer 1 to override any global configurations and drop specified incoming SIP provisional response messages only if SDP is present:

```
Router> enable
Router# configure
 terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip block 183 sdp present
```

The following example shows how to configure dial peer 1 to override any global configurations and drop incoming SIP provisional response messages only when SDP is not present:

```
Router> enable
Router# configure
 terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip block 180 sdp absent
```

The following example shows how to configure a dial peer to use the global configuration settings for dropping incoming SIP provisional response messages:

```
Router> enable
Router# configure
 terminal
```

```
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip block 181 system
```

The following example shows how to configure a dial peer to pass all incoming SIP provisional response messages regardless of global configuration settings:

```
Router> enable
Router# configure
 terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# no voice-class sip block 180
```

Related Commands

Command	Description
block	Configures global configuration for dropping specified SIP provisional response messages on a Cisco IOS voice gateway or Cisco UBE.
map resp-code	Configures global settings on a Cisco UBE for mapping specific incoming SIP provisional response messages to a different SIP response message.
voice-class sip map resp-code	Configures a specific dial peer on a Cisco UBE to map specific incoming SIP provisional response messages to a different SIP response message.

voice-class sip call-route

To enable call routing based on the Destination-Route-String, P-called-party-id and History-Info header values at the dial-peer configuration level, use the **voice-class sip call-route** command in dial peer voice configuration mode. To disable Header-based routing, use the **no** form of this command.

voice-class sip call-route {**dest-route-string** | **p-called-party-id** | **history-info** | **url**} [**system**]
no voice-class sip call-route {**dest-route-string** | **p-called-party-id** | **history-info** | **url**}

Syntax Description

dest-route-string	Enables call routing based on the Destination-Route-String.
p-called-party-id	Enables call routing based on the P-Called-Party-Id header.
history-info	Enables call routing based on the History-Info header.
url	Enables call routing based on the URL.
system	(Optional) Uses the global configuration settings to enable call routing based on the header values on this dial peer.

Command Default

Support for call routing based on the Destination-Route-String, P-Called-Party-Id, History-Info headers and URL at the dial peer level is disabled.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(2)T	This command was modified. The **history-info** keyword was added.
15.2(1)T	This command was modified. The **url** keyword was added.
15.3(3)M	This command was modified. The **dest-route-string** keyword was added.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S.

Usage Guidelines

Use the **voice-class sip call-route** command on the inbound dial peer to enable the gateway to route calls based on the received header in a received INVITE message.

The **voice-class sip call-route** command takes precedence over the **call-route** command in voice service VoIP SIP configuration mode. However, if the **voice-class sip call-route** command is used with the **system** keyword, the gateway uses the settings configured globally by the **call-route** command.

If multiple call routes are configured, call routing enabled based on destination route string takes precedence over other header configurations. Destination route string configuration is applicable only for outbound dial-peer matching.

Examples

The following example shows how to enable call routing based on the Destination-Route-String, P-Called-Party-Id, History-Info header values and URL at the dial peer configuration level:

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 2611 voip
Device(config-dial-peer)# voice-class sip call-route dest-route-string
Device(config-dial-peer)# voice-class sip call-route p-called-party-id
Device(config-dial-peer)# voice-class sip call-route history-info
Device(config-dial-peer)# voice-class sip call-route url
```

Related Commands

Command	Description
call-route	Enables call routing based on the Destination-Route-String, P-Called-Party-Id and History-Info header values at the global configuration level.

voice-class sip calltype-video

To configure the bearer capability setting on an H.320 dial peer so that it supports unrestricted digital media, use the **voice-class sip calltype-video** command in dial peer voice configuration mode. To return the bearer capability setting for an H.320 dial peer to the default, use the **no** form of this command.

voice-class sip calltype-video
no voice-class sip calltype-video

Syntax Description

This command has no arguments or keywords.

Command Default

Bearer capability setting for support of unrestricted digital media support is disabled.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

H.320 dial peers support only voice calls by default. Use the **voice-class sip calltype-video** command to configure the bearer capability setting, which enables support of unrestricted digital media calls on an H.320 dial peer.

Examples

The following example shows how to configure the bearer capability setting on dial peer 2 so that it supports unrestricted digital media:

```
Router> enable

Router# configure
 terminal
Router(config)# dial-peer voice 2 voip

Router(config-dial-peer)# voice-class sip call-type video
```

voice-class sip content sdp version increment

To increment the SDP version for any RE-INVITE with SDP change even if the previous offer sent by CUBE was rejected, use **voice-class sip content sdp version increment** command in dial-peer configuration mode.

voice-class sip content sdp version increment {**system**}

system	Uses the system level configuration for sdp version increment

Command Default

SDP version will not be incremented for any RE-INVITE with SDP change even if the previous offer sent by CUBE was rejected.

Command Modes

dial-peer configuration mode (config-dial-peer)

Command History

Release	Modification
Cisco IOS 15.5(2)T	This command was introduced.
Cisco IOS XE 3.15	

Usage Guidelines

Use **voice-class sip content sdp version increment** command to increment the SDP version for any RE-INVITE with SDP change even if the previous offer sent by CUBE was rejected.

Example

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 1 voip
Device(config-dial-peer)# voice-class sip content sdp version increment
```

voice-class sip copy-list

To configure a list of entities to be sent to the peer call leg on a dial peer, use the **voice-class sip copy-list**command in dial peer configuration mode. To disable the configuration, use the **no** form of this command.

voice-class sip copy-list {*tag* | **system**}
no voice-class sip copy-list

Syntax Description

tag	Tag number of the Session Initiation Protocol (SIP) copy list. The range is from 1 to 10000.
system	Specifies to use the global level configuration to copy the list.

Command Default

Entries configured at the global level are sent to the peer call leg.

Command Modes

Dial peer configuration (config-dial-peer)

Voice class tenant

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use the **voice-class sip copy-list** command to configure Cisco Unified Border Element (UBE) to pass an unsupported parameter present in a mandatory header from one peer call leg to another. You can copy the inbound message headers into variables and pass the headers to the outbound peer call leg.

Examples

The following example shows how to configure a SIP list to be sent to the peer call leg:

```
Router(config)# dial-peer voice 66 voip
Router(config-dial-peer)# voice-class sip copy-list 4
```

Related Commands

Command	Description
voice class sip-copylist	Configures a list of entities to be sent to the peer call leg.

voice-class sip e911

To enable SIP E911 system services on a dial peer, use the **voice-class sip e911**command in VoIP dialpeer configuration mode. To disable SIP E911 services, use the **no** form of this command.

voice-class sip e911
no voice-class sip e911

Syntax Description

This command has no arguments or keywords.

Command Default

The dial peer uses the global setting.

Command Modes

VoIP dialpeer configuration mode.

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

The **no** form of this command sets the dial peer configuration to disable, which indicates that E911 will not be used for this peer. Because the **no** version of the command causes non default behavior, it can been seen in the **show running-config** output. See also the **voice service voip sip e911** and **debug csm neat** commands.

Examples

The following examples enable and disable E911 services on a VoIP dial peer:

```
Router(config)# dial-peer voice 2
Router(config-dial-peer)# voice-class sip e911
*Jun 06 00:47:20.611: setting peer 2 to enable
Router(config-dial-peer)# no voice-class sip e911

*Jun 06 00:49:58.931: setting peer 2 to disable
```

Related Commands

Command	Description
debug csm neat	Turns on debugging for all Call Switching Module (CSM) Voice over IP (VoIP) calls.
show running-config	Displays the running configuration.
e911	Enables E911 system services for SIP voice service VoIP.

voice-class sip-event-list

To configure lists of SIP events to be passed through. To disable this feature, use the **no** form of this command.

voice-class sip-event-list *tag*
no voice-class sip-event-list *tag*

Syntax Description

tag	Event list tag. Range is 1-10000.

Command Default

No default value.

Command Modes

Global configuration (config).

Voice class tenant configuration (config-class).

Command History

Release	Modification
Cisco IOS XE 3.11S	The command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use this command for troubleshooting to determine which SIP event was configured as passed through. To set the sip event, use the **voice class sip-event-list** command.

To set the voice class sip-event-list in the dial peer, use the **voice-class sip pass-thru subscribe-notify-events <event id | all>** command.

To set the voice class sip-event-list in the voice service VoIP under sip, use the **pass-thru subscribe-notify-events <event id | all>** command.

To set the voice class sip-event-list in the voice class tenant, use the **pass-thru subscribe-notify-events <event id | all>** command.

Examples

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#voice class sip-event-list 12
Router(config-class)#event ?
  WORD  name of event to be added in event list
Router(config-class)#event sipevent1
Router(config-class)#event sipevent2
```

Related Commands

Command	Description

voice-class sip early-media update block

To block the UPDATE requests with SDP in an early dialog, use **voice-class sip early-media update block** command in dial-peer configuration mode. To disable, use **no** form of this command.

voice-class sip early-media update block [**re-negotiate**]
no voice-class sip early-media update block [**re-negotiate**]

Syntax Description

re-negotiate	Enables end to end renegotiation if the UPDATE request contains changes in caller ID, transcoder addition or deletion, or video escalation or de-escalation.

Command Default

CUBE allows pass-through of early dialog UPDATE requests from one user agent to the other.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
Cisco IOS 15.5(3)M, Cisco IOS-XE 3.16S	This command was introduced.

Usage Guidelines

Use **voice-class sip early-media update block** command on the dial-peer where you want to block the Early Dialog UPDATE requests.

Use **re-negotiate** keyword to enable end to end renegotiation if the UPDATE request contains changes in caller ID, transcoder addition or deletion, or video escalation or de-escalation.

Examples

The following example shows early dialog update block being configured in dial-peer configuration mode:

```
Router(config-dial-peer)# voice-class sip early-media update block
```

voice-class sip encap clear-channel

To enable RFC 4040-based clear-channel codec negotiation for Session Initiation Protocol (SIP) calls on an individual dial peer, overriding the global setting on a Cisco IOS voice gateway or Cisco Unified Border Element (Cisco UBE), use the **voice-class sip encap clear-channel** command in dial peer voice configuration mode. To disable RFC 4040-based clear-channel codec negotiation on an individual dial peer for SIP calls on a Cisco IOS voice gateway or Cisco UBE, use the **no** form of this command.

voice-class sip encap clear-channel [**standard** | **system**]
no voice-class sip encap clear-channel standard

Syntax Description

standard	(Optional) Specifies standard RFC 4040 encapsulation.
system	(Optional) Configures the dial peer to use global configuration settings for clear-channel codec negotiation.

Command Default

The dial peer uses the system configuration. (If the global **encap clear-channel standard** command is not enabled, then legacy encapsulation [X-CCD/8000] is used for clear-channel codec negotiation.)

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.0(1)XA	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

Use the **voice-class sip encap clear-channel standard** command in dial peer voice configuration mode to override global settings for clear-channel codec negotiation on a Cisco IOS voice gateway or Cisco UBE and enable RFC 4040-based clear-channel codec negotiation [CLEARMODE/8000] for SIP calls on a specific dial peer. RFC 4040-based clear-channel codec negotiation allows dial peers on Cisco IOS voice gateways and Cisco UBEs to successfully interoperate with third-party SIP gateways that do not support legacy Cisco IOS clear-channel codec encapsulation [X-CCD/8000].

When the **voice-class sip encap clear-channel standard** command is enabled on a specific dial peer on a Cisco IOS voice gateway or Cisco UBE, SIP calls on that dial peer that use the Cisco IOS clear channel codec are translated into calls that use [CLEARMODE/8000] regardless of the global configuration so that the calls do not get rejected when they reach third-party SIP gateways.

You can also use the **voice-class sip encap clear-channel system** command to configure a specific dial peer to use global configuration settings for clear-channel codec negotiation. To enable RFC 4040 clear-channel codec negotiation for SIP calls globally on a Cisco IOS voice gateway or Cisco UBE, use the **encap clear-channel standard** command in voice service SIP configuration mode. To override global settings and disable RFC 4040-based clear-channel codec negotiation on a specific dial peer, use the **no voice-class sip encap clear-channel standard** command in dial peer voice configuration mode.

Examples

The following example shows how to configure dial peer 1 to override any global configurations and enable RFC 4040-based clear-channel codec negotiation for SIP calls:

```
Router> enable
Router# configure
 terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip encap clear-channel standard
```

The following example shows how to configure dial peer 1 to use the global configuration for clear-channel codec negotiation for SIP calls:

```
Router> enable
Router# configure
 terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip encap clear-channel system
```

Related Commands

Command	Description
encap clear-channel standard	Enables RFC 4040-based clear-channel codec negotiation for SIP calls globally on a Cisco IOS voice gateway or Cisco UBE.



voice-class sip error-code-override through vxml version 2.0

- voice-class sip error-code-override, on page 370
- voice-class sip g729 annexb-all, on page 373
- voice-class sip history-info, on page 375
- voice-class sip localhost, on page 376
- voice-class sip map resp-code, on page 378
- voice-class sip midcall-signaling, on page 380
- voice-class sip nat media-keepalive, on page 382
- voice-class sip options-keepalive, on page 384
- voice-class sip options-keepalive profile, on page 386
- voice-class sip outbound-proxy, on page 387
- voice-class sip preloaded-route, on page 389
- voice-class sip privacy, on page 390
- voice-class sip privacy-policy, on page 393
- voice-class sip random-contact, on page 395
- voice-class sip random-request-uri validate, on page 397
- voice-class sip referto-passing, on page 399
- voice-class sip registration passthrough, on page 400
- voice-class sip rel1xx, on page 402
- voice-class sip requri-passing, on page 404
- voice-class sip reset timer expires, on page 405
- voice-class sip resource priority dscp-profile, on page 407
- voice-class sip resource priority mode (dial-peer), on page 408
- voice-class sip resource priority namespace (dial-peer), on page 409
- voice-class sip rsvp-fail-policy, on page 411
- voice-class sip send 180 sdp, on page 413
- voice-class sip srtp-auth, on page 414
- voice-class sip srtp-crypto, on page 416
- voice-class sip srtp negotiate, on page 418
- voice-class sip tel-config to-hdr, on page 420
- voice-class sip tenant, on page 421
- voice-class sip transport switch, on page 422

- voice-class sip url, on page 423
- voice-class source interface, on page 425
- voice-class stun-usage, on page 426
- voice-class tone-signal, on page 427
- voice-ctl-file, on page 428
- voice confirmation-tone, on page 429
- voice dnis-map, on page 430
- voice dnis-map load, on page 432
- voice dsp crash-dump, on page 433
- voice dsp invalid-msg drop, on page 435
- voice echo-canceller extended, on page 436
- voice enum-match-table, on page 439
- voice hpi capture, on page 441
- voice hunt, on page 443
- voice iec syslog, on page 448
- voice local-bypass, on page 449
- voice mlpp, on page 450
- voicemail (stcapp-fsd), on page 451
- voice pcm capture, on page 453
- voice-phone-proxy, on page 455
- voice-phone-proxy file-buffer, on page 456
- voice-phone-proxy tftp-address, on page 457
- voiceport, on page 458
- voice-port, on page 460
- voice-port (MGCP profile), on page 462
- voice-port busyout, on page 463
- voice rtp send-recv, on page 464
- voice rtp source-filter, on page 465
- voice-service dsp-reservation, on page 466
- voice service, on page 467
- voice sip sip-profiles, on page 468
- voice sip oauth get-keys, on page 469
- voice source-group, on page 470
- voice statistics accounting method, on page 471
- voice statistics display-format separator, on page 473
- voice statistics field-params, on page 475
- voice statistics max-storage-duration, on page 477
- voice statistics push, on page 479
- voice statistics time-range, on page 481
- voice statistics type csr, on page 484
- voice statistics type iec, on page 486
- voice translation-profile, on page 487
- voice translation-rule, on page 488
- voice vad-time, on page 489
- voice vrf, on page 490
- voip-incoming translation-profile, on page 491

- voip-incoming translation-rule, on page 492
- voip trunk group, on page 494
- volume, on page 495
- vxml allow-star-digit, on page 497
- vxml logging-tag, on page 498
- vxml audioerror, on page 499
- vxml tree memory, on page 500
- vxml version 2.0, on page 501

voice-class sip error-code-override

To configure the Session Initiation Protocol (SIP) error code that a dial peer uses for options-keepalive failures, call spike, or cac-bandwidth failures, use the **voice-class sip error-code-override** command in dial peer voice configuration mode. To disable the SIP error code configuration, use the **no** form of this command.

voice-class sip error-code-override {**options-keepalive failure** | **call spike failure** | **cac-bandwidth failure**} {*sip-status-code-number* | **system**}
no voice-class sip error-code-override {**options-keepalive failure** | **call spike failure** | **cac-bandwidth failure**}

Syntax Description

options-keepalive failure	Configures the SIP error code for options-keepalive failures.
call spike failure	Configures the SIP error code for call spike failures.
cac-bandwidth failure	Configures the SIP error code for Call Admission Control bandwidth failures.
sip-status-code-number	The SIP status code that is sent for the options keepalive, call spike, or cac-bandwidth failure. The range is from 400 to 699. The default value is 503. The table below in the "Usage Guidelines" section describes these error codes.
system	Specifies the system configuration used for keepalive, call spike, or cac-bandwidth failures.

Command Default

By default the SIP error code is not configured.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.0(1)XA	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.1(3)T	This command was modified. The **call spike failure** keyword was added.
15.2(2)T	This command was modified. The **cac-bandwidth failure** keyword was added.

Usage Guidelines

The **voice-class sip error-code-override** command in dial peer voice configuration mode configures the error code response for keepalive options, call spike, or cac-bandwidth failures at the dial peer level. The **error-code-override** command in voice service SIP configuration mode configures the error code responses for options-keepalive, call spike, or cac-bandwidth failures globally.

The table below describes the SIP error codes.

Table 5: SIP Error Codes

Error Code Number	Description
400	Bad request
401	Unauthorized
402	Payment required
403	Forbidden
404	Not found
408	Request timed out
416	Unsupported Uniform Resource Identifier (URI)
480	Temporarily unavailable
482	Loop detected
484	Address incomplete
486	Busy here
487	Request terminated
488	Not acceptable here
500–599	SIP 5xx—server/service failure
500	Internal server error
502	Bad gateway
503	Service unavailable
600–699	SIP 6xx—global failure

Examples

The following example shows how to configure the SIP error code for options-keepalive failures using the **voice-class sip error-code-override** command:

```
Router(config)# dial-peer voice 432 voip system
Router(config-dial-peer)# voice-class sip error-code-override options-keepalive failure 502
```

The following example shows how to configure the SIP error code for call spike failures using the **voice-class sip error-code-override** command:

```
Router(config)# dial-peer voice 432 voip system
Router(config-dial-peer)# voice-class sip error-code-override call spike failure 502
```

The following example shows how to configure the SIP error code for Call Admission Control bandwidth failures:

```
Router(config)# dial-peer voice 432 voip system
Router(config-dial-peer)# voice-class sip error-code-override cac-bandwidth failure 502
```

Related Commands

Command	Description
error-code-override	Configures the SIP error code for options-keepalive, call spike, or cac-bandwidth failures in voice service SIP and dial peer voice configuration mode, respectively.

voice-class sip g729 annexb-all

To configure settings on a Cisco IOS Session Initiation Protocol (SIP) gateway that determine if a specific dial peer on the gateway treats the G.729br8 codec as superset of G.729r8 and G.729br8 codecs for interoperation with Cisco Unified Communications Manager, use the **voice-class sip g729 annexb-all** command in dial peer voice configuration mode. To prevent a dial peer from treating the G.729br8 codec as a superset of the G.729r8 and G.729br8 codecs, use the **no** form of this command.

voice-class sip g729 annexb-all [**system**]
no voice-class sip g729 annexb-all

Syntax Description

annexb-all	Specifies that the G.729br8 codec is treated as a superset of G.729r8 and G.729br8 codecs to communicate with Cisco Unified Communications Manager.
system	(Optional) Specifies that the dial peer allow communication between incompatible G.729 codecs according to global settings configured for this feature on the Cisco IOS SIP gateway.

Command Default

The dial peer defers to global (system) settings for the Cisco IOS gateway.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

There are four variations of the G.729 coder-decoder (codec), which fall into two categories:

High Complexity

- G.729 (g729r8)--a high complexity algorithm codec on which all other G.729 codec variations are based.
- G.729 Annex-B (g729br8 or G.729B)--a variation of the G.729 codec that allows the DSP to detect and measure voice activity and convey suppressed noise levels for re-creation at the other end. Additionally, the Annex-B codec includes Internet Engineering Task Force (IETF) voice activity detection (VAD) and comfort noise generation (CNG) functionality.

Medium Complexity

- G.729 Annex-A (g729ar8 or G.729A)--a variation of the G.729 codec that sacrifices some voice quality to lessen the load on the DSP. All platforms that support G.729 also support G.729A.
- G.729A Annex-B (g729abr8 or G.729AB)--a variation of the G.729 Annex-B codec that, like G.729B, sacrifices voice quality to lessen the load on the DSP. Additionally, the G.729AB codec also includes IETF VAD and CNG functionality.

The VAD and CNG functionality is what causes the instability during communication attempts between two DSPs where one DSP is configured with Annex-B (G.729B or G.729AB) and the other without (G.729 or G.729A). All other combinations interoperate. To configure a dial peer on a Cisco IOS SIP gateway for

interoperation with Cisco Unified Communications Manager (formerly known as the Cisco CallManager, or CCM), use the **voice-class sip g729 annexb-all** command in dial peer voice configuration mode to do one of the following:

- Override global settings for a Cisco IOS gateway and configure the dial peer to accept and connect calls between two DSPs with incompatible G.729 codecs.
- Specify that an individual dial peer use the global (**system**) settings on the Cisco IOS SIP gateway.
- Use the no form of the command to override global settings for the Cisco IOS gateway and specify that the dial peer does not treat the G.729br8 codec as a superset of G.729r8 and G.729br8 codecs.

Use the **g729 annexb-all** command in voice service SIP configuration mode to configure the global settings for the Cisco IOS SIP gateway.

Examples

The following example shows how to configure a dial peer on a Cisco IOS SIP gateway to connect calls between two DSPs using incompatible G.729 codecs, overriding global gateway settings for this feature:

```
Router> enable
Router# configure
 terminal
Router(config)# dial-peer
 voice 1
Router(config-dial-peer)# voice-class sip g729 annexb-all
```

Related Commands

Command	Description
g729 annexb-all	Configure global settings that determine if a Cisco IOS SIP gateway treats the G.729br8 codec as superset of G.729r8 and G.729br8 codecs.

voice-class sip history-info

To enable Session Initiation Protocol (SIP) history-info header support on the Cisco IOS gateway at the dial-peer level, use the **voice-class sip history-info** command in dial peer configuration mode. To disable SIP history-info header support, use the **no** form of this command.

voice-class sip history-info [**system**]
no voice-class sip history-info

Syntax Description

system	(Optional) Enables history-info support using global configuration settings.

Command Default

History-info header support is disabled.

Command Modes

Dial peer configuration (conf-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S

Usage Guidelines

Use this command to enable history-info header support at the dial-peer level. The history-info header (as defined in RFC 4244) records the call or dialog history. The receiving application uses the history-info header information to determine how and why the call has reached it.



Note The Cisco IOS SIP gateway cannot use the information in the history-info header to make routing decisions.

Examples

The following example enables SIP history-info header support at the dial-peer level:

```
Router(config)# dial-peer voice 2 voip
Router(config-dial-peer)# voice-class sip history-info
```

The following example enables SIP history-info header support at the dial-peer level using the global configuration settings:

```
Router(config)# dial-peer voice 2 voip
Router(config-dial-peer)# voice-class sip history-info system
```

Related Commands

Command	Description
history-info	Enables SIP history-info header support on Cisco IOS gateway at a global level.

voice-class sip localhost

To configure individual dial peers to override global settings on Cisco IOS voice gateways, Cisco Unified Border Element (Cisco UBE), or Cisco Unified Communications Manager Express (Cisco Unified CME) and substitute a Domain Name System (DNS) hostname or domain as the localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers in outgoing messages, use the **voice-class sip localhost** command in dial peer voice configuration mode. To disable substitution of a localhost name on a specific dial peer, use the **no** form of this command. To configure a specific dial peer to defer to global settings for localhost name substitution, use the **default** form of this command.

voice-class sip localhost dns:[*hostname*]*domain*[**preferred**]
no voice-class sip localhost
default voice-class sip localhost

Syntax Description

dns: [*hostname.*]*domain*	Alphanumeric value representing the DNS domain (consisting of the domain name with or without a specific hostname) in place of the physical IP address that is used in the host portion of the From, Call-ID, and Remote-Party-ID headers in outgoing messages. This value can be the hostname and the domain separated by a period (**dns:** *hostname.domain*) or just the domain name (**dns:** *domain*). In both case, the **dns:** delimiter must be included as the first four characters.
preferred	(Optional) Designates the specified DNS hostname as preferred.

Command Default

The dial peer uses the global configuration setting to determine whether a DNS localhost name is substituted in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(2)T	This command was introduced.
15.0(1)XA	This command was modified. The **preferred** keyword was added to specify the preferred localhost if multiple registrars are configured on a SIP trunk.
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

Use the **voice-class sip localhost** command in dial peer voice configuration mode to override the global configuration on Cisco IOS voice gateways, Cisco UBEs, or Cisco Unified CME and configure a DNS localhost name to be used in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages on a specific dial peer. When multiple registrars are configured for an individual dial peer you can then use the **voice-class sip localhost preferred** command to specify which host is preferred for that dial peer.

To globally configure a localhost name on a Cisco IOS voice gateway, Cisco UBE, or Cisco Unified CME, use the **localhost** command in voice service SIP configuration mode. Use the **no voice-class sip localhost** command to remove localhost name configurations for the dial peer and to force the dial peer to use the physical IP address in the host portion of the From, Call-ID, and Remote-Party-ID headers regardless of the global configuration.

Examples

The following example shows how to configure dial peer 1 (overriding any global configuration) to substitute a domain (no hostname specified) as the preferred localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages:

```
Router> enable
Router# configure
 terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip localhost dns:example.com preferred
```

The following example shows how to configure dial peer 1 (overriding any global configuration) to substitute a specific hostname on a domain as the preferred localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages:

```
Router> enable
Router# configure
 terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip localhost dns:MyHost.example.com preferred
```

The following example shows how to force dial peer 1 (overriding any global configuration) to use the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages:

```
Router> enable
Router# configure
 terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# no voice-class sip localhost
```

Related Commands

Command	Description
authentication (dial peer)	Enables SIP digest authentication on an individual dial peer.
authentication (SIP UA)	Enables SIP digest authentication.
credentials (SIP UA)	Configures a Cisco UBE to send a SIP registration message when in the UP state.
localhost	Configures global settings for substituting a DNS localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages.
registrar	Enables Cisco IOS SIP gateways to register E.164 numbers on behalf of FXS, EFXS, and SCCP phones with an external SIP proxy or SIP registrar.

voice-class sip map resp-code

To configure an individual dial peer on a Cisco Unified Border Element (Cisco UBE) to map specific received Session Initiation Protocol (SIP) provisional response messages to a different SIP provisional response message on the outgoing SIP dial peer, use the **voice-class sip map resp-code** command in dial peer voice configuration mode. To disable mapping of received SIP provisional response messages on an individual dial peer, use the **no** form of this command. To configure a specific dial peer to defer to global settings for mapping of incoming SIP provisional response messages, use the **default** form of this command.

voice-class sip map resp-code 181 to 183
no voice-class sip map resp-code 181 to 183
default voice-class sip map resp-code 181 to 183

Syntax Description

181	The code representing the specific incoming SIP provisional response messages to be mapped and replaced.
to	The designator for specifying that the specified incoming SIP provisional response message should be mapped to and replaced with a different SIP provisional response message on the outgoing SIP dial peer.
183	The code representing the specific SIP provisional response message on the outgoing dial peer to which incoming SIP message responses should be mapped.

Command Default

Mapping behavior is determined by the global configuration setting, which, if not specifically configured, means that incoming SIP provisional responses are passed, as is to the outbound SIP dial peer.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.0(1)XA	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

Use the **voice-class sip map resp-code**command in dial peer voice configuration mode to configure an individual dial peer on a Cisco UBE to map incoming SIP 181 provisional response messages to SIP 183 provisional response messages on the outgoing SIP dial peer.



Note If the **block** command is configured for incoming SIP 181 messages, either globally or at the dial-peer level, the messages may be dropped before they can be passed or mapped to a different message--even when the **voice-class sip map resp-code** command is enabled. To globally configure whether and when incoming SIP 181 messages are dropped, use the **block** command in voice service SIP configuration mode (or use the **voice-class sip block** command in dial peer voice configuration mode to configure drop settings on individual dial peers).

To configure mapping of SIP provisional response messages globally on a Cisco UBE, use the **map resp-code** command in voice service SIP configuration mode. To disable mapping of SIP 181 message for an individual dial peer on a Cisco UBE, use the **no voice-class sip map resp-code** command in voice service SIP configuration mode.

As an example, to enable interworking of SIP endpoints that do not support the handling of SIP 181 provisional response messages, you could use the **block** command to configure a Cisco UBE to drop SIP 181 provisional response messages received on the SIP trunk or you can use the **map resp-code** command to configure the Cisco UBE to map the incoming messages to and send out, instead, SIP 183 provisional response messages to the SIP line in Cisco Unified Communications Manager Express (Cisco Unified CME).



Note This command is supported only for SIP-to-SIP calls and will have no effect on H.323-to-SIP or time-division multiplexing (TDM)-to-SIP calls.

Examples

The following example shows how to configure dial peer 1 to map incoming SIP 181 provisional response messages to SIP 183 provisional response messages on the outbound dial peer:

```
Router> enable
Router# configure
 terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip map resp-code 181 to 183
```

Related Commands

Command	Description
block	Configures global settings for dropping specific SIP provisional response messages on a Cisco IOS voice gateway or Cisco UBE.
map resp-code	Configures global settings on a Cisco UBE for mapping specific incoming SIP provisional response messages to a different SIP response message.
voice-class sip block	Configures an individual dial peer on a Cisco IOS voice gateway or Cisco UBE to drop specified SIP provisional response messages.

voice-class sip midcall-signaling

To configure the method used for signaling messages, use the **voice-class sip midcall-signaling** command in SIP configuration mode or dial peer configuration mode. To disable the mid-call signaling feature, use the **no** form of this command.

voice-class sip midcall-signaling {**passthru media-change** | **block** | **preserve-codec**}
no voice-class sip midcall-signaling

Syntax Description

passthru media-change	Passes SIP messages that inolve media-change from one IP leg to another IP leg.
block	Blocks all SIP messages during mid-call.
preserve-codec	Preserves codec negotiated during call initialization. Mid-call codec change is disabled.

Command Default

Mid call-signaling is disabled. Codec negotiation in the middle of a call is enabled.

Command Modes

Dial peer configuration mode (config-dial-peer)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T. The **media-change** and **block** keywords were added.
15.3(2)S, 15.3(1)T	This command was modified. The **preserve-codec** keyword was added.

Usage Guidelines

The **voice-class sip midcall-signaling** command distinguishes between the way Cisco Unified Communications Express and Cisco Unified Border Element handle signaling messages. Most SIP-to-SIP video and SIP-to-SIP reinvite based supplementary services require the **voice-class sip midcall-signaling** command to be configured before configuring other supplementary services. Supplementary service features that are functional without configuring **voice-class sip midcall-signaling** include: session refresh, fax, and refer-based supplementary services. The **voice-class sip midcall-signaling** command is for SIP-to-SIP calls only. All other calls (H323-to-SIP, and H323-to-H323) do not require the **voice-class sip midcall-signaling**command be configured. The **allow-connections sip-to-sip** command must be configured before the **voice-class sip midcall-signaling** command.

Configuring the Session Refresh with Reinvites feature on a dial-peer basis is not supported.

Examples

The following example shows SIP messages configured to passthrough from one IP leg to another IP leg:

```
Router(config)#voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# voice-class sip midcall-signaling passthru
```

The following example shows SIP messages configured to media passthru from one IP leg to another IP leg:

```
Router(config)#voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# voice-class sip midcall-signaling passthru media-change
```

The following example shows how to block SIP messages.

```
Router(config)#voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# voice-class sip midcall-signaling block
```

The following example shows how to disable codec negotiation in the middle of a call and retains the codec negotiated at the start of the call.

```
Router(config)#voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# voice-class sip midcall-signaling preserve-codec
```

Related Commands

Command	Description
allow-connections	Allows connections between specific types of endpoints in a Cisco Unified BE.

voice-class sip nat media-keepalive

To enable media keepalive packets when the device is configured behind NAT, use the **voice-class sip nat** command in dial-peer configuration mode. To disable media, use the **no** or **default** form of this command.

voice-class sip nat media-keepalive *interval*
no voice-class sip nat
default voice-class sip nat

Syntax Description

media-keepalive	Specifies media keepalive to subscriber if it's located behind NAT.
interval	Specifies keepalive interval in seconds. Range is 1—50. Default is 10.

Command Default

By default, media-keepalive is disabled.

Command Modes

Dial-peer configuration mode (config-dial-peer)

Command History

Release	Modification
Cisco IOS XE 17.13.1a Cisco IOS XE Dublin 17.12.2	This command was introduced.

Usage Guidelines

If the dial-peer is associated with a tenant, the configurations are applied in the following order of preference:

- Dial-peer configuration
- Tenant configuration
- Global configuration

A newly created dial peer remains defined and active until you delete it with the **no** form of the **dial-peer voice** command.

Examples

The following example shows how to configure media keepalive to enable media keepalive packets to be transmitted for the interval specified in seconds:

```
Device(config)# dial-peer voice 999 voip
Device(config-dial-peer)# voice-class sip nat media-keepalive 40
```

Note The **voice-class sip nat media-keepalive** command takes affect immediately after it is applied.

Related Commands

Command	Description
nat media-keepalive	Uses the SIP Network Address Translation (NAT) global configuration.

Command	Description
voice class tenant *tag*	Associates a dial-peer with a specific tenant configuration.

voice-class sip options-keepalive

To monitor connectivity between Cisco Unified Border Element VoIP dial-peers and SIP servers to, use the **voice-class sip options-keepalive** command in dial peer configuration mode. To disable monitoring connectivity, use the **no** form of this command.

voice-class sip options-keepalive *keepalive-group-profile-id* { **up-interval** *seconds* | **down-interval** *seconds* | **retry** *retries* }
no voice-class sip options-keepalive

Syntax Description

keepalive-group-profile-id	Specifies the keepalive group profie id.
up-interval *seconds*	Number of up-interval seconds allowed to pass before marking the UA as unavailable.The range is 5-1200. The default is 60.
down-interval *seconds*	Number of down-interval seconds allowed to pass before marking the UA as unavailable.The range is 5-1200. The default is 30.
retry *retries*	Number of retry attempts before marking the UA as unavailable. The range is 1 to 10. The default is 5 attempts.

Command Default

The dial-peer is active (UP).

Command Modes

Dial peer configuration mode (config-dial-peer).

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use the **voice-class sip options-keepalive** command to configure a out-of-dialog (OOD) Options Ping mechanism between any number of destinations. When monitored endpoint heartbeat responses fails, the configured dial-peer is busied out. If there is a alternate dial-peer configured for the same destination pattern, the call is failed over to the next preference dial peer or the on call is rejected with an error cause code.

The response to options ping will be considered unsuccessful and dial-peer will be busied out for following scenarios:

Table 6: Error Codes that busyout the endpoint

Error Code	Description
503	service unavailable
505	sip version not supported
no response	i.e. request timeout

All other error codes, including 400 are considered a valid response and the dial peer is not busied out.

Examples

The following example shows a sample configuration of dial peer 100 configured to reset:

```
dial-peer voice 100 voip
  voice-class sip options-keepalive up-interval 12 down-interval 65 retry 3
```

Related Commands

Command	Description
dial-peer voice	Defines a particular dial peer and specifies the method of voice encapsulation.

voice-class sip options-keepalive profile

To associate the dial peer with the specified keepalive group profile, use the **voice-class sip options-keepalive profile** command in dial peer configuration mode.

voice-class sip options-keepalive profile *keepalive-group-profile-id*

Syntax Description

keepalive-group-profile-id	Specifies the keepalive group profile id.

Command Default

The dial-peer is active (UP).

Command Modes

Dial peer configuration mode (config-dial-peer)

Command History

Release	Modification
Cisco IOS XE Dublin 17.11.1a	This command was introduced.

Usage Guidelines

The dial peer is monitored by CUBE according to the parameters defined by options-keepalive profile.

Examples

The following example shows a sample configuration of an outbound SIP dial peer and association with a keepalive profile group:

```
dial-peer voice 123 voip
 session protocol sipv2
!
voice-class sip options-keepalive profile 171
end
```

voice-class sip outbound-proxy

To configure an outbound proxy, use the **voice-class sip outbound-proxy** command in dial peer configuration mode. To reset the outbound proxy value to its default, use the **no** form of this command.

voice-class sip outbound-proxy {**dhcp** | **ipv4:** *ipv4-address* | **ipv6:** [*ipv6-address*] | **dns:** *host: domain*} [*:port-number*]
no voice-class sip outbound-proxy

Syntax Description

dhcp	Specifies that the outbound-proxy IP address is retrieved from a DHCP server.
ipv4: *ipv4-address*	Configures proxy on the server, sending all initiating requests to the specified IPv4 address destination. The colon is required.
ipv6:[*ipv6- address* **]**	Configures proxy on the server, sending all initiating requests to the specified IPv6 address destination. Brackets must be entered around the IPv6 address. The colon is required.
dns: *host:domain*	Configures proxy on the server, sending all initiating requests to the specified domain destination. The colons are required.
: *port-number*	(Optional) Port number for the Session Initiation Protocol (SIP) server. The colon is required.

Command Default

An outbound proxy is not configured.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(22)T	This command was modified. Support for IPv6 was added.
12.4(22)YB	This command was modified. The dhcp keyword was added.
15.0(1)M	This command was integrated in Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **voice-class sip outbound-proxy** command, in dial peer configuration mode, takes precedence over the command in SIP global configuration mode.

Brackets must be entered around the IPv6 address.

Examples

The following example shows how to configure the **voice-class sip outbound-proxy**command on a dial peer to generate an IPv4 address (10.1.1.1) as an outbound proxy:

```
Router> enable
Router# configure
 terminal
```

```
Router(config)# dial
-peer
 voice
 111
 voip
Router(config-dial-peer)# voice-class sip outbound-proxy ipv4:10.1.1.1
```

The following example shows how to configure the **voice-class sip outbound-proxy**command on a dial peer to generate a domain (sipproxy:cisco.com) as an outbound proxy:

```
Router> enable
Router# configure
 terminal
Router(config)# dial
-peer
 voice
 111
 voip
Router(config-dial-peer)# voice-class sip outbound-proxy dns:sipproxy:cisco.com
```

The following example shows how to configure the **voice-class sip outbound-proxy**command on a dial peer to generate an outbound proxy using DHCP:

```
Router> enable
Router# configure
 terminal
Router(config)# dial
-peer
 voice
 111
 voip
Router(config-dial-peer)# voice-class sip outbound-proxy dhcp
```

Related Commands

Command	Description
dial -peer voice	Defines a particular dial peer, specifies the method of voice encapsulation, and enters dial peer configuration mode.
voice service	Enters voice-service configuration mode and specifies a voice encapsulation type.

voice-class sip preloaded-route

To enable preloaded route support for dial-peer Session Initiation Protocol (SIP) calls, use the **voice-class sip preloaded-route**command in dial peer voice configuration mode. To reset to the default value, use the **no** form of this command.

voice-class sip preloaded-route {[**sip-server**] **service-route** | **system**}
no voice-class sip preloaded-route

Syntax Description

sip-server	(Optional) Adds SIP server information to the Route header.
service-route	Adds the Service-Route information to the Route header.
system	Uses the global system value. This is the default.

Command Default

SIP calls at the dial-peer level use the global configuration level settings.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **voice-class sip preloaded-route** command takes precedence over the **preloaded-route** command configured in SIP configuration mode. However, if the **voice-class sip preloaded-route** command is used with the **system** keyword, the gateway uses the global settings configured by the **preloaded-route** command.

Examples

The following example shows how to configure the dial peer to include SIP server and Service-Route information in the Route header:

```
dial-peer voice 102 voip
 voice-class sip preloaded-route sip-server service-route
```

The following example shows how to configure the dial peer to include only Service-Route information in the Route header:

```
dial-peer voice 102 voip
 voice-class sip preloaded-route service-route
```

Related Commands

Command	Description
preloaded-route	Enables preloaded route support for VoIP SIP calls.

voice-class sip privacy

To set privacy support at the dial-peer level as defined in RFC 3323, use the **voice-class sip privacy** command in dial peer configuration mode. To remove privacy support as defined in RFC 3323, use the **no** form of this command.

voice-class sip privacy {**disable** | **pstn** | **system** | *privacy-option* [**critical**]}
no voice-class sip privacy

Syntax Description

disable	Disables the privacy service for this dial peer regardless of prior implementations. When selected, this becomes the only valid option.
pstn	Requests that the privacy service implements a privacy header using the default Public Switched Telephone Network (PSTN) rules for privacy (based on information in Octet 3a). When selected, this becomes the only valid option.
system	Uses the global configuration settings to enable the privacy service on this dial peer. When selected, this becomes the only valid option.
privacy-option	The privacy support options to be set at the dial-peer level. The following keywords can be specified for the *privacy-option* argument: • **header** -- Requests that privacy be enforced for all headers in the Session Initiation Protocol (SIP) message that might identify information about the subscriber. • **history** -- Requests that the information held in the history-info header is hidden outside the trust domain. • **id** -- Requests that the Network Asserted Identity that authenticated the user be kept private with respect to SIP entities outside the trusted domain. • **session** -- Requests that the information held in the session description is hidden outside the trust domain. • **user** -- Requests that privacy services provide a user-level privacy function. **Note** The keywords can be used alone, altogether, or in any combination with each other, but each keyword can be used only once.
critical	(Optional) Requests that the privacy service performs the specified service or fail the request. **Note** This optional keyword is only available after at least one of the *privacy-option* keywords (**header**, **history**, **id**, **session**, or **user**) has been specified and can be used only once per command.

Command Default

Privacy support is disabled.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(22)T	The **history** keyword was added to provide support for the history-info header information.

Usage Guidelines

Use the **voice-class sip privacy** command to instruct the gateway to add a Proxy-Require header, set to a value supported by RFC 3323, in outgoing SIP request messages at the dial-peer level.

Use the **voice-class sip privacy critical**command to instruct the gateway to add a Proxy-Require header with the value set to critical. If a user agent sends a request to an intermediary that does not support privacy extensions, the request fails.

The **voice-class sip privacy** command takes precedence over the **privacy** command in voice service voip sip configuration mode. However, if the **voice-class sip privacy** command is used with the **system** keyword, the gateway uses the settings configured globally by the **privacy** command.

Examples

The following example shows how to disable the privacy on dial peer 2:

```
Router> enable

Router# configure
 terminal
Router(config)# dial-peer voice 2 voip

Router(config-dial-peer)# voice-class sip privacy disable
```

The following example shows how to configure the **voice-class sip privacy** command so that the information held in the history-info header is hidden outside the trust domain:

```
Router> enable

Router# configure
 terminal
Router(config)# dial-peer voice 2 voip

Router(config-dial-peer)# voice-class sip privacy history
```

Related Commands

Command	Description
asserted-id	Sets the privacy level and enables either PAI or PPI privacy headers in outgoing SIP requests or response messages.
calling-info pstn-to-sip	Specifies calling information treatment for PSTN-to-SIP calls.
clid (voice-service-voip)	Passes the network-provided ISDN numbers in an ISDN calling party information element screening indicator field, removes the calling party name and number from the calling-line identifier in voice service voip configuration mode, or allows a presentation of the calling number by substituting for the missing Display Name field in the Remote-Party-ID and From headers.

Command	Description
privacy	Sets privacy support at the global level as defined in RFC 3323.

voice-class sip privacy-policy

To configure the privacy header policy options at the dial-peer level, use the **voice-class sip privacy-policy** command in dial peer voice configuration mode. To disable privacy-policy options, use the **no** form of this command.

voice-class sip privacy-policy {**passthru** | **send-always** | **strip** {**diversion** | **history-info**}} [**system**]
no voice-class sip privacy-policy {**passthru** | **send-always** | **strip** {**diversion** | **history-info**}}

Syntax Description

passthru	Passes the privacy values from the received message to the next call leg.
send-always	Passes a privacy header with a value of None to the next call leg, if the received message does not contain privacy values but a privacy header is required.
strip	Strip the diversion or history-info headers received from the next call leg.
diversion	Strip the diversion header received from the next call leg.
history-info	Strip the history-info header received from the next call leg.
system	(Optional) Uses the global configuration settings to configure the dial peer.

Command Default

No privacy-policy settings are configured.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(2)T	This command was integrated into Cisco IOS Release 15.1(2)T. The **strip**, **diversion**, and **history-info** keywords were added.

Usage Guidelines

If a received message contains privacy values, use the **voice-class sip privacy-policy passthru** command to ensure that the privacy values are passed from one call leg to the next. If a received message does not contain privacy values but the privacy header is required, use the **voice-class sip privacy-policy send-always** command to set the privacy header to None and forward the message to the next call leg. You can configure the system to support both options at the same time.

The **voice-class sip privacy-policy** command takes precedence over the **privacy-policy** command in voice service voip sip configuration mode. However, if the **voice-class sip privacy-policy** command is used with the **system** keyword, the gateway uses the settings configured globally by the **privacy-policy** command.

Examples

The following example shows how to enable the pass-through privacy policy on the dial peer:

```
Router> enable
```

```
Router# configure
 terminal
Router(config)# dial-peer voice 2611 voip
Router(config-dial-peer)# voice-class sip privacy-policy passthru
```

The following example shows how to enable the pass-through, send-always, and strip policies on the dial peer:

```
Router> enable

Router# configure
 terminal
Router(config)# dial-peer voice 2611 voip
Router(config-dial-peer)# voice-class sip privacy-policy passthru
Router(config-dial-peer)# voice-class sip privacy-policy send-always
Router(config-dial-peer)# voice-class sip privacy-policy strip diversion
Router(config-dial-peer)# voice-class sip privacy-policy strip history-info
```

The following example shows how to enable the send-always privacy policy on the dial peer:

```
Router> enable

Router# configure
 terminal
Router(config)# dial-peer voice 2611 voip
Router(config-dial-peer)# voice-class sip privacy-policy send-always
```

The following example shows how to enable both the pass-through privacy policy and send-always privacy policies on the dial peer:

```
Router> enable

Router# configure
 terminal
Router(config)# dial-peer voice 2611 voip
Router(config-dial-peer)# voice-class sip privacy-policy passthru
Router(config-dial-peer)# voice-class sip privacy-policy send-always
```

Related Commands

Command	Description
asserted-id	Sets the privacy level and enables either PAID or PPID privacy headers in outgoing SIP requests or response messages.
privacy-policy	Configures the privacy header policy options at the global configuration level.

voice-class sip random-contact

To populate the outgoing INVITE message with random-contact information (instead of clear contact information) at the dial-peer level, use the **voice-class sip random-contact** command in dial peer voice configuration mode. To disable random contact information, use the **no** form of this command.

voice-class sip random-contact [**system**]
no voice-class sip random-contact

Syntax Description

system	(Optional) Uses the global configuration settings to populate the INVITE message with random contact information.

Command Default

Support for random contact at the dial-peer level uses the the global configuration level settings.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

To populate outbound INVITE messages (from the Cisco Unified Border Element) with random-contact information instead of clear-contact information at the dial-peer level, use the **voice-class sip random-contact** command. This functionality will work only when the Cisco Unified Border Element is configured for SIP registration with random-contact, using the **credentials** and **registrar** commands.

The **voice-class sip random-contact** command takes precedence over the **random-contact** command in voice service voip sip configuration mode. However, if the **voice-class sip random-contact** command is used with the **system** keyword, the gateway uses the settings configured globally by the **random-contact** command.

Examples

The following example shows how to populate outbound INVITE messages, at the dial-peer level, with random-contact information:

```
Router> enable

Router# configure
 terminal
Router(config)# dial-peer voice 2611 voip
Router(config-dial-peer)# voice-class sip random-contact
```

Related Commands

Command	Description
credentials (sip ua)	Sends a SIP registration message from a Cisco Unified Border Element in the UP state.
registrar	Enables SIP gateways to register E.164 numbers on behalf of FXS, EFXS, and SCCP phones with an external SIP proxy or SIP registrar.

Command	Description
random-contact	Populates the outgoing INVITE message with random contact information at the global level.

voice-class sip random-request-uri validate

To enable the validation of the called-number based on the random value generated during the registration of the number, at dial-peer configuration level, use the **voice-class sip random-request-uri validate** command in dial peer voice configuration mode. To disable validation, use the **no** form of this command.

voice-class sip random-request-uri validate [**system**]
no voice-class sip random-request-uri validate

Syntax Description

system	(Optional) Uses the global configuration settings to enable called-number validation on this dial peer.

Command Default

Validation is disabled.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

The system generates a random string when registering a new number. An INVITE message with the P-Called-Party-ID value can have the Request-URI set to this random number. To enable the system to identify the called number from the random number in the Request-URI, use the **voice-class sip random-request-uri validate** command on the inbound dial peer.

If the P-Called-Party-ID is not set in the INVITE message, the Request URI for that message must contain the called party information (and cannot contain a random number). Therefore validation is performed only on INVITE messages with a P-Called-Party-ID.

The **voice-class sip random-request-uri validate** command takes precedence over the **random-request-uri validate** command in voice service voip sip configuration mode. However, if the **voice-class sip random-request-uri validate** command is used with the **system** keyword, the gateway uses the settings configured globally by the **random-request-uri validate** command.

Examples

The following example shows how to enable call routing based on the P-Called-Party-ID header value at the dial-peer configuration level:

```
Router> enable

Router# configure
 terminal
Router(config)# dial-peer voice 2611 voip

Router(config-dial-peer)# voice-class sip random-request-uri validate
```

Related Commands

Command	Description
credentials (sip ua)	Sends a SIP registration message from a Cisco Unified Border Element in the UP state.
random-request-uri validate	Validates the called number based on the random value generated during the registration of the number at the global configuration level.
registrar	Enables SIP gateways to register E.164 numbers on behalf of FXS, EFXS, and SCCP phones with an external SIP proxy or SIP registrar.

voice-class sip referto-passing

To disable the modification of the Refer-To header during REFER message pass-through on the Cisco Unified Border Element (UBE) on the specified dial peer, use the **voice-class sip referto-passing** command in dial peer voice configuration mode. To allow the modification of the Refer-To header during REFER message pass-through on the Cisco UBE, use the **no** form of this command.

voice-class sip referto-passing [**system**]
no voice-class sip referto-passing

Syntax Description

system	(Optional) Enables the **referto-passing** command configured in global configuration mode.

Command Default

The Refer-To header modification is enabled.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.2(1)T	This command was introduced.

Usage Guidelines

The dial peer configuration setting of the **voice-class sip referto-passing** command takes precedence over the global configuration setting of the **referto-passing** command. You can use the **system** keyword to toggle the precedence.

Examples

The following example shows how to enable REFER message pass-through on the Cisco UBE for dial peer 22:

```
Router(config)# dial-peer voice 22 voip
Router(config-dial-peer)# voice-class sip referto-passing
```

Related Commands

Command	Description
dial-peer voice	Defines a particular dial peer, specifies the method of encapsulation, and enters dial peer voice configuration mode.
referto-passing	Disables dial peer lookup and modification of the Refer-To header when the Cisco UBE passes across a REFER message during a call transfer

voice-class sip registration passthrough

To configure Session Initiation Protocol (SIP) registration pass-through options on a dial peer, use the **voice-class sip registration passthrough**command in dial peer voice configuration mode. To disable the configuration, use the **no** form of this command.

voice-class sip registration passthrough [[**static**] [**rate-limit** [**expires** *value*] [**fail-count** *value*]] [**registrar-index** [*index*]] | **system**]
no voice-class sip registration passthrough

Syntax Description

static	(Optional) Configures Cisco Unified Border Element (UBE) to use static registrar details for SIP registration. Cisco UBE works in point-to-point mode when the **static** keyword is used.
rate-limit	(Optional) Configures SIP registration pass-through rate-limiting options.
expires *value*	(Optional) Sets the expiry value for rate limiting, in seconds. The range is from 60 to 65535. The default is 3600.
fail-count *value*	(Optional) Sets the fail-count value for rate limiting. The range is from 2 to 20. The default is 0.
registrar-index	(Optional) Configures the registrar index used for registration pass-through.
index	(Optional) Registration index value. The range is from 1 to 6.
system	(Optional) Uses global registration pass-through configuration to configure the SIP registration pass-through options.

Command Default

SIP registration pass-through options that are configured at the global level are configured.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

You can use the **voice-class sip registration passthrough** command to configure the following SIP pass-through functionalities on a dial peer:

- Back-to-back registration facility to register phones for call routing.
- Options to configure the rate-limiting values, such as the expiry time, fail-count, and a list of registrars to be used for registration.

Examples

The following example shows how to set the registrar index of 1 for the SIP registration pass-through rate limiting:

```
Router# configure terminal
Router(config)# dial-peer voice 444 voip
Router(config-dial-peer)# voice-class sip registration passthrough static rate-limit
registrar-index 1
```

Related Commands

Command	Description
registration passthrough	Configures SIP registration pass-through options at the global level.

voice-class sip rel1xx

To enable all Session Initiation Protocol (SIP) provisional responses (other than 100 Trying) to be sent reliably to the remote SIP endpoint, use the **voice-class sip rel1xx** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

voice-class sip rel1xx {**supported** *value* | **require** *value* | **system** | **disable**}
no sip rel1xx

Syntax Description

supported *value*	Supports reliable provisional responses. The *value* argument may have any value, as long as both the user-agent client (UAC) and user-agent server (UAS) configure it the same.
require *value*	Requires reliable provisional responses. The *value* argument may have any value, as long as both the UAC and UAS configure it the same.
system	Uses the value configured in voice service mode. This is the default.
disable	Disables the use of reliable provisional responses.

Command Default

system

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was applicable to the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.

Usage Guidelines

There are two ways to configure reliable provisional responses:

- Dial-peer mode. You can configure reliable provisional responses for the specific dial peer only by using the **voice-class sip rel1xx** command.
- SIP mode. You can configure reliable provisional responses globally by using the **rel1xx**command.

The use of resource reservation with SIP requires that the reliable provisional feature for SIP be enabled either at the VoIP dial-peer level or globally on the router.

This command applies to the dial peer under which it is used or points to the global configuration for reliable provisional responses. If the command is used with the **supported** keyword, the SIP gateway uses the Supported header in outgoing SIP INVITE requests. If it is used with the **require** keyword, the gateway uses the Required header.

This command, in dial-peer configuration mode, takes precedence over the **rel1xx** command in global configuration mode with one exception: If this command is used with the system keyword, the gateway uses what was configured under the **rel1xx** command in global configuration mode.

Examples

The following example shows how to use this command on either an originating or a terminating SIP gateway:

- On an originating gateway, all outgoing SIP INVITE requests matching this dial peer contain the Supported header where *value* is 100rel.
- On a terminating gateway, all received SIP INVITE requests matching this dial peer support reliable provisional responses.

```
Router(config)# dial-peer voice 102 voip
Router(config-dial-peer)# voice-class sip rel1xx supported 100rel
```

Related Commands

Command	Description
rel1xx	Provides provisional responses for calls on all VoIP calls.

voice-class sip requri-passing

To enable the pass through of Session Initiation Protocol (SIP) Uniform Resource Locator (URI) headers, use the **voice-class sip requri-passing** command in dial peer voice configuration mode. To disable this configuration, use the **no** form of the command.

voice-class sip requri-passing [**system**]
no voice-class sip requri-passing

Syntax Description

system	(Optional)

Command Default

The pass through of SIP URI headers is not enabled.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.4(1)T	This command was introduced.

Example

The following example shows how to enable the pass through of SIP URI headers using the **voice-class sip requri-passing** command:

```
Device> enable
Device# configure terminal
Device(config)# voice class uri mydesturi sip
Device(config-voice-uri-class)# host example.com
Device(config-voice-uri-class)# exit
Device(config)# dial-peer voice 22 voip
Device(config-dial-peer)# session protocol sipv2
Device(config)# destination uri mydesturi
Device(config-dial-peer)# session target ipv4:10.1.1.2
Device(config-dial-peer)# voice-class sip requri-passing system
Device(config-dial-peer)# end
```

Related Commands

Command	Description
contact-passing	Configures pass-through of the contact header from one leg to the other leg for 302 pass-through.
requri-passing	Enables pass through of the host part of the Request-URI and To SIP headers.
session target sip-uri	Derives session target from incoming URI.
voice-class sip requri-passing	Enables the pass through of SIP URI headers.

voice-class sip reset timer expires

To configure an individual dial peer on Cisco Unified Communications Manager Express (Cisco Unified CME), a Cisco IOS voice gateway, or a Cisco Unified Border Element (Cisco UBE) to reset the expires timer upon receipt of a Session Initiation Protocol (SIP) 183 Session In Progress message, use the **voice-class sip reset timer expires** command in dial peer voice configuration mode. To globally disable resetting of the expires timer upon receipt of SIP 183 messages, use the **no** form of this command.

voice-class sip reset timer expires 183
no voice-class sip reset timer expires 183

Syntax Description

183	Specifies resetting of the expires timer upon receipt of SIP 183 Session In Progress messages.

Command Default

The expires timer is not reset after receipt of SIP 183 Session In Progress messages and a session or call that is not connected within the default expiration time (three minutes) is dropped.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.0(1)XA	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

In some scenarios, early media cut-through calls (such as emergency calls) rely on SIP 183 with session description protocol (SDP) Session In Progress messages to keep the session or call alive until receiving a FINAL SIP 200 OK message, which indicates that the call is connected. In these scenarios, the call can time out and be dropped if it does not get connected within the default expiration time (three minutes).



Note The expires timer default is three minutes. However, you can configure the expiration time to a maximum of 30 minutes using the **timers expires** command in SIP user agent (UA) configuration mode.

To prevent early media cut-through calls from being dropped on a specific dial peer because they reach the expires timer limit, use the **voice-class sip reset timer expires** command in dial peer voice configuration mode.

To globally configure all dial peers on Cisco Unified CME, a Cisco IOS voice gateway, or a Cisco UBE so that the expires timer is reset upon receipt of any SIP 183 message, use the **reset timer expires** command in voice service SIP configuration mode. To disable resetting of the expires timer on receipt of SIP 183 messages for an individual dial peer, use the **no voice-class sip reset timer expires** command in dial peer voice configuration mode.

Examples

The following example shows how to configure dial peer 1 on Cisco Unified CME, a Cisco IOS voice gateway, or a Cisco UBE to reset the expires timer each time a SIP 183 message is received:

```
Router> enable
Router# configure
 terminal
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class sip reset timer expires 183
```

Related Commands

Command	Description
reset timer expires	Globally configures Cisco Unified CME, a Cisco IOS voice gateway, or a Cisco UBE to reset the expires timer upon receipt of a SIP 183 message.
timers expires	Specifies how long a SIP INVITE request remains valid before it times out if no appropriate response is received for keeping the session alive.

voice-class sip resource priority dscp-profile

To apply a differentiated services code point (DSCP) profile to a dial peer, use the **voice-class sip resource priority dscp-profile** in dial peer voice configuration mode. To disable the configuration, use the **no** form of this command.

voice-class sip resource priority dscp-profile *tag*
no voice-class sip resource priority dscp-profile

Syntax Description

tag	DSCP profile group tag number. The range is from 1 to 10000.

Command Default

A DSCP profile is not applied.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

You can use the **voice-class sip resource priority dscp-profile** command to apply the DSCP profile that is configured using the **dscp media** command for a dial peer.

Examples

The following example shows how to configure a DSCP profile for a dial peer:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 4 voip
Router(config-dial-peer)# voice-class sip resource priority dscp-profile 1
```

Related Commands

Command	Description
dial-peer voice	Configures a dial peer and enters dial peer voice configuration mode.
dscp media	Specifies the RPH to DSCP mapping.

voice-class sip resource priority mode (dial-peer)

To push the user access server (UAS) to operate in a loose or strict mode, use the **voice-class sip resource priority mode** command in dial peer voice configuration mode. To disable the **voice-class sip resource priority mode**, use the **no** form of this command.

voice-class sip resource priority mode [**loose** | **strict**]
no voice-class sip resource priority mode [**loose** | **strict**]

Syntax Description

loose	(Optional) In the loose mode, unknown values of name space or priority values received in the Resource-Priority header in Session Initiation Protocol (SIP) requests are ignored by the gateway. The request is processed as if the Resource-Priority header was not present.
strict	(Optional) In the strict mode, unknown values of name space or priority values received in the Resource-Priority header in SIP requests are rejected by the gateway using a SIP response code 417 (Unknown Resource-Priority) message response. An Accept-Resource-Priority header enumerating the supported name space and values is included in the 417 message response.

Command Default

The default value is **loose mode**.

Command Modes

Dial peer voice configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

When the no version of this command is executed, the call operates in the **loose** mode.

Examples

The following example shows how to set up the **voice-class sip resource priority mode** command in loose mode:

```
Router(config)# dial-peer voice 102 voip
Router(config-dial-peer)# voice-class sip resource priority mode loose
```

The following example shows how to set up the **voice-class sip resource priority mode** command in strict mode:

```
Router(config)# dial-peer voice 102 voip
Router(config-dial-peer)# voice-class sip resource priority mode strict
```

Related Commands

Command	Description
voice-class sip resource priority namespace	Priorities mandatory call prioritization handling for initial original INVITE message requests.

voice-class sip resource priority namespace (dial-peer)

To prioritize mandatory call prioritization handling for initial original INVITE message requests, use the **voice-class sip resource priority namespace** command in dial peer voice configuration mode. To disable the **voice-class sip resource priority namespace** command, use the **no** form of this command.

voice-class sip resource priority namespace [**drsn** | **dsn** | **q735**]
no voice-class sip resource priority namespace [**drsn** | **dsn** | **q735**]

Syntax Description

drsn	(Optional) U. S. Defense Red Switched Network (DRSN).
dsn	(Optional) U. S. Defense Switched Network (DSN).
q735	(Optional) International Telecommunications Union, *Stage 3 description for community of interest supplementary services using Signaling System No. 7: Multilevel precedence and preemption, Recommendation Q.735.3* , March 1993.

Command Default

When the no version of this command is executed using namespace, the Cisco IOS gateway transparently passes the multilevel precedence and preemption (MLPP) values that were received on the PSTN side.

Command Modes

Dial peer voice configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

When the no version of this command is executed using the namespace, the Cisco IOS gateway transparently passes the multilevel precedence and preemption (MLPP) values that were received on the PSTN side.

Examples

The following example shows how to set up the **voice-class sip resource priority namespace** command in the U. S. DSN format name space:

```
Router(config)# dial-peer voice 102 voip
Router(config-dial-peer)# voice-class sip resource priority namespace dsn
```

The following example shows how to set up the **voice-class sip resource priority namespace** command in the U. S. DRSN format name space:

```
Router(config)# dial-peer voice 102 voip
Router(config-dial-peer)# voice-class sip resource priority namespace drsn
```

The following example shows how to set up the **voice-class sip resource priority namespace** command in the Public SS7 Network format name space:

```
Router(config)# dial-peer voice 102 voip
Router(config-dial-peer)# voice-class sip resource priority namespace q735
```

Related Commands

Command	Description
voice-class sip resource priority mode	Pushes the UAS to operate in a loose or strict mode.

voice-class sip rsvp-fail-policy

To specify the action that takes place at the dial peer level on a Cisco IOS Session Initiation Protocol (SIP) gateway when Resource Reservation Protocol (RSVP) negotiation fails, use the **voice-class sip rsvp-fail-policy** command in dial peer configuration mode. To reset failure behavior to the default settings, use the **no** form of this command.

voice-class sip rsvp-fail-policy {**video** | **voice**} **post-alert** {**optional keep-alive** | **mandatory** {**keep-alive** | **disconnect retry** *retry-attempts*}} **interval** *seconds*
no voice-class sip rsvp-fail-policy {**video** | **voice**} **post-alert** {**optional** [**keep-alive**] | **mandatory** [**keep-alive** | **disconnect retry** *retry-attempts*]} [**interval** *seconds*]

Syntax Description

video	Specifies the video RSVP stream type.
voice	Specifies the audio or fax RSVP stream type.
post-alert	Specifies that behavior takes place only when the call state is post alert.
optional	Specifies that behavior takes place when RSVP fails even if RSVP negotiation is optional.
mandatory	Specifies that behavior takes place when RSVP fails only if RSVP negotiation is mandatory.
keep-alive	Specifies the sending of keepalive messages when RSVP fails.
disconnect	Specifies that the call is disconnected if RSVP fails after the specified number of retry settings.
retry	Specifies the number of reconnection attempts before disconnecting the call.
retry-attempts	The number of retry attempts. Valid entries are from 1 to 100.
interval	Specifies the interval between keepalive or retry attempts.
seconds	The retry interval in seconds. Valid entries are from 5 to 3600.

Command Default

Keepalive messages are sent at 30-second intervals when a post alert voice or video call fails to negotiate RSVP regardless of the RSVP negotiation setting (mandatory or optional).

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

Use this command to configure call handling behavior when a call fails RSVP negotiation. You can configure the behavior that takes place for either optional or mandatory RSVP negotiation but the behavior will apply only to calls in a post alert call state. To configure the behavior that takes place when RSVP negotiation fails, use the **voice-class sip rsvp-fail-policy** command in dial peer configuration mode.

If a call fails RSVP negotiation where negotiation is optional, then RSVP negotiation should be retried using the keepalive function at specified intervals until RSVP negotiation is successful.

If a call fails RSVP negotiation where negotiation is mandatory, then RSVP negotiation should be configured in one of two ways:

- The call that failed RSVP negotiation is disconnected after a specified number of attempts to renegotiate RSVP with each retry taking place at a specified interval. If negotiation succeeds during these retry attempts, counters and timers are reset to zero.
- The call that failed RSVP negotiation is kept alive with keepalive messages sent at specified intervals until negotiation is successful.

Examples

The following example shows how to specify sending of keepalive messages at 60-second intervals for a call that fails RSVP negotiation when negotiation is optional:

```
Router(config)# dial-peer voice 102 voip
Router(config-dial-peer)# voice-class sip rsvp-fail-policy voice post-alert optional
keep-alive interval 60
```

Related Commands

Command	Description
acc-qos	Defines the acceptable QoS for inbound and outbound calls on a VoIP dial peer.
handle-replaces	Configures fallback to legacy handling of SIP INVITE.
ip qos defending-priority	Configures the RSVP defending priority value.
ip qos dscp	Sets the DSCP value for QoS.
ip qos policy-locator	Configures application-specific reservations (application IDs) used for specifying bandwidth reservations.
ip qos preemption-priority	Configures the RSVP preemption priority value.
req-qos	Requests a particular QoS using RSVP to be used in reaching a specified dial peer in VoIP.
show-sip-ua calls	Displays the active UAC and UAS information on SIP calls.

voice-class sip send 180 sdp

To configure a Cisco Unified Border Element (Cisco UBE) to map an incoming 180 Session Description Protocol (SDP) message to a 180 SDP message, use the **voice-class sip send 180 sdp** command in dial peer voice configuration mode or SIP configuration mode. To disable this functionality, use the **no** form of this command.

voice-class sip send 180 sdp
novoice-class sip send 180 sdp

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled. Cisco UBE converts an incoming 180 SDP message to a 183 SDP message.

Command Modes

Dial peer voice configuration (config-dialpeer)

SIP configuration (conf-serv-sip)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

This command must be enabled at the inbound dial peer. Enable the **voice-class sip send 180 sdp** command to map a 180 SDP message to a 180 SDP message. When this command is disabled, an incoming 180 SDP (Ringing) message is mapped to a 183 SDP (Session in Progress) message.

Examples

The following example shows how to configure the **voice-class sip send 180 sdp** command at dial peer level:

```
Device> enable
Device# configure terminal
Device(config)# dial peer voice
Device(config-dialpeer)# voice-class sip send 180 sdp
Device(config-dialpeer)# exit
```

Related Commands

Command	Description
voice-class sip block	Configures an individual dial peer on a Cisco IOS voice gateway or Cisco UBE to drop (not pass) specific incoming Session Initiation Protocol (SIP) provisional response messages.

voice-class sip srtp-auth

Note Effective Cisco IOS XE Everest Releases 16.5.1b, **srtp-auth** command is deprecated. Although this command is still available in Cisco IOS XE Everest software, executing this command does not cause any configuration changes. Use **voice class srtp-crypto** command to configure SRTP connection using preferred crypto-suites. For more information, see voice-class sip srtp-crypto, on page 416 command documentation.

To configure a Secure Real-time Transport Protocol (SRTP) connection on Cisco Unified Border Element (Cisco UBE) using the preferred crypto suite in the dial peer level, use the **voice-class sip srtp-auth** command in dial peer voice configuration mode. To disable this configuration, use the **no** form of the command.

voice-class sip srtp-auth {**sha-32** | **sha-80** | **system**}
no voice-class sip srtp-auth

Syntax Description

sha-32	Allows secure calls with AES_CM_128_HMAC_SHA1_32 authentication suite.
sha-80	Allows secure calls with AES_CM_128_HMAC_SHA1_80 authentication suite.
system	Uses the global configuration.

Command Default

The sha-32 crypto suite is configured by default.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.4(1)T	This command was introduced.
Cisco IOS XE Everest 16.5.1b	This command was deprecated.

Usage Guidelines

Use the **system** keyword with the **voice-class sip srtp-auth** command to use the crypto suite configured at the global level.

Example

The following example shows how to configure an SRTP connection on Cisco UBE in the dial peer level using the AES_CM_128_HMAC_SHA1_80 crypto suite:

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 15 voip
Device(config-dial-peer)# voice-class sip srtp-auth sha1-80
```

Related Commands

Command	Description
srtp-auth	Configures a Secure Real-time Transport Protocol (SRTP) connection on Cisco Unified Border Element (Cisco UBE) in the global level using the preferred crypto suite.
show sip-ua srtp	Displays Session Initiation Protocol (SIP) user-agent (UA) Secure Real-time Transport Protocol (SRTP) information.

voice-class sip srtp-crypto

To assign a previously configured crypto-suite selection preference to a dial-peer, use the **voice-class sip srtp-crypto** command. To remove the crypto-suite preference from the dial-peer and return to the default preference list, use the **no** or **default** form of this command.

voice-class sip srtp-crypto *crypto-tag*
no voice-class sip srtp-crypto
default voice-class sip srtp-crypto

Syntax Description

crypto-tag	Unique number assigned to the voice class. The range is from 1 to 10000. This number maps to the tag created using the **voice class srtp-crypto** command available in global configuration mode.

Command Default

No crypto-suite preference is assigned to the dial-peer.

Command Modes

dial-peer configuration (config-dial-peer)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1b	This command was introduced.

Usage Guidelines

Note Ensure that an srtp voice-class is created using the **voice class srtp-crypto** *crypto-tag* command before executing the **voice-class sip srtp-crypto** *crypto tag* command to apply the crypto-tag under global or tenant configuration mode.

You can assign only one crypto-tag. If you assign another crypto-tag, the last crypto-tag assigned replaces the previous crypto-tag.

Example

```
Device enable
Device# configure terminal
Device(config)# dial-peer voice 300 voip
Device(config-dial-peer)# voice-class sip srtp-crypto 102
```

Related Commands

Command	Description
srtp-crypto	Assigns a previously configured crypto-suite selection preference list globally or to a voice class tenant.
crypto	Specifies the preference for a SRTP cipher-suite that will be offered by Cisco Unified Border Element (CUBE) in the SDP in offer and answer.

Command	Description
show sip-ua calls	Displays active user agent client (UAC) and user agent server (UAS) information on Session Initiation Protocol (SIP) calls.
show sip-ua srtp	Displays Session Initiation Protocol (SIP) user-agent (UA) Secure Real-time Transport Protocol (SRTP) information.

voice-class sip srtp negotiate

To enable Secure Real-Time Transport Protocol (SRTP) negotiation so that an individual dial peer on a Cisco IOS Session Initiation Protocol (SIP) gateway can accept and send an RTP Audio/Video Profile (AVP) in response to an RTP Secure AVP offer (also known as an SRTP profile), use the **voice-class sip srtp negotiate** command in dial peer voice configuration mode. To return to the default (global) SRTP negotiation setting on a dial peer, use the **system** keyword. To disable SRTP negotiation on a dial peer, use the **no** form of this command.

voice-class sip srtp negotiate {**cisco** | **system**}
no voice-class sip srtp negotiate

Syntax Description

cisco	Enables an individual dial peer on a Cisco IOS SIP gateway to negotiate the sending and accepting of RTP profiles in response to SRTP offers, overriding the global setting for the gateway.
system	Specifies that the individual dial peer use global (system) SRTP negotiation settings for the Cisco IOS SIP gateway. This is the default setting.

Command Default

SRTP negotiation is determined by global settings for the Cisco IOS gateway (**voice-class sip srtp negotiate system**).

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(22)T	Support was extended to the Cisco Unified Border Element.

Usage Guidelines

The **srtp fallback** command enables a SIP gateway (or individual dial peer on a SIP gateway) to allow SRTP fallback using SIP 4*xx* message responses. With the **srtp negotiate** command, a SIP gateway can be configured to accept and send an RTP (nonsecure) profile in response to an SRTP profile.

Use the **voice-class sip srtp negotiate** command in dial peer voice configuration mode to enable SRTP negotiation for an individual dial peer on a Cisco IOS SIP gateway, overriding the global settings on the gateway. Enabling SRTP negotiation allows a dial peer to accept and send nonsecure RTP profiles in response to SRTP offers. To configure global SRTP negotiation settings for a SIP gateway, use the **srtp negotiate** command in voice service SIP configuration mode.

There are two scenarios for SRTP negotiation when the **voice-class sip srtp negotiate** command is enabled:

- On a SIP dial peer with the **srtp fallback** command enabled, the dial peer accepts RTP answers to SRTP offers.
- On a SIP dial peer with the **srtp fallback** command disabled, the dial peer allows incoming SRTP calls and responds with an RTP answer.

These behaviors are accomplished using the "X-cisco-srtp-fallback" extension in the supported header of initial SIP messages involved in establishment of the session.

Examples

The following example shows SRTP negotiation being enabled on a dial peer, overriding global settings:

```
Device(config)# dial-peer voice 1
Device(config-dial-peer)# voice-class sip srtp negotiate cisco
```

Related Commands

Command	Description
srtp (dial peer)	Specifies that an individual dial peer use SRTP to enable secure calls and, optionally, enables fallback to RTP (overriding global settings).
srtp (voice)	Specifies use of SRTP to enable secure calls and, optionally, enables fallback to RTP globally on a Cisco IOS SIP gateway.
srtp negotiate	Enables SRTP negotiation globally on a Cisco IOS SIP gateway.

voice-class sip tel-config to-hdr

To configure the To: Header (to hdr) request Uniform Resource Identifier (URI) to telephone (TEL) format for dial-peer VoIP Session Initiation Protocol (SIP) calls, use the **voice-class sip tel-config to-hdr**command in dial peer voice configuration mode. To reset to the default, use the **no** form of this command.

voice-class sip tel-config to-hdr {**phone-context** | **system**}
no voice-class sip tel-config to-hdr

Syntax Description

phone-context	Appends the phone context parameter to the TEL URL on a dial-peer basis.
system	Uses the system value. This is the default.

Command Default

The To: Header request URIs at the dial-peer level use the global configuration level settings.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

The **voice-class sip tel-config to-hdr** command takes precedence over the **tel-config to-hdr** command configured in SIP configuration mode. However, if the **voice-class sip tel-config to-hdr** command is used with the **system** keyword, the gateway uses the global settings configured by the **tel-config to-hdr** command.

Examples

The following example configures the To: header in TEL format for a dial peer VoIP SIP call, and appends the phone-context parameter:

```
dial-peer voice 102 voip
 voice-class sip tel-config to-hdr phone-context
```

Related Commands

Command	Description
tel-config to-hdr	Configures the To: Header Request URI to telephone format for VoIP SIP calls.

voice-class sip tenant

To associate a dial-peer with a specific tenant configuration, use the **voice-class sip tenant** command in dial-peer configuration mode. To remove the association, use the **no** form of this command.

voice-class sip tenant *tag*
no voice-class sip tenant *tag*

Syntax Description

tag	A number used to identify voice-class sip tenant. The range is from 1 to 10000.

Command Default

No default behavior or values.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.6(2)T and IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

Use the **voice-class sip tenant** <*tag*> command in dial-peer configuration mode to associate the dial-peer with a **voice-class sip tenant** <*tag*>. If the dial-peer is associated with a tenant, the configurations are applied in the following order of preference:

1. Dial-peer configuration
2. Tenant configuration
3. Global configuration

If there are no tenants configured under dial-peer, then configurations are applied using the default behavior in the following order:

1. Dial-peer configuration
2. Global configuration

Examples

The following example shows how to configure the **voice-class sip tenant<tag>** command in dial-peer configuration mode:

```
Router(config)# dial-peer voice 10 voip
Router(config-dial-peer)# voice-class sip tenant <tag>
Router(config-dial-peer)# end
```

voice-class sip transport switch

To enable switching between UDP and TCP transport mechanisms for large Session Initiation Protocol (SIP) messages for a specific dial peer, use the **voice-class sip transport switch**command in dial-peer configuration mode. To disable switching between UDP and TCP transport mechanisms for large SIP messages for a specific dial peer, use the **no** form of this command.

voice-class sip transport switch udp tcp
no voice-class sip transport switch udp tcp

Syntax Description

udp	Enables switching transport from UDP on the basis of the size of the SIP request being greater than the MTU size.
tcp	Enables switching transport to TCP.

Command Default

Disabled.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **voice-class sip transport switch**command takes precedence over the global **transport switch**command.

Examples

The following example shows how to set up the **voice-class sip transport switch**command:

```
Router(config)# dial-peer voice 102 voip
Router(config-dial-peer)# voice-class sip transport switch udp tcp
```

Related Commands

Command	Description
debug ccsip transport	Enables tracing of the SIP transport handler and the TCP or UDP process.
transport switch	Enables switching between transport mechanisms globally if the SIP message is larger than 1300 bytes.

voice-class sip url

To configure URLs to either the Session Initiation Protocol (SIP), SIP security (SIPS), or telephone (TEL) format for your dial-peer SIP calls, use the **voice-class sip url** command in dial peer voice configuration mode. To reset to the default value use the **no** form of this command.

voice-class sip url {**sip** | **sips** | **tel** [**phone-context**] | **system**}
no voice-class sip url

Syntax Description

sip	Generates URLs in the SIP format for calls on a dial-peer basis.
sips	Generates URLs in the SIPS format for calls on a dial-peer basis.
tel	Generates URLs in the TEL format for calls on a dial-peer basis.
phone-context	(Optional) Appends the phone context parameter to the TEL URL on a dial-peer basis.
system	Uses the system value. This is the default.

Command Default

SIP calls at the dial-peer level use the global configuration level settings.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.
12.4(6)T	The **sips** keyword was added.
12.4(22)YB	The **phone-context** keyword was added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

This command affects only user-agent clients (UACs), because it causes the use of a SIP, SIPS, or TEL URL in the request line of outgoing SIP INVITE requests. SIP URLs indicate the originator, recipient, and destination of the SIP request; TEL URLs indicate voice-call connections.

The **voice-class sip url** command takes precedence over the **url** command configured in SIP configuration mode. However, if the **voice-class sip url** command is used with the **system** keyword, the gateway uses what was globally configured with the **url** command.

Examples

The following example shows how to configure the **voice-class sip url**command to generate URLs in the SIP format:

```
dial-peer voice 102 voip
 voice-class sip url sip
```

The following example shows how to configure the **voice-class sip url**command to generate URLs in the SIPS format:

```
dial-peer voice 102 voip
 voice-class sip url sips
```

The following example shows how to configure the **voice-class sip url**command to generate URLs in the TEL format:

```
dial-peer voice 102 voip
 voice-class sip url tel
```

The following example shows how to configure the **voice-class sip url**command to generate URLs in the TEL format, and append the phone-context parameter:

```
dial-peer voice 102 voip
 voice-class sip url tel phone-context
```

Related Commands

Command	Description
sip url	Generates URLs in the SIP, SIPS, or TEL format.
url	Configures URLs to either SIP, SIPS, or TEL format.

voice-class source interface

To allow a loopback interface to be associated with a VoIP or VoIPv6 dial-peer profile, use the **voice-class source interface** command in dial peer configuration mode. To disable this association, use the **no** form of this command.

voice-class source interface loopback *interface-id* [*ipv4-addressipv6-address*]
no voice-class source interface loopback *interface-id* [*ipv4-addressipv6-address*]

Syntax Description

loopback	Specifies the loopback interface address.
interface-id	Specifies the interface on which the address is to be configured.
ipv4-address	(Optional) IPv4 address used in the loopback interface address.
ipv6-address	(Optional) IPv6 address used in the loopback interface address.

Command Default

No loopback interface is associated with a VoIPv6 dial-peer profile.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

When the **voice-class source interface** command is configured, the source address of Routing Time Protocol (RTP) generated by the DSPs in the voice gateway is taken from the address configured under the loopback interface. This command is used for policy-based routing (PBR) of RTP packets originated by the gateway. The policy route map is configured under the loopback interface, and then the loopback interface is specified under the VoIP or VoIPv6 dial peer using the voice-class source interface command.

This command only applies to voice gateway scenarios for routers connecting telephony equipment through E1/T1, BRI or analog ports to the IP network. It does not apply to Cisco Unified Border Element (CUBE) in IP to IP voice scenarios (with or without transcoding). PBR for RTP traffic is not implemented in CUBE.

Examples

The following example associates a loopback interface with a VoIPv6 dial-peer profile:

```
Router(config)# dial-peer voice 1 voip
Router (config-dial-peer)# voice-class source interface loopback0
```

Related Commands

Command	Description
dial-peer voice	Defines a particular dial peer, specifies the method of voice encapsulation, and enters dial peer configuration mode.

voice-class stun-usage

To configure voice class, enter voice class configuration mode called stun-usage and use the **voice-class stun-usage** command in global, dial-peer, ephone, ephone template, voice register pool, or voice register pool template configuration mode. To disable the voice class, use the **no** form of this command.

voice-class stun-usage *tag*
no voice-class stun-usage *tag*

Syntax Description

tag	Unique identifier in the range 1 to 10000.

Command Default

The voice class is not defined.

Command Modes

Global configuration (config)
Dial peer configuration (config-dial-peer)
Ephone configuration (config-ephone)
Ephone template configuration (config-ephone-template)
Voice register pool configuration (config-register-pool)
Voice register pool template configuration (config-register-pool)

Command History

Release	Cisco Product	Modification
12.4(22)T	Cisco Unified CME 7.0	This command was introduced.
15.1(2)T	Cisco Unified CME 8.1	This command was modified. This command can be enabled in ephone summary, ephone template, voice register pool, or voice register pool template configuration mode.

Usage Guidelines

When the voice-class stun-usage is removed, the same is removed automatically from the dial-peer, ephone, ephone template, voice register pool, or voice register pool template configurations.

Examples

The following example shows how to set the **voice class stun-usage** tag to 10000:

```
Router(config)# voice class stun-usage 10000
Router(config-ephone)# voice class stun-usage 10000
Router(config-voice-register-pool)# voice class stun-usage 10000
```

Related Commands

Command	Description
stun usage firewall-traversal flowdata	Enables firewall traversal using STUN.
stun flowdata agent-id	Configures the agent ID.

voice-class tone-signal

To assign a previously configured tone-signal voice class to a voice port, use the **voice-class tone-signal** command in voice-port configuration mode. To delete a tone-signal voice class, use the **no** form of this command.

voice-class tone-signal *tag*
no voice-class tone-signal *tag*

Syntax Description

tag	Unique label assigned to the voice class. The *tag* label maps to the tag label created using the **voice class tone-signal** global configuration command. Can be up to 32 alphanumeric characters.

Command Default

Voice ports have no tone-signal voice class assigned.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

The **voice-class tone-signal** command is available on an ear and mouth (E&M) voice port only if the signal type for that port is Land Mobile Radio (LMR). Note that the hyphenation in this command differs from the hyphenation used in a similar command, **voice class tone-signal**, which is used in global configuration mode.

Examples

The following example assigns a previously configured voice class to voice port 1/1/0:

```
voice-port 1/0/0
 voice-class tone-signal mytones
```

Related Commands

Command	Description
voice class tone-signal	Enters voice-class configuration mode and assigns an identification tag number for a tone-signal voice class.

voice-ctl-file

To create a Cisco Certificate Trust List (CTL) file for a Cisco Unified Communications Manager (CUCM) cluster and to enter CTL file configuration mode, use the **voice-ctl-file** command in global configuration mode. To remove a CTL file for a CUCM cluster, use the **no** form of the command.

voice-ctl-file *ctl-file-name*
no voice-ctl-file *ctl-file-name*

Syntax Description

ctl-file-name	Name of the CTL file. A maximum number of 30 characters can be entered for the CTL file name.

Command Default

None

Command Modes

Global configuration mode (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

The **voice-ctl-file** command allows you to create an instance of a CTL file for a CUCM cluster. In CTL file configuration mode you can specify the trustpoints to be used for the creation of the CTL file.

Example

The following example shows how to create a CTL file instance called “myctl”:

```
Device(config)# voice-ctl-file myctl
```

voice confirmation-tone

To disable the two-beep confirmation tone for private line, automatic ringdown (PLAR), or PLAR off-premises extension (OPX) connections, use the **voice confirmation-tone** command in voice-port configuration mode. To enable the two-beep confirmation tone, use the **no** form of this command.

voice confirmation-tone
no voice confirmation-tone

Syntax Description

This command has no arguments or keywords.

Command Default

The two-beep confirmation tone is heard on PLAR and PLAR OPX connections.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on Cisco MC3810.

Usage Guidelines

Use this command to disable the two-beep confirmation tone that a caller hears when picking up the handset for PLAR and PLAR OPX connections. This command is valid only if the voice-port **connection** command is set to PLAR or PLAR OPX.

Examples

The following example disables the two-beep confirmation tone on voice port 1/0/0:

```
voice-port 1/0/0
 connection plar-opx
 voice confirmation-tone
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.

voice dnis-map

To create or modify a Digital Number Identification Service (DNIS) map, use the **voice dnis-map** command in global configuration mode. To delete a DNIS map, use the **no** form of this command.

voice dnis-map *map-name* [*url*]
no voice dnis-map map-name

Syntax Description

map-name	Name of the DNIS map.
url	(Optional) URL of an external text file that contains a list of DNIS entries.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 3640 and Cisco 3660.

Usage Guidelines

A DNIS map is a table of DNIS numbers associated with a single dial peer. For applications such as VoiceXML, using a DNIS map makes it possible to configure a single dial peer for all DNIS numbers used to refer to VoiceXML documents. Keep the following considerations in mind when using voice DNIS maps.

- A separate entry must be made for each DNIS entry in a DNIS map. Wildcards are not supported.
- If a URL is not supplied, the command enters DNIS-map configuration mode, permitting the entry of DNIS numbers by using the **dnis** command.
- The URL argument points to the location of an external text file containing a list of DNIS entries **(**forexample: tftp://dnismap.txt). This allows the administrator to maintain a single primary file of all DNIS map entries, if desired, rather than configuring the DNIS entries on each gateway.

The name of the text file extension is not significant; .doc, .txt, or .cfg are all acceptable because the extension is not checked. The entries in the file should look the same as a DNIS entry configured in Cisco IOS software (for example: dnis 5553305 url tftp://global/tickets/movies.vxml).

- External text files used for DNIS maps must be stored on TFTP servers; they cannot be stored on HTTP servers.
- To associate a DNIS map with a dial peer, use the **dnis-map** command.
- To view the configuration information for DNIS maps, use the **show voice dnis-map** command.

Examples

The following example shows how the voice dnis-map command is used to create a DNIS map:

```
voice dnis-map dmap1
```

The following example shows the voice dnis-map command used with a URL that specifies the location of a text file containing the DNIS entries:

```
voice dnis-map dmap2 tftp://keyer/dmap2/dmap2.txt
```

Following is an example of the contents of a text file comprising a DNIS map:

```
!Example dnis-map with 8 entries.
!
dnis 5550112 url tftp://global/ticket/vapptest1.vxml
dnis 5550111 url tftp://global/ticket/vapptest2.vxml
dnis 5550134 url tftp://global/ticket/vapptest3.vxml
dnis 5550178
dnis 5550100
dnis 5550101
dnis 5550102
dnis 5550103
```

Related Commands

Command	Description
dnis	Adds a DNIS number to a DNIS map.
dnis-map	Associates a DNIS map with a dial peer.
show voice dnis-map	Displays configuration information about DNIS maps.
voice dnis-map load	Reloads a DNIS map that has changed since the previous load.

voice dnis-map load

To reload a DNIS map that has been modified, use the **voice dnis-map load** command in privileged EXEC mode. This command does not have a **no** form.

voice dnis-map load *map-name*

Syntax Description

map-name	Name of the DNIS map to reload.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 3640 and Cisco 3660.

Usage Guidelines

This command reloads a DNIS map residing on an external server. Use this command when the DNIS map file has changed since the previous load.

To create or modify a DNIS map, use the **voice dnis-map** command.

Examples

The following example reloads a DNIS map named "mapfile1":

```
Router# voice dnis-map load mapfile1
```

Related Commands

Command	Description
dnis	Adds a DNIS number to a DNIS map.
dnis-map	Associates a DNIS map with a dial peer.
show voice dnis-map	Displays configuration information about DNIS maps.
voice dnis-map	Enters DNIS map configuration mode to create a DNIS map.

voice dsp crash-dump

To enable the crash dump feature and to specify the destination file and the file limit, enter the **voice dsp crash-dump**command in global configuration mode. To disable the feature, use the **no** form of the command.

voice dsp crash-dump [**destination** *url* | **file-limit** *limit-number*]
no voice dsp crash-dump

Syntax Description

destination *url*	Designates a valid file system where crash dump analysis is stored. The *url* argument must be set to a valid file system. The destination url can be one of the following • The file on a TFTP server with the following format: tftp://x.x.x.x/subfolder/filename. The x.x.x.x value is the IP address of the TFTP server • The file on the flashcard of the router, with the following format: slot0:filename **Note** The digital signal processor (DSP) crash dump feature is disabled when either the crash-dump destination is not specified.
file-limit *limit-number*	The crash dump file-limit keyword must be set to a non-zero value. The default is that the crash dump capability is turned off, as the url argument is empty, and the file-number argument is zero. The limit-number argument may range from 0 (no file will be written) to 99. **Note** The DSP crash dump feature is disabled when the crash-dump file limit is set to 0.

Command Default

Crash dump capability is turned off.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

To configure the router to write a crash dump file, the destination url in the **voice dsp crash-dump** command must be set to a valid file system, and the crash dump file limit must be set to a non-zero value. The default is that the crash dump capability is turned off, as the url field is empty, and the file limit is zero.

As each crash-dump file is created, the name of the file has a number appended to the end. This number is incremented from 1 to up to the file limit for each subsequent crash dump file written. If the router reloads, the number is reset back to 1, and so file number 1 is written again. After the file number reaches the maximum file limit, no more files are written.

The file count can be manually reset by setting the file limit to zero and then setting it to a non-zero limit. This has the effect of restarting the count of files written, causing the files 1 to the file limit of 99 to be able to be written again, thus overwriting the original files.

Setting the file-number argument to zero (the default) disables the collection of the dump from the DSP. In this case, the memory is not collected from the DSP, and the stack is not displayed on the console. If the keepalive mechanism detects a crashed DSP, the DSP is simply restarted.

Setting the file-number argument to a non-zero number but having a null destination url causes the dump to be collected and the stack to be displayed on the console, but no dump file is written.

If auto-recovery is turned off for the router, no DSP dump functions are enabled, no keepalive checks are done, and no dumps are collected or written.

Note Some types of flash need to be completely erased to free up space from deleted files, and some types of flash cannot have files overwritten with new versions until the entire flash is erased. As a result, you might want to set the file limit so that only one or two dump files are written to flash. This prevents flash from being filled up.

Note It is not recommended to write crash dump files to internal flash or bootflash, because these files are normally used to hold configuration information and Cisco IOS software images. Cisco recommends writing crash dump files to spare flash cards, which can be inserted into slot 0 or slot 1 on many of the routers. These cards usually do not hold critical information and may be erased. Additionally, these cards can be conveniently removed from the router and sent to Cisco, so that the crash dump files can be analyzed.

Examples

The following example enables the crash dump feature and specifies the destination file in slot 0:

```
Router configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# voice dsp crash-dump destination slot0:banjo-152-s
Router# end
1w0d:%SYS-5-CONFIG_I:Configured from console by console
```

Check your configuration by entering the show voice dsp crash-dump command in privileged EXEC configuration mode:

```
Router# show voice dsp crash-dump
Voice DSP Crash-dump status:
    Destination file url is slot0:banjo-152-s
File limit is 20
    Last DSP dump file written was
          tftp://112.29.248.12/tester/26-152-t2
    Next DSP dump file written will be slot0:banjo-152-s1
```

Related Commands

Command	Description
debug voice dsp crash-dump	Displays crash dump debug information.
show voice dsp crash-dump	Displays voice dsp crash dump information.

voice dsp invalid-msg drop

To drop the invalid Digital Signal Processor (DSP) messages, use the **voice dsp invalid-msg drop** command in global configuration mode. To disable this feature, use the **no** form of the command.

voice dsp invalid-msg drop
no voice dsp invalid-msg drop

Command Default

Invalid DSP messages are not dropped.

Command Modes

Global configuration (config)

Command History

Release	Modification
IOS XE Fuji Release 16.8.1	This command was introduced.

Usage Guidelines

The Voice DSP Control Message Logger feature enables debugging of the logged control messages to examine voice- related problems. Use the **voice dsp invalid-msg drop** command to drop the messages that are invalid.

Examples

The following example drops the invalid DSP messages.

```
Router# voice dsp invalid-msg drop
```

voice echo-canceller extended

To enable the extended G.168 echo canceller (EC) on the Cisco 1700 series, Cisco ICS7750, or Cisco AS5300, use the **voice echo-canceller extended**command in global configuration mode. To reset to the default, use the **no** form of this command.

Cisco 1700 series and Cisco ICS 7750
voice echo-canceller extended
no voice echo-canceller extended

Cisco AS5300
voice echo-canceller extended [**codec small** *codec* **large** *codec*]
no voice echo-canceller extended

Syntax Description

codec	(Optional) Defines restricted codecs, both small and large.
small *codec*	Small footprint codec. Valid values for the *codec* argument are: • **g711** • **g726**
large *codec*	Large footprint codec. Valid values for the *codec* argument are: • **fax-relay** • **g723** • **g728** • **g729** • **gsmefr** • **gsmfr**

Command Default

Proprietary Cisco G.165 EC is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.3(3)	This command was modified to allow unrestricted codecs on the Cisco AS5300. The **codec** keyword was made optional.

Usage Guidelines

Cisco 1700 series and Cisco ICS7750

You do not have to shut down all the voice ports on the Cisco 1700 series or Cisco ICS7750 to switch the echo canceller, but you should make sure that when you switch the echo canceller, there are no active calls on the router.

Because echo cancellation is an invasive process that can minimally degrade voice quality, you should disable this command if it is not needed.

Cisco AS5300

This command is available only on the Cisco AS5300 with C542 or C549 digital signal processor module (DSPM) high-complexity firmware.

The **voice echo-canceller extended** command enables the extended EC on a Cisco AS5300 using C549 DSP firmware with one channel of voice per DSP and unrestricted codecs. Any codec is supported.

The **voice echo-canceller extended codec** command enables the extended EC on a Cisco AS5300 using C542 or C549 DSP firmware with two channels of voice per DSP and restricted codecs. Only specific codecs can be used with the extended EC.

If fax-relay is not selected as the large codec, the VoIP dial peer requires that you use the fax rate disabled command in dial-peer configuration mode.

After choosing the codecs to be supported by the extended echo canceller, either remove all dial peers with different codecs not supported by your new configuration or modify the dial-peer codec selection by selecting a voice codec or fax-relay. When codecs are restricted, only one selection is allowed. You must have a VoIP dial peer configured with an extended EC-compatible codec to ensure voice quality on the connection.

This command is not accepted if there are active calls. If the EC is already in effect and a codec choice is changed, the system scans the dial peers. Any dial peers that do not conform to the new global command settings are changed, and the user is informed of the changes. Similarly, modem relay is incompatible with the extended EC and must be disabled globally for all dial peers.



Note This command is valid only when the **echo-cancel enable** command and the echo-cancel coveragecommand are enabled.

Examples

The following example sets the extended G.168 EC on the Cisco 1700 series or Cisco ICS7750:

```
Router(config)# voice echo-canceller extended
```

The following example sets the extended G.168 EC on the Cisco AS5300 with restricted codecs:

```
Router(config)# voice echo-canceller extended codec small g711 large g726
```

The following example shows an error message that displays when a restricted codec is not allowed:

```
Cannot configure now, dial-peer 8800 is configured with codec=g728, fax rate=disable,
modem=passthrough system.If necessary set this command to 'no', re-configure dial-peer
codec, fax rate and/or modem. Then re-enter this command.
```

In the above example, dial peer 8800 is misconfigured with a codec type, g728, that was not selected for the large codec type using the **voice echo-canceller extended** command.

Related Commands

Command	Description
echo-cancel coverage	Enables the cancellation of voice that is sent out the interface and is received on the same interface.
echo-cancel enable	Enables the cancellation of voice that is sent and received on the same interface.

voice enum-match-table

To create an ENUM match table for voice calls, use the **voice enum-match-table** in global configuration mode. To delete the ENUM match table, use the **no**form of this command.

voice enum-match-table *table-number*
no voice enum-match-table *table-number*

Syntax Description

table-number	Number of the ENUM match table. Range is from 1 to 15. There is no default value.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

The ENUM match table is a set of rules for matching incoming calls. When a call comes in, its called number is matched against the match pattern of the rule with the highest preference.

If it matches, the replacement pattern is applied to the number. The resulting number and the domain name of the rule are used to make an ENUM query.

If the called number does not match the match pattern, the next rule in order of preference is selected.

Examples

The following example creates ENUM match table 3 for voice calls:

```
Router(config)# voice enum-match-table 3
Router(config-enum)# rule 1 5/(.*)/ /\1/e164.cisco.com
Router(config-enum)# rule 2 4/^9011\(.*\)/ /\1/e164.arpa
```

In this table, rule 1 matches any number. The resulting number is the same as the called number. That number and the domain name "e164.cisco.com" are used to make an ENUM query.

Rule 2 matches any number that starts with 9011. The 9011 is removed from the incoming number. The resulting number and the domain name "e164.arpa" are used for the ENUM query.

Suppose an incoming call has a called number of 4085550112. [Rule 2 is applied] first because it has a higher preference. The first few digits, 4085, do not match the 9011 pattern of rule 2, so [rule 1 is applied] next. The called number matches rule 1, and the resulting number is 4085550112. This number and "e164.cisco.com" form the ENUM query (2.1.2.1.5.5.5.8.0.4.e164.cisco.com).

Related Commands

Command	Description
rule (ENUM configuration)	Defines the matching, replacement, and rejection patterns for an ENUM match table.
show voice enum-match-table	Displays the configuration of voice ENUM match tables.

Command	Description
test enum	Tests the functionality of an ENUM match table.

voice hpi capture

To allocate the Host Port Interface (HPI) capture buffer size (in bytes) and to set up or change the destination URL for captured data, use the **voice hpi capture** command in global configuration mode. To stop all logging and file operations, to disable data transport from the capture buffer, and to automatically set the buffer size to 328, use the **no** form of this command.

voice hpi capture [**buffer** *size* | **destination** *url*]
no voice hpi capture buffer *size*

Syntax Description

buffer *size*	(Optional) Size of HPI capture buffer, in bytes. Range is from 328 to 9000000. The default is 328.
destination *url*	(Optional) Destination URL for storing captured data.

Command Default

328 bytes (no buffer is used if it is not configured explicitly)

Command Modes

Global configuration

Command History

Release	Modification
12.2(10)	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

If you want to change the size of an existing non-zero buffer, you must first reset it to 0 and then change it from 0 to the new size.

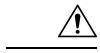
The **destination***url* option sets up or changes the destination URL for captured data. To disable data transport from the capture buffer, use the **no** form of the command. If the buffer is allocated, captured data is sent to the current URL (if it was already configured) until the new URL is specified.

If a new URL differs from the current URL and logging is enabled, the current URL is closed and all further data is sent to the new URL. Entering a blank URL or prefixing the command with **no** disables data transport from the capture buffer, and (if capture is enabled) captured data is stored in the capture buffer until it reaches its capacity.

Once the buffer-queueing program is running, the transport process attempts to connect to a new or existing "capture destination" URL. A version message is written to the URL, and if the message is successfully received, any further messages placed into the message queue are written to that URL. If a new URL is entered using the voice hpi capture destination url command, the open URL is closed, and the system attempts to write to the new URL. If the new URL does not work, the transport process exits. The transport process is restarted when another URL is entered or the system is restarted.

The buffer size option sets the maximum amount of memory (in bytes) that the capture system allocates for its buffers when it is active. The capture buffer is where the captured messages are stored before they are sent to the URL specified by the capture destination. The system is started by choosing the amount of memory (greater than 0 bytes) that the buffer-queueing system can allocate to the free message pool. HPI messages can then be captured until buffer capacity is reached. Entering **0** for the buffer size and prefixing the command with **no** stops all logging and file operations and automatically sets the buffer size to 0.

The **voice hpi capture** command can be saved with the router configuration so that the command is active during router startup. This allows you to capture the HPI messages sent during router bootup before the CLI is enabled. After you have configured the buffer size in the running configuration (valid range is from 328 to 9000000), save it to the startup configuration using the **write** command or to the TFTP server using the **copy run tftp** command.



Caution Using the message logger feature in a production network environment impacts CPU and memory usage on the gateway.

Examples

The following example changes the size (in bytes) of the HPI capture buffer and initializes the buffer-queueing program:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# voice hpi capture buffer 40000
Router(config)# end
Router#
03:23:31:caplog:caplog_cli_interface:hpi capture buffer size set to 40000 bytes
03:23:31:caplog:caplog_logger_init:TRUE, Started task HPI Logger (PID 64)
03:23:31:caplog:caplog_cache_init:TRUE, malloc_named(39852), 123 elements (each 324 bytes
big)
03:23:31:caplog:caplog_logger_proc:Attempting to open ftp://172.23.184.233/c:b-38-117
03:23:32:%SYS-5-CONFIG_I:Configured from console by console
Router#
```

The following example sets the capture destination by entering a destination URL using FTP:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# voice hpi capture destination ftp://172.23.184.233/c:b-38-117a
Router(config)#
04:05:10:caplog:caplog_cli_interface:hpi capture destination:ftp://172.23.184.233/c:b-38-117a
04:05:10:caplog:caplog_logger_init:TRUE, Started task HPI Logger (PID 19)
04:05:10:caplog:caplog_cache_init:Cache must be at least 324 bytes
04:05:10:caplog:caplog_logger_proc:Terminating...
Router(config)# end
Router#
```

Related Commands

Command	Description
debug hpi	Turns on the debug output for the logger.
show voice hpi capture	Displays the capture status and statistics.

voice hunt

To configure an originating or tandem router so that it continues dial-peer hunting if it receives a specified disconnect cause code from a destination router, use the **voice hunt** command in global configuration mode. To configure the router so that it stops dial-peer hunting if it receives a specified disconnect cause code (the default condition), use the **no** form of this command. To restore the default dial-peer hunt setting, use the **default** form of this command.

voice hunt { *disconnect-cause-code* | **all** }
no voice hunt { *disconnect-cause-code* | **all** }
default voice hunt

Syntax Description

disconnect-cause-code	A code returned from the destination router to indicate why an attempted end-to-end call was unsuccessful. If the specified disconnect cause code is returned from the last destination endpoint, dial peer hunting is enabled or disabled. The table below in the "Usage Guidelines" section describes the possible values. You can enter the keyword, decimal value, or hexadecimal value.
all	Continue dial-peer hunting for all disconnect cause codes returned from the destination endpoint.
default	Restores the default dial-peer hunt setting, that is, the router stops dial-peer hunting if it receives the user-busy or no-answer disconnect cause code.

Command Default

The router stops dial-peer hunting if it receives the user-busy or no-answer disconnect cause code.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced for VoFR on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810. It was also introduced for VoIP on the Cisco 2600 series and Cisco 3600 series.
12.0(7)T	This command was implemented for VoIP on the Cisco AS5300 and Cisco AS5800.
12.0(7)XK	This command was implemented for VoIP on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T and implemented for VoIP on the Cisco MC3810.
12.1(3)XI	The **invalid-number**and **unassigned-number** keywords were added, and the command name was changed to **voice hunt**.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	Keywords were added for more disconnect cause codes.
12.3(8)T	The *disconnect-cause-code* argument was modified to accept nonstandard disconnect cause codes.

Usage Guidelines

This command is used with routers that act as originating or tandem nodes in a VoIP, VoFR, or Voice over ATM environment.

For an outgoing call from an originating VoIP gateway configured for rotary dial-peer hunting, more than one dial peer may match the same destination number. The matching dial peers may have different routes. After the voice call using the first dial peer gets disconnected, it will return a disconnect cause code. To have the router to pick up the next matching dial peer in the rotary group and set up a call, the router must be configure to continue hunting the various routes. Use this command to configure the router's hunting behavior when specified cause codes are received.

You can use this command to enable and disable dial-peer hunting when nonstandard disconnect cause codes are received. Nonstandard disconnect cause codes are those that are not defined in ITU-T Recommendation Q.931, but are used by service providers. When this command is used to disable dial-peer hunting for a specific disconnect cause code, it appears in the running configuration of the router.

The disconnect cause codes are described in the table below. The decimal and hexadecimal value of the disconnect cause code follows the description of each possible keyword.



Note While configuring **voice hunt**, it is necessary to configure **reason header override** in the sip-ua configuration mode to ensure that correct cause codes are sent to the other leg. For more information on **reason header override** configuration, see reason-header override command.

Table 7: Standard Disconnect Cause Codes

Keyword	Description	Decimal	Hex
access-info-discard	Access information discarded.	43	0x2b
all	Continue dial-peer hunting for all disconnect cause codes received from a destination router.		
b-cap-not-implemented	Bearer capability not implemented.	65	0x41
b-cap-restrict	Restricted digital information bearer capability only.	70	0x46
b-cap-unauthorized	Bearer capability not authorized.	57	0x39
b-cap-unavail	Bearer capability not available.	58	0x3a
call-awarded	Call awarded.	7	0x7
call-cid-in-use	Call exists, call ID in use.	83	0x53
call-clear	Call cleared.	86	0x56
call-reject	Call rejected.	21	0x15
cell-rate-unavail	Cell rate not available.	37	0x25
channel-unacceptable	Channel unacceptable.	6	0x6
chantype-not-implement	Channel type not implemented.	66	0x42

Keyword	Description	Decimal	Hex
cid-in-use	Call ID in use.	84	0x54
codec-incompatible	Codec incompatible.	171	0xab
cug-incalls-bar	Closed user group (CUG) incoming calls barred.	55	0x37
cug-outcalls-bar	CUG outgoing calls barred.	53	0x35
dest-incompatible	Destination incompatible.	88	0x58
dest-out-of-order	Destination out of order.	27	0x1b
dest-unroutable	No route to destination.	3	0x3
dsp-error	Digital signal processor (DSP) error.	172	0xac
dtl-trans-not-node-id	Designated transit list (DTL) transit not my node ID.	160	0xa0
facility-not-implemented	Facility not implemented.	69	0x45
facility-not-subscribed	Facility not subscribed.	50	0x32
facility-reject	Facility rejected.	29	0x1d
glare	Glare.	15	0xf
glaring-switch-pri	Glaring switch PRI.	180	0xb4
htspm-oos	Holst Telephony Service Provider Module (HTSPM) out of service.	129	0x81
ie-missing	Mandatory information element missing.	96	0x60
ie-not-implemented	Information element not implemented.	99	0x63
info-class-inconsistent	Inconsistency in information and class.	62	0x3e
interworking	Interworking.	127	0x7f
invalid-call-ref	Invalid call reference value.	81	0x51
invalid-ie	Invalid information element contents.	100	0x64
invalid-msg	Invalid message.	95	0x5f
invalid-number	Invalid number.	28	0x1c
invalid-transit-net	Invalid transit network.	91	0x5b
misdialled-trunk-prefix	Misdialed trunk prefix.	5	0x5
msg-incomp-call-state	Message in incomplete call state.	101	0x65
msg-not-implemented	Message type not implemented.	97	0x61

Keyword	Description	Decimal	Hex
msgtype-incompatible	Message type not compatible.	98	0x62
net-out-of-order	Network out of order.	38	0x26
next-node-unreachable	Next node unreachable.	128	0x80
no-answer	No user answer.	19	0x13
no-call-suspend	No call suspended.	85	0x55
no-channel	Channel does not exist.	82	0x52
no-circuit	No circuit.	34	0x22
no-cug	Nonexistent CUG.	90	0x5a
no-dsp-channel	No DSP channel.	170	0xaa
no-req-circuit	No requested circuit.	44	0x2c
no-resource	No resource.	47	0x2f
no-response	No user response.	18	0x12
no-voice-resources	No voice resources available.	126	0x7e
non-select-user-clear	Nonselected user clearing.	26	0x1a
normal-call-clear	Normal call clearing.	16	0x10
normal-unspecified	Normal, unspecified.	31	0x1f
not-in-cug	User not in CUG.	87	0x57
number-changeed	Number changed.	22	0x16
param-not-implemented	Nonimplemented parameter passed on.	103	0x67
perm-frame-mode-oos	Permanent frame mode out of service.	39	0x27
perm-frame-mode-oper	Permanent frame mode operational.	40	0x28
precedence-call-block	Precedence call blocked.	46	0x2e
preempt	Preemption.	8	0x8
preempt-reserved	Preemption reserved.	9	0x9
protocol-error	Protocol error.	111	0x6f
qos-unavail	QoS unavailable.	49	0x31
rec-timer-exp	Recovery on timer expiry.	102	0x66
redirect-to-new-destination	Redirect to new destination.	23	0x17

Keyword	Description	Decimal	Hex
req-vpci-vci-unavail	Requested VPCI VCI not available.	35	0x23
send-infotone	Send information tone.	4	0x4
serv-not-implemented	Service not implemented.	79	0x4f
serv/opt-unavail-unspecified	Service or option not available, unspecified.	63	0x3f
stat-enquiry-resp	Response to status enquiry.	30	0x1e
subscriber-absent	Subscriber absent.	20	0x14
switch-congestion	Switch congestion.	42	0x2a
temp-fail	Temporary failure.	41	0x29
transit-net-unroutable	No route to transit network.	2	0x2
unassigned-number	Unassigned number.	1	0x1
unknown-param-msg-discard	Unrecognized parameter message discarded.	110	0x6e
unsupported-aal-parms	ATM adaptation layer (AAL) parameters not supported.	93	0x5d
user-busy	User busy.	17	0x11
vpci-vci-assign-fail	Virtual path connection identifier virtual channel identifier (VPCI VCI) assignment failure.	36	0x24
vpci-vci-unavail	No VPCI VCI available.	45	0x2d

Examples

The following example configures the originating or tandem router to continue dial-peer hunting if it receives a user-busy disconnect cause code from a destination router:

```
voice hunt user-busy
```

The following example configures the originating or tandem router to continue dial-peer hunting if it receives an invalid-number disconnect cause code from a destination router:

```
voice hunt 28
```

The following example configures the originating or tandem router to continue dial-peer hunting if it receives a facility-not-subscribed disconnect cause code from a destination router:

```
voice hunt 0x32
```

Related Commands

Command	Description
huntstop	Disables all further dial-peer hunting if a call fails when using hunt groups.
preference	Indicates the preferred order of a dial peer within a rotary hunt group.

voice iec syslog

To enable viewing of Internal Error Codes as they are encountered in real time, use the voice iec syslog command in global configuration mode. To disable IEC syslog messages, use the **no** form of this command.

voice iec syslog
no voice iec syslog

Syntax Description

This command has no arguments or keywords.

Command Default

IEC syslog messages are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Cupertino 17.7.1	Introduced support for YANG models.

Examples

The following example enables IEC syslog messages:

```
Router(config)# voice iec syslog
```

Related Commands

Command	Description
clear voice statistics	Clears voice statistics, resetting the statistics collection.
show voice statistics iec	Displays iec statistics
show voice statistics interval-tag	Displays interval options available for IEC statistics
voice statistics type iec	Enables collection of IEC statistics

voice local-bypass

To configure local calls to bypass the digital signal processor (DSP), use the **voice local-bypass command in**global configuration mode. To direct local calls through the DSP, use the **no** form of this command.

voice local-bypass
no voice local-bypass

Syntax Description

This command has no arguments or keywords.

Command Default

Local calls bypass the DSP.

Command Modes

Global configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced.
12.0(7)XK	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Local calls (calls between voice ports on a router or concentrator) normally bypass the DSP to minimize use of system resources. Use the **no** form of the **voice local-bypass**command if you need to direct local calls through the DSP. Input gain and output attenuation can be configured only if calls are directed through the DSP.

Examples

The following example configures a Cisco router to pass local calls through the DSP:

```
no voice local-bypass
```

Related Commands

Command	Description
input gain	Configures a specific input gain value.
output attenuation	Configures a specific output attenuation value.

voice mlpp

To enter MLPP configuration mode to enable MLPP service, use the voice service command in global configuration mode. To disable MLPP service, use the **no** form of this command.

voice mlpp
no voice mlpp

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

G
lobal configuration (config)

Command History

Cisco IOS Release	Cisco Products	Modification
12.4(22)YB	Cisco Unified CME 7.1	This command was introduced.
12.4(24)T	Cisco Unified CME 7.1	This command was integrated into Cisco IOS Release 12.4(24)T.

Voice-mlpp configuration mode is used for the gateway globally.

Examples

The following example shows how to enter voice-mlpp configuration mode:

```
Router(config)# voice mlpp
Router(config-voice-mlpp)# access-digit
```

Related Commands

Command	Description
access-digit	Defines the access digit that phone users dial to request a precedence call.
mlpp preemption	Enables calls on an SCCP phone or analog FXS port to be preempted.
preemption trunkgroup	Enables preemption capabilities on a trunk group.

voicemail (stcapp-fsd)

To designate an SCCP telephony control (STC) application feature speed-dial code to speed dial the voice-mail number, use the **voicemail** command in STC application feature speed-dial configuration mode. To return the code to its default, use the **no** form of this command.

voicemail *keypad-character*
no voicemail

Syntax Description

keypad-character	One or two digits that can be dialed on a telephone keypad. Range is 0 to 9 for one-digit codes; 00 to 99 for two-digit codes. Default is 0 (zero) for one-digit codes; 00 (two zeroes) for two-digit codes. **Note** Number of digits depends on the value set with the **digit** command.

Command Default

The default voice-mail code is 0 (zero) for one-digit codes; 00 (two zeros) for two-digit codes.

Command Modes

STC application feature speed-dial configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(6)T	The *keypad-character* argument was modified to allow two-digit codes.

Usage Guidelines

This command is used with the STC application, which enables certain features on analog FXS endpoints that use Skinny Client Control Protocol (SCCP) for call control.

To use the speed-dial to voice-mail feature on a phone, dial the feature speed-dial (FSD) prefix and the code that has been configured with this command (or the default if this command was not used). For example, if the FSD prefix is * (the default), and you want to dial the voice-mail phone number, dial *0.

Note that the number that will be speed-dialed for voice mail must be set on Cisco CallManager or the Cisco CallManager Express system.

This command is reset to its default value if you modify the value of the **digit** command. For example, if you set the **digit** command to 2, then change the **digit** command back to its default of 1, the voice-mail FSD code is reset to 0 (zero).

If you set this code to a value that is already in use for another FSD code, you receive a warning message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **show stcapp feature codes** command.

The **show running-config** command displays nondefault FSD codes only. The **show stcapp feature codes** command displays all FSD codes.

Examples

The following example sets an FSD prefix of two pound signs (##) and a voice-mail code of 8. After these values have been configured, a phone user presses ##8 to dial the voice-mail number.

```
Router(config)# stcapp feature speed-dial
Router(stcapp-fsd)# prefix ##
Router(stcapp-fsd)# voicemail 8
Router(stcapp-fsd)# exit
```

Related Commands

Command	Description
digit	Designates the number of digits for STC application feature speed-dial codes.
prefix (stcapp-fsd)	Designates a prefix to precede the dialing of an STC application feature speed-dial code.
redial	Designates an STC application feature speed-dial code to dial again the last number that was dialed.
show running-config	Displays current nondefault configuration settings.
show stcapp feature codes	Displays configured and default STC application feature codes.
speed dial	Designates a range of STC application feature speed-dial codes.
stcapp feature speed-dial	Enters STC application feature speed-dial configuration mode to set feature speed-dial codes.

voice pcm capture

To allocate the number of Pulse Code Modulation (PCM) capture buffers, to set up or change the destination URL for captured data, to enable PCM capture on-demand, and to change the PCM capture trigger string by the user, use the **voice pcm capture** command in global configuration mode. To stop all logging and file operations, to disable data transport from the capture buffer, and to automatically set the number of buffers to 0, use the **no** form of this command.

voice pcm capture {**buffer** *number* | **destination** *url* | **on-demand-trigger** | **user-trigger-string** *start-string stop-string* **stream** *bitmap* **duration** *call-duration*}
no voice pcm capture {**buffer** *number* | **destination** *url* | **on-demand-trigger** | **user-trigger-string**}

Syntax Description

buffer *number*	Allocates the number of PCM capture buffers. The range is from 0 to 200000. The default is 0.
destination *url*	Specifies the destination URL for storing captured data.
on-demand-trigger	(Optional) Configures PCM capture user trigger on-demand.
user-trigger-string *start-string stop-string* **stream** *bitmap* **duration** *call-duration*	(Optional) Configures PCM user trigger string. • *start-string*—Start string up to 15 characters. • *stop-string*—Stop string up to 15 characters. • **stream**—Configures the PCM capture stream bitmap. • *bitmap*—PCM stream bitmap in hexadecimal. The range is from 1 to FFFFFFF. The default is 7. • **duration**—Configures the duration for PCM capture. • *call-duration*—Duration of call. The range is from 0 to 255. The default is 0.

Command Default

The default values are as follows:

- Number of buffers: 0
- Start string: 123
- Stop string: 456
- Stream: 7
- Call duration: 0

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

If you want to change the number of an existing nonzero buffer, you must first reset it to 0 and then change it from 0 to the new number.

The **destination** *url* option sets up or changes the destination URL for captured data. To disable data transport from the capture buffer, use the **no** form of this command. If the buffer is allocated, captured data is sent to the current URL (if it was already configured) until the new URL is specified.

If a new URL differs from the current URL and logging is enabled, the current URL is closed and all further data is sent to the new URL. Entering a blank URL or prefixing the command with **no** disables data transport from the capture buffer, and (if capture is enabled) captured data is stored in the capture buffer until it reaches its capacity.

Once the buffer-queueing program is running, the transport process attempts to connect to a new or existing "capture destination" URL. A version message is written to the URL, and if the message is successfully received, any further messages placed into the message queue are written to that URL. If a new URL is entered using the **voice pcm capture destination url** command, the open URL is closed, and the system attempts to write to the new URL. If the new URL does not work, the transport process exits. The transport process is restarted when another URL is entered or the system is restarted.

Examples

The following example shows how to configure the number of PCM capture buffers:

```
Router> enable
Router# configure terminal
Router(config)# voice pcm capture buffer 200
```

The following example shows how to configure the destination URL for storing captured data:

```
Router> enable
Router# configure terminal
Router(config)# voice pcm capture destination tftp://10.0.1.10/acphan/
```

The following example shows how to configure user trigger PCM capture:

```
Router> enable
Router# configure terminal
Router(config)# voice pcm capture on-demand-trigger
```

The following example shows how to change the default user trigger PCM capture start and stop string, stream, and call duration:

```
Router> enable
Router# configure terminal
Router(config)# voice pcm capture #132 #543 stream ff duration 230
```

Related Commands

Command	Description
show voice pcm capture	Displays PCM capture status and statistics.

voice-phone-proxy

To create a voice phone proxy instance and to enter phone-proxy configuration mode, use the **voice-phone-proxy** command in global configuration mode. To remove a voice phone proxy instance use the **no** form of the command.

voice-phone-proxy *pp-name*
no voice-phone-proxy *pp-name*

Syntax Description

pp-name	The phone proxy instance name.

Command Default

none

Command Modes

Global configuration mode (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

The **voice-phone-proxy** command allows you to create an instance of a voice phone proxy. In phone-proxy configuration mode you can specify settings such as the service and server settings for the phone proxy instance.

Example

The following example shows how to create a phone proxy instance called first-pp, enter phone-proxy configuration mode, set the description for this instance, and specify a Certificate Trust List (CTL) file for this cluster:

```
Device(config)# voice-phone-proxy first-pp
Device(config-phone-proxy)# description cluster-test
Device(config-phone-proxy)# ctl-file my-cluster-test-ctl-file
```

voice-phone-proxy file-buffer

To create the phone proxy buffer files, use the **voice-phone-proxy file-buffer** command in global configuration mode.

voice-phone-proxy file-buffer size *size* **aging** *time*

Syntax Description

size *size*	Buffer size in MB. The range is from 10 to 60.
aging	Checks the age of the phone proxy buffer files.
time	Time in seconds. The range is from 10 to 3600. Based on the set time, the file buffer will be periodically checked.

Command Default

No default phone proxy exists.

Command Modes

Global configuration (config)

Command History

Release	Modification
IOS XE Fuji Release 16.8.1	This command was introduced.

Usage Guidelines

The maximum buffer size that can be allocated for the phone proxy buffer files is 60 MB. If the buffer size exceeds the threshold value, new phone proxy buffer files cannot be created. To remove the old buffer files, use the command **voice-phone-proxy file-buffer size** *size* **aging** *time* . Based on the set time, the buffer will be checked at regular intervals and the old phone proxy buffer files will be removed if the buffer size exceeds the maximum limit.

Example

The following example sets the file buffer size as 30 MB and checks the file buffer at an interval of 100 seconds.

```
Router (config)# voice-phone-proxy file-buffer size 30 aging 100
```

voice-phone-proxy tftp-address

To specify the IP address and VRF name of the TFTP server and to enter phone-proxy configuration mode, use the **voice-phone-proxy tftp-address** command in global configuration mode. To remove the IP address and VRF name of the TFTP server, use the **no** form of the command.

voice-phone-proxy tftp-address {**ipv4** *ipv4-address* | **ipv6** *ipv6-address* } [**vrf** *vrf-name*]
no voice-phone-proxy tftp-address {**ipv4** *ipv4-address* | **ipv6** *ipv6-address* } [**vrf** *vrf-name*]

Syntax Description

ipv4 *ipv4-address*	IPv4 address of the TFTP server.
ipv6 *ipv6-address*	IPv6 address of the TFTP server.
vrf *vrf-name*	Name of the TFTP server's VRF.

Command Default

No IP address or VRF name of the TFTP server is specified.

Command Modes

Global configuration mode (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.
IOS XE Fuji Release 16.8.1	This command was enhanced to add the ipv6 keyword.

Example

The following example shows how to specify the IP address and VRF of the TFTP server:

```
Device(config)# phone-proxy tftp-address ipv4 198.51.100.1 vrf vrf1
```

voiceport

To enable a private line automatic ringdown (PLAR) connection for an analog phone, use the **voiceport** command in SCCP PLAR configuration mode. To remove PLAR from the voice port, use the **no** form of this command.

voiceport *port-number* **dial** *dial-string* [**digit** *dtmf-digits* [**wait-connect** *wait-msecs*] [**interval** *inter-digit-msecs*]]
no voiceport *port-number*

Syntax Description

port-number	Analog foreign exchange station (FXS) voice port number. Range: 2/0 to 2/23.
dial *dial-string*	String of up to 16 characters that can be dialed on a telephone keypad. Valid characters are 0 through 9, A through D, an * (asterisk) and # (pound sign). The voice gateway sends this string to the call-control system when the analog phone goes off hook.
digit *dtmf-digits*	(Optional) String of up to 16 characters that can be dialed on a telephone keypad. Valid characters are 0 through 9, A through D, an * (asterisk), # (pound sign), and comma (,). The voice gateway sends this string to the call-control system after the *wait-msecs* expires. Each comma represents a one second wait.
wait-connect *wait-msecs*	(Optional) Number of milliseconds that the voice gateway waits after voice cut-through before out-pulsing the DTMF digits. Range: 0 to 30000, in multiples of 50. Default: 50. If 0, DTMF digits are sent automatically by voice gateway after call is connected.
interval *inter-digit-msecs*	(Optional) Number of milliseconds between the DTMF digits. Range: 50 to 500, in multiples of 50. Default: 50.

Command Default

Disabled (PLAR is not set for the voice port).

Command Modes

SCCP PLAR configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command enables PLAR on analog FXS ports that use Skinny Client Control Protocol (SCCP) for call control. If the **digit** keyword is not used, DTMF digits are not out-pulsed; the voice port uses a simple PLAR connection and the other keywords are not available.

Voice ports can be configured in any order. For example, you can configure port 2/23 before port 2/0. The **show running-config** command lists the ports in ascending order.

Before a PLAR port can become operational, the STC application must first be enabled in the corresponding dial-peer using the **service stcapp** command. If you configure a port for PLAR before enabling the STC application in the dial peer you receive a warning message.

PLAR phones support most of the same features as normal analog phones. The PLAR phone handles incoming calls and supports hookflash for basic supplementary features such as call transfer, call waiting, and conference. The PLAR phone does not support other features such as call forwarding, redial, speed dial, call park, call pick up from a PLAR phone, AMWI, or caller ID.

Examples

The following example enables the PLAR feature on port 2/0, 2/1, and 2/3. When a phone user picks up the handset on the analog phone connected to port 2/0, the system automatically rings extension 3660 and after waiting 500 milliseconds, dials 1234. The DTMF digits are out-pulsed to the destination port at an interval of 200 milliseconds.

```
Router(config)# sccp plar
Router(config-sccp-plar)# voiceport 2/0 dial 3660 digit 1234 wait-connect 500 interval 200
Router(config-sccp-plar)# voiceport 2/1 dial 3264 digit 678,,,9*0,,#123 interval 100
Router(config-sccp-plar)# voiceport 2/3 dial 3478 digit 34567 wait-connect 500
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and defines a dial peer.
sccp plar	Enters SCCP PLAR configuration mode.

voice-port

To enter voice-port configuration mode, use the **voice-port** command in global configuration mode.

Cisco 1750 and Cisco 1751
voice-port *slot-number*/*port*

Cisco 2600 series, Cisco 3600 Series, and Cisco 7200 Series
voice-port {*slot-number*/*subunit-number*/*port* | *slot*/*port*:*ds0-group-no*}

Cisco 2600 and Cisco 3600 Series with a High-Density Analog Network Module (NM-HDA)
slot-number/*subunit-number*/*port***voice-port**

Cisco AS5300
voice-port *controller-number* **:D**

Syntax Description

slot-number	Number of the slot in the router in which the voice interface card (VIC) is installed. Valid entries are from 0 to 2, depending on the slot in which it has been installed.
port	Voice port number. Valid entries are 0 and 1.

slot-number	Number of the slot in the router in which the VIC is installed. Valid entries are from 0 to 3, depending on the slot in which it has been installed.
subunit-number	Subunit on the VIC in which the voice port is located. Valid entries are 0 or 1.
port	Voice port number. Valid entries are 0 and 1.
slot	The router location in which the voice port adapter is installed. Valid entries are from 0 to 3.
port:	Indicates the voice interface card location. Valid entries are 0 and 3.
ds0-group-no	Indicates the defined DS0 group number. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.

controller-number	T1 or E1 controller.
:D	D channel associated with ISDN PRI.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
11.3(1)T	This command was introduced.

Release	Modification
11.3(3)T	This command was implemented on the Cisco 2600 series.
12.0(3)T	This command was implemented on the Cisco AS5300.
12.0(7)T	This command was implemented on the Cisco AS5800, Cisco 7200 series, and Cisco 1750. Arguments were added for the Cisco 2600 series and Cisco 3600 series.
12.2(8)T	This command was implemented on Cisco 1751 and Cisco 1760. This command was modified to accommodate the additional ports of the NM-HDA on the Cisco 2600 series, Cisco 3640, and Cisco 3660.
12.2(2)XN	Support for enhanced MGCP voice gateway interoperability was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2 and implemented on the Cisco IAD2420 series.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. This command does not support the extended echo canceller (EC) feature on the Cisco AS5300 or the Cisco AS5800.

Usage Guidelines

Use the **voice-port**global configuration command to switch to voice-port configuration mode from global configuration mode. Use the **exit** command to exit voice-port configuration mode and return to global configuration mode.



Note This command does not support the extended echo canceller (EC) feature on the Cisco AS5300.

Examples

The following example accesses voice-port configuration mode for port 0, located on subunit 0 on a VIC installed in slot 1:

```
voice-port 1/0/0
```

The following example accesses voice-port configuration mode for a Cisco AS5300:

```
voice-port 1:D
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.

voice-port (MGCP profile)

The **voice-port**(MGCP profile)command is replaced by the **port**(MGCP profile) command in Cisco IOS Release 12.2(8)T. See the **port** (MGCP profile) command for more information.

voice-port busyout

To place all voice ports associated with a serial or ATM interface into a busyout state, use the **voice-port busyout**command in interfaceconfiguration mode. To remove the busyout state on the voice ports associated with this interface, use the **no** form of this command.

voice-port busyout
no voice-port busyout

Syntax Description

This command has no arguments or keywords.

Command Default

The voice ports on the interface are not in busyout state.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco MC3810.

Usage Guidelines

This command busies out all voice ports associated with the interface, except any voice ports configured to busy out under specific conditions using the **busyout monitor** and **busyout seize** commands.

Examples

The following example places the voice ports associated with serial interface 1 into busyout state:

```
interface serial 1
 voice-port busyout
```

The following example places the voice ports associated with ATM interface 0 into busyout state:

```
interface atm 0
 voice-port busyout
```

Related Commands

Command	Description
busyout forced	Forces a voice port into the busyout state.
busyout monitor	Places a voice port into the busyout monitor state.
busyout seize	Changes the busyout action for an FXO or FXS voice port.
show voice busyout	Displays information about the voice busyout state.

voice rtp send-recv

To establish a two-way voice path when the Real-Time Transport Protocol (RTP) channel is opened, use the **voice rtp send-recv command in**global configuration mode. To reset to the default, use the **no** form of this command.

voice rtp send-recv
no voice rtp send-recv

Syntax Description

This command has no arguments or keywords.

Command Default

The voice path is cut-through in only the backward direction when the RTP channel is opened.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced on Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco 7500 series, Cisco AS5300, Cisco AS5800, and Cisco MC3810 platforms.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T.

Usage Guidelines

This command should be enabled only when the voice path must be cut-through (established) in both the backward and forward directions before a Connect message is received from the destination switch. This command affects all VoIP calls when it is enabled.

Examples

The following example enables the voice path to cut-through in both directions when the RTP channel is opened:

```
voice rtp send-recv
```

voice rtp source-filter

To verify source of a Real-time Transport Protocol (RTP) or RTP Control Protocol (RTCP) stream while receiving the packets for H.323, MGCP, SIP or SCCP protocols, use the **voice rtp source-filter** command. To disable filtering, use the **no** form of this command.



Note The **voice rtp source-filter** command is applicable only to ISR-G2 (3945e) routers.

voice rtp source-filter
no voice rtp source-filter

Command Default

Voice RTP source filtering is enabled.

Command Modes

Voice service voip configuration (conf-voi-serv)

Command History

Release	Modification
15.5(3)M9	This command was introduced.
15.6(3)M6	

Usage Guidelines

Public Switched Telephone Network (PSTN) callers may experience security risk when the IOS gateway receives an invalid RTP stream destined to the same IP address and port of an active call. The invalid stream has a different source IP address and port. The gateway mixes both the valid and invalid RTP streams and plays it to the PSTN caller. Use the **voice rtp source-filter** command when you want to filter RTP packets with a source IP address and port number that are different from the one negotiated through VOIP signaling.

Examples

The following example shows how to filter RTP packets:

```
Device>enable
Device#configure terminal
Device(config)#voice service voip
Device(conf-voi-serv)#voice rtp source-filter
```

Related Commands

Command	Description
voice service voip	Specifies the voice-encapsulation type and enters voice service configuration mode.
voice rtp send-recv	Establishes a two-way voice path when the Real-Time Transport Protocol (RTP) channel is opened.

voice-service dsp-reservation

To specify the percentage of DSP resources that are reserved strictly for VOIP on the voice card, use the **voice-service dsp-reservation**command in voice-card configuration. To reset the percentage of DSP resources, use the **no** form of this command.

voice-service-dsp reservation *percentage*
no voice-service-dsp reservation *percentage*

Syntax Description

percentage	Percentage of DSP resources on this voice card that are reserved for voice services. The remaining DSP resources will be available for video services.

Command Default

The default voice reservation is 100%.

Command Modes

voice-card configuration (config-voicecard)

Command History

Release	Modification
15.1(4)M	The command was introduced.

Usage Guidelines

Use this command to reserve a percentage of the voice card for voice services. The remaining DSP resources will be used for video services. A reservation of 100% specified that all DSP resources will be used for voice services.

Note You can configure a percentage less than 100% only when there is a video license and the appropriate PVDM# modules are installed.

Tip DSP can become fragmented when you change the percentage of DSP resources reserved for voice services when there are TDM voice or DSP farm profiles configured. To ensure the best system performance, reload the router when you change the **voice-service-dsp-reservation**.

Examples

The following example enters voice-card configuration mode and sets the percentage of DSP resources for voice to 60%:

```
Router(config)# voice card 0
Router(config-voicecard)# voice-service dsp-reservation 60
```

Related Commands

Command	Description
dspfarm profile	Adds the specified voice card to those participating in a DSP resource pool.

voice service

To enter voice-service configuration mode and to specify a voice-encapsulation type, use the voice service command in global configuration mode..

voice service {**pots** | **voatm** | **vofr** | **voip**}

Syntax Description

pots	Telephony voice service.
voatm	Voice over ATM (VoATM) encapsulation.
vofr	Voice over Frame Relay (VoFR) encapsulation.
voip	Voice over IP (VoIP) encapsulation.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)XA	This command was introduced on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T for VoIP on the Cisco 2600 series and the Cisco 3600 series.
12.1(3)XI	This command was implemented on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

Voice-service configuration mode is used for packet telephony service commands that affect the gateway globally.

Examples

The following example enters voice-service configuration mode for VoATM service commands:

```
voice service voatm
```

voice sip sip-profiles

To upgrade or downgrade SIP profile configurations to rule format or non-rule format, use **voice sip sip-profiles** command.

voice sip sip-profiles {**upgrade** | **downgrade** }

Syntax Description

upgrade	Upgrades all SIP profile configurations to rule format.
downgrade	downgrades all SIP profile configurations to non-rule format.

Command Default

none

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.5(2)T, Cisco IOS-XE Release 3.15S	This command was introduced.

Example

For upgrading SIP profile configurations to rule format:

```
Device# voice sip sip-profiles upgrade
```

For downgrading SIP profile configurations to non-rule format:

```
Device# voice sip sip-profiles downgrade
```

voice sip oauth get-keys

To retrieve OAuth keys from the CUCM, use the **voice sip oauth get-keys** command.

voice sip oauth get-keys

Command Default

None.

Command Modes

SIP configuration mode.

Command History

Release	Modification
Cisco IOS XE Cupertino 17.8.1a	This command was introduced.

Usage Guidelines

Use the **voice sip oauth get-keys** command on SRST to get keys from the call manager.

voice source-group

To define a source IP group for voice calls, use the **voice source-group** command in global configuration mode. To delete the source IP group, use the **no** form of this command.

voice source-group *name*
no voice source-group *name*

Syntax Description

name	Name of the IP group. Maximum length of the source IP group name is 31 alphanumeric characters.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use the **voice source-group** command to assign a name to a set of source IP group characteristics. The terminating gateway uses these characteristics to identify and translate the incoming VoIP call.

Carrier IDs and trunk group labels must not have the same names.

Do not mix carrier IDs and trunk group labels within a source IP group.

A terminating gateway can be configured with carrier ID source IP groups and trunk-group-label source IP groups. Th e name of the source IP group must be unique to the gateway.

Examples

The following example initiates source IP group "utah2" for VoIP calls:

```
Router(config)# voice source-group utah2
```

Related Commands

Command	Description
access-list	Defines a list of source groups for identifying incoming calls.
carrier-id (voice source group)	Specifies the carrier handling a VoIP call.
description (voice source group)	Assigns a disconnect cause to a source IP group.
h323zone-id (voice source group)	Assigns a zone ID to an incoming H.323 call.
translation-profile (source group)	Assigns a translation profile to a source IP group.
trunk-group-label (voice source group)	Specifies the trunk handling a VoIP call.

voice statistics accounting method

To enable voice accounting statistics to be collected for a specific accounting method list and to specify the pass criteria for call legs, use the **voice statistics accounting method**command in global configuration mode. To disable the collection of statistics for the accounting method, use the **no** form of this command.

voice statistics accounting method *method-list-name* **pass** {**start-interim-stop** | **start-stop** | **stop-only**}
no voice statistics accounting method *method-list-name* **pass** {**start-interim-stop** | **start-stop** | **stop-only**}

Syntax Description

method-list-name	Name of the accounting method list. The method-list-name argument is the same as that configured using the **method** command in gateway accounting AAA configuration mode.
pass	The pass criteria for call legs (PSTN or IP) and call directions (inbound or outbound) that is used by the method list. **Note** The definition of pass implies that all start, stop, or interim messages are acknowledged by the designated servers. The definition of failure implies that any start, stop, or interim message is rejected or is timed out by the designated servers.
start-interim-stop	All start, interim, and stop pass criteria records are counted.
start-stop	All start and stop pass criteria records are counted.
stop-only	Only stop pass criteria records are counted.

Command Default

No statistics for the specified accounting method list are collected.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows that h323 is specified as the method list and that the pass criterion is stop-only:

```
Router(config)# voice statistics accounting method h323 pass stop-only
```

Related Commands

Command	Description
method	Specifies the AAA method list name to be used.
show voice statistics csr interval accounting	Displays statistical information by configured intervals for accounting statistics.

Command	Description
show voice statistics csr since-reset accounting	Displays all accounting CSRs since the last reset.
voice statistics display-format separator	Specifies the format for CSR display.
voice statistics field-params	Specifies MCD, lost-packet, packet-latency, and packet-jitter parameters.
voice statistics max-storage-duration	Specifies the maximum time for which CSRs are stored in system memory.
voice statistics push	Specifies an FTP or syslog server for downloading CSRs, the maximum file size, and the maximum message size.
voice statistics time-range	Specifies the time range to collect CSRs.
voice statistics type	Enables the collection of accounting and signaling CSRs.

voice statistics display-format separator

To configure the display format of the statistics on the gateway, use the **voice statistics display-format separator**command in global configuration mode. To return the display format of the statistics to the default value, use the **no** form of this command.

voice statistics display-format separator {**space** | **tab** | **new-line** | **char** *char*}
no voice statistics display-format separator {**space** | **tab** | **new-line** | **char** *char*}

Syntax Description

separator	Type of separator used in the displayed format.
space	A space is used for the formatting between each statistic in the displayed output.
tab	A tab is used for the formatting between each statistic in the displayed output.
new-line	A new line is used for the formatting between each statistic in the displayed output.
char *char*	A character is used for the formatting between each statistic in the displayed output. The char argument is a visible ASCII character used for the formatting between each statistic in the displayed output.

Command Default

A comma (,) is the default separator.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows that a space is specified as the display separator:

```
Router(config)# voice statistics display-format separator space
```

Related Commands

Command	Description
voice statistics accounting method	Enables the accounting method and the pass and fail criteria.
voice statistics field-params	Specifies MCD, lost-packet, packet-latency, and packet-jitter parameters.
voice statistics max-storage-duration	Specifies the maximum time for which CSRs are stored in system memory.
voice statistics push	Specifies an FTP or syslog server for downloading CSRs, the maximum file size, and the maximum message size.
voice statistics time-range	Specifies the time range to collect CSRs.

Command	Description
voice statistics type	Enables the collection of accounting and signaling CSRs.

voice statistics field-params

To configure the parameters of call statistics fields on the gateway, use the **voice statistics field-params** command in global configuration mode. To return the call statistics parameters to the default values, use the **no** form of this command.

voice statistics field-params {**mcd** *value* | **lost-packet** *value* | **packet-latency** *value* | **packet-jitter value**}
no voice statistics field-params {**mcd** *value* | **lost-packet** *value* | **packet-latency** *value* | **packet-jitter value**}

Syntax Description

mcd	Minimum call duration. The value argument is an integer that represents the number of milliseconds. Valid values are from 0 to 30. The default is 2.
lost-packet	Lost voice packet threshold. The value argument is an integer that represents milliseconds. Valid values are from 0 to 65535. The default is 1000.
packet-latency	Voice packet latency threshold. The value argument is an integer that represents milliseconds. Valid values are from 0 to 500. The default is 250.
packet-jitter	Voice packet jitter threshold. The value argument is an integer that represents milliseconds. Valid values are from 0 to 1000. The default is 250.

Command Default

MCD is 2 milliseconds. Lost packet threshold is 1000 milliseconds. Packet latency threshold is 250 milliseconds. Packet jitter threshold is 250 milliseconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example configures a minimum call duration of 5 milliseconds:

```
Router(config)# voice statistics field-params mcd 5
```

The following example configures a lost packet threshold of 250 milliseconds:

```
Router(config)# voice statistics field-params lost-packet 250
```

The following example configures a packet-latency threshold of 300 milliseconds:

```
Router(config)# voice statistics field-params packet-latency 300
```

The following example configures a packet-jitter threshold of 245 milliseconds:

```
Router(config)# voice statistics field-params packet-jitter 245
```

Related Commands

Command	Description
voice statistics accounting method	Enables the accounting method and the pass and fail criteria.
voice statistics display-format separator	Specifies the format for CSR display.
voice statistics max-storage-duration	Specifies the maximum time for which CSRs are stored in system memory.
voice statistics push	Specifies an FTP or syslog server for downloading CSRs, the maximum file size, and the maximum message size.
voice statistics time-range	Specifies the time range to collect CSRs.
voice statistics type	Enables the collection of accounting and signaling CSRs.

voice statistics max-storage-duration

To configure the maximum amount of time for which collected statistics are stored in the system memory of the gateway, use the **voice statistics max-storage-duration**command in global configuration mode. To remove the configured maximum storage duration, use the **no** form of this command.

voice statistics max-storage-duration {**day***value* | **hour** *value* | **minute***value*}
no voice statistics max-storage-duration {**day***value* | **hour** *value* | **minute***value*}

Syntax Description

day	Number of days for which call statistics data are to be stored. The value argument has a valid range from 0 to 365.
hour	Number of hours for which call statistics data are to be stored. The value argument has a valid range from 0 to 720.
minute	Number of minutes for which call statistics data are to be stored. The value argument has a valid range from 0 to 1440.

Command Default

If no length of time is configured, no memory is allocated for those call statistic records that have stopped after the end of their collection intervals. If no memory is allocated, only active call statistic record buffers are kept in system memory.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The maximum storage duration means the time-to-exist duration of the call statistic records on the gateway.

The values entered using this command also apply to the collection of VoIP internal error codes (IECs).

Examples

The following example shows that the maximum storage duration for the collection of voice call statistics has been set for 60 minutes:

```
Router(config)# voice statistics max-storage-duration minute 60
```

Related Commands

Command	Description
voice statistics accounting method	Enables the accounting method and the pass and fail criteria.
voice statistics display-format separator	Specifies the format for CSR display.
voice statistics field-params	Specifies MCD, lost-packet, packet-latency, and packet-jitter parameters.

Command	Description
voice statistics push	Specifies an FTP or syslog server for downloading CSRs, the maximum file size, and the maximum message size.
voice statistics time-range	Specifies the time range to collect CSRs.
voice statistics type	Enables the collection of accounting and signaling CSRs.

voice statistics push

To configure the method for pushing signaling statistics, VoIP AAA accounting statistics, or Cisco internal error codes (IECs) to an FTP or syslog server, use the **voice statistics push** command in global configuration mode. To disable the configured push method, use the **no** form of this command.

{**voice statistics push ftp url** *ftp-url* [**max-file-size** *value*] | **syslog** [**max-msg-size** *value*]}
{**no voice statistics push ftp url** *ftp-url* [**max-file-size** *value*] | **syslog** [**max-msg-size** *value*]}

Syntax Description

ftp url	URL of the FTP server to which voice statistics are to be pushed. The syntax of the ftp-url argument follows: ftp://user:password@host:port//directory1/directory2
max-file-size	(Optional) Maximum size of a voice statistics file to be pushed to an FTP server, in bytes. The valid range of the *value* argument is from 1024 to 4294967296. The default value is 400000000 (4 GB).
syslog	Voice statistics are pushed to a syslog server.
max-msg-size	(Optional) Maximum size of a voice statistics file to be pushed to a syslog server, in bytes. The valid range of the *value* argument is from 1024 to 4294967296. The default value is 400000000 (4 GB).

Command Default

Voice statistics are not pushed to an FTP or syslog server.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The gateway configuration should be consistent with the configuration on the FTP or syslog servers. This command may also be used to push Cisco VoIP internal error codes (IECs) to either an FTP server or a syslog server.

Examples

The following is a configuration example showing a specified FTP server and maximum file size:

```
Router(config)# voice statistics push ftp url
ftp://john:doe@abc:23//directory1/directory2 max-file-size 10000
```

Related Commands

Command	Description
voice statistics accounting method	Enables the accounting method and the pass and fail criteria.
voice statistics display-format separator	Specifies the format for CSR display.
voice statistics field-params	Specifies MCD, lost-packet, packet-latency, and packet-jitter parameters.

Command	Description
voice statistics max-storage-duration	Specifies the maximum time for which CSRs are stored in system memory.
voice statistics time-range	Specifies the time range to collect CSRs.
voice statistics type	Enables the collection of accounting and signaling CSRs.

voice statistics time-range

To specify a time range to collect statistics from the gateway on a periodic basis, since the last reset, or for a specific time duration , use the **voice statistics time-range**command in global configuration mode. To disable the time-range settings, use the **no** form of this command.

Statistics Collection on a Periodic Basis
voice statistics time-rangeperiodic*interval***start***hh:mm* {**days-of-week** {**Monday** | **Tuesday** | **Wednesday** | **Thursday** | **Friday** | **Saturday** | **Sunday** | **daily** | **weekday** | **weekend**}}[**end***hh:mm* {**days-of-week** | **Monday** | **Tuesday** | **Wednesday** | **Thursday** | **Friday** | **Saturday** | **Sunday** | **daily** | **weekday** | **weekend**}]
no voice statistics time-rangeperiodic*interval***start***hh:mm* {**days-of-week** {**Monday** | **Tuesday** | **Wednesday** | **Thursday** | **Friday** | **Saturday** | **Sunday** | **daily** | **weekday** | **weekend**}}[**end***hh:mm* {**days-of-week** | **Monday** | **Tuesday** | **Wednesday** | **Thursday** | **Friday** | **Saturday** | **Sunday** | **daily** | **weekday** | **weekend**}]

Statistics Collection Since the Last Reset or Reboot of the Gateway
voice statistics time-range since-reset
no voice statistics time-range since-reset

Statistics Collection at a Specific Time Duration
voice statistics time-range specific start *hh* **:** *mm day month year end hh* **:** *mm day month year*
no voice statistics time-range specific start *hh* **:** *mm day month year end hh* **:** *mm day month year*

Syntax Description

Statistics Collection on a Periodic Basis:	
periodic	Call statistics are collected for a configured period.
interval	Specifies the periodic interval during which statistics will be collected. Valid entries for this value are **5minutes**, **15minutes**, **30minutes**, **60minutes**, or **1day**.
start/end	Specifies the start and ending periods of the statistics collection. If no end time is entered, then the statistics collection continues nonstop. By default, there is no end of the collection period.
hh:mm	Specifies the start and ending times for the periodic statistics collection in hours and minutes. The times entered must be in 24-hour format.
days-of-week	Specifies the start and ending days of the week that call statistics are collected. You can configure a specific day of the week, or one of the following: • daily--Call statistics are collected daily. • weekdays--Call statistics are collected on weekdays only. • weekend--Call statistics are collected on weekends only. The default value is daily.

Statistics Collection Since the Last Reset or Reboot of the Gateway	
since-reset	Call statistics are collected only since a reset or reboot of the gateway. **Note** Voice statistics collection on the gateway is reset using the **clear voice statistics csr**command.
Statistics Collection at a Specified Time Duration:	
specific	Call statistics are collected for a specific time duration.
start/end	Specifies the start and end times of the statistics collection. The required arguments for both the start and end keywords are as follows: • hh**:**mm--Hour and minute. The times entered must be in 24-hour format. • day--Day of the month. Valid values are from 1 to 31. • month--Month for the statistics collection to start. Enter the month name, for example, January, or February. The default is the current month. • year--Year. Valid values are from 1993 to 2035. The default is the current year.

No statistics are collected by default.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

There should be only one specific or periodic configuration at any one time. If a second specific or periodic configuration is configured, the request is rejected and a warning message displays. If the no form of the command is used during the specific time range, the corresponding collection will stop and FTP or syslog messages will not be sent.

Examples

The following example shows that the time range is periodic and set to collect statistics for a 60-minute period on weekdays only beginning at 12:00 a.m.:

```
Router(config)# voice statistics time-range periodic 60minutes start 12:00 days-of-week
weekdays
```

The following example configures the gateway to collect call statistics since the last reset (specified with the **clear voice statistics csr**command) or since the last time the gateway was rebooted:

```
Router(config)# voice statistics time-range since-reset
```

The following example configures the gateway to collect statistics from 10:00 a.m. on the first day of January to 12:00 a.m. on the second day of January:

```
Router(config)
# voice statistics time-range specific start 10:00 1 January 2004 end 12:00 2 January 2004
```

Related Commands

Command	Description
clear voice statistics	Clears voice statistics, resetting the statistics collection.
voice statistics accounting method	Enables the accounting method and the pass and fail criteria.
voice statistics display-format separator	Specifies the format for CSR display.
voice statistics field-params	Specifies MCD, lost-packet, packet-latency, and packet-jitter parameters.
voice statistics max-storage-duration	Specifies the maximum time for which CSRs are stored in system memory.
voice statistics push	Specifies an FTP or syslog server for downloading CSRs, the maximum file size, and the maximum message size.
voice statistics type	Enables the collection of accounting and signaling CSRs.

voice statistics type csr

To configure a gateway to collect VoIP AAA accounting statistics or voice signaling statistics, independently or at the same time, use the **voice statistics type csr**command in global configuration mode. To disable the counters, use the **no** form of this command.

voice statistics type csr [**accounting** | **signaling**]
no voice statistics type csr [**accounting** | **signaling**]

Syntax Description

accounting	(Optional) VoIP AAA accounting statistics are collected.
signaling	(Optional) Voice signaling statistics are collected.

Command Default

No accounting or signaling call statistics records (CSRs) are collected on the gateway.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

If you do not specify a keyword, both accounting and signaling CSRs are collected. Accounting and signaling CSR collection can be enabled and disabled independently.

Examples

The following example shows that both types of CSRs will be collected:

```
Router(config)# voice statistics type csr
```

The following example enables accounting CSRs to be collected:

```
Router(config)# voice statistics type csr accounting
```

The following example enables signaling CSRs to be collected:

```
Router(config)# voice statistics type csr signaling
```

The following example disables the collection of both signaling and accounting CSRs:

```
Router(config)# no
voice statistics type csr
```

The following example disables the collection of signaling CSRs only:

```
Router(config)# no
voice statistics type csr signaling
```

Related Commands

Command	Description
voice statistics accounting method	Enables the accounting method and the pass and fail criteria.
voice statistics display-format separator	Specifies the format for CSR display.
voice statistics field-params	Specifies MCD, lost-packet, packet-latency, and packet-jitter parameters.
voice statistics max-storage-duration	Specifies the maximum time for which CSRs are stored in system memory.
voice statistics push	Specifies an FTP or syslog server for downloading CSRs, the maximum file size, and the maximum message size.
voice statistics time range	Specifies the time range to collect CSRs.

voice statistics type iec

To enable collection of Internal Error Code (IEC) statistics, use the voice statistics type iec command in global configuration mode. To disable IEC statistics collection, use the **no** form of this command.

voice statistics type iec
no voice statistics type iec

Syntax Description

This command has no arguments or keywords.

Command Default

IEC statistics collection is disabled.

Command Modes

Global configuration.

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Examples

The following example enables IEC statistics collection:

```
Router(config)# voice statistics type iec
```

Related Commands

Command	Description
clear voice statistics	Clears voice statistics, resetting the statistics collection.
show voice statistics	Displays voice statistics
show voice statistics interval-tag	Displays interval options available for IEC statistics
voice statistics time-range since-reset	Enables collection of call statistics accumulated since the last resetting of IEC counters

voice translation-profile

To define a translation profile for voice calls, use the **voice translation-profile** command in global configuration mode. To delete the translation profile, use the **no** form of this command.

voice translation-profile *name*
no voice translation-profile *name*

Syntax Description

name	Name of the translation profile. Maximum length of the voice translation profile name is 31 alphanumeric characters.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

After translation rules are defined, they are grouped into profiles. The profiles collect a set of rules that, taken together, translate the called, calling, and redirected numbers in specific ways. Up to 1000 profiles can be defined. Each profile must have a unique name .

These profiles are referenced by trunk groups, dial peers, source IP groups, voice ports, and interfaces for handling call translations.

Examples

The following example initiates translation profile "westcoast" for voice calls. The profile uses translation rules 1, 2, and 3 for various types of calls.

```
Router(config)# voice translation-profile westcoast
Router(cfg-translation-profile)# translate calling 2
Router(cfg-translation-profile)# translate called 1
Router(cfg-translation-profile)# translate redirect-called 3
```

Related Commands

Command	Description
rule (voice translation-rule)	Defines call translation criteria.
show voice translation-profile	Displays one or more translation profiles.
translate (translation profiles)	Associates a translation rule with a voice translation profile.

voice translation-rule

To define a translation rule for voice calls, use the **voice translation-rule** command in global configuration mode. To delete the translation rule, use the **no** form of this command.

voice translation-rule *number*
no voice translation-rule *number*

Syntax Description

number	Number that identifies the translation rule. Range is from 1 to 2147483647.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

Use the **voice translation-rule** command to create the definition of a translation rule. Each definition includes up to 15 rules that include SED-like expressions for processing the call translation. A maximum of 128 translation rules are supported.

These translation rules are grouped into profiles that are referenced by trunk groups, dial peers, source IP groups, voice ports, and interfaces.

Examples

The following example initiates translation rule 150, Which includes two rules:

```
Router(config)# voice translation-rule 150
Router(cfg-translation-rule)# rule 1 reject /^408\(.(\)/
Router(cfg-translation-rule)# rule 2 /\(^...\)853\(...\)/ /\1525\2/
```

Related Commands

Command	Description
rule (voice translation-rule)	Defines the matching, replacement, and rejection patterns for a translation rule.
show voice translation-rule	Displays the configuration of a translation rule.

voice vad-time

To change the minimum silence detection time for voice activity detection (VAD), use the **voice vad-time** command in global configuration mode. To reset to the default, use the **no** form of this command.

voice vad-time *milliseconds*
no voice vad-time

Syntax Description

milliseconds	Waiting period, in milliseconds, before silence detection and suppression of voice-packet transmission. Range is from 250 to 65536. The default is 250.

Command Default

250 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Thiscommand affects all voice ports on a router or concentrator, but it does not affect calls already in progress.

You can use this command in transparent common-channel signaling (CCS) applications in which you want VAD to activate when the voice channel is idle, but not during active calls. With a longer silence detection delay, VAD reacts to the silence of an idle voice channel, but not to pauses in conversation.

Thiscommand does not affect voice codecs that have ITU-standardized built-in VAD features--for example, G.729B, G.729AB, G.723.1A. The VAD behavior and parameters of these codecs are defined exclusively by the applicable ITU standard.

Examples

The following example configures a 20-second delay before VAD silence detection is enabled:

```
voice vad-time 20000
```

Related Commands

Command	Description
vad (dial peer)	Enables voice activity detection on a network dial peer.

voice vrf

To configure a voice VRF, use the **voice vrf**command in global configuration mode. To remove the voice VRF configuration, use the **no** form of this command.

voice vrf *vrfname*
no voice vrf *vrfname*

Syntax Description

vrfname	A name assigned to the voice vrf.

Command Default

No voice VRF is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

You must create a VRF using the **ip vrf** *vrfname* command before you can configure it as a voice VRF.

To ensure there are no active calls on the voice gateway during a VRF change, voices services must be shut down on the voice gateway before you configure or make changes to a voice VRF.

Examples

The following example shows that a VRF called *vrf1* was created and then configured as a voice VRF:

```
ip vrf vrf1
 rd 1:1
 route-target export 1:2
 route-target import 1:2
!
voice vrf vrf1
!
voice service voip
```

Related Commands

Command	Description
ip vrf	Defines a VPN VRF instance and enters VRF configuration mode.

voip-incoming translation-profile

To specify a translation profile for all incoming VoIP calls, use the **voip-incoming translation-profile** command in global configuration mode. To delete the profile, use the **no** form of this command.

voip-incoming translation-profile *name*
no voip-incoming translation-profile *name*

Syntax Description

name	Name of the translation profile.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use the **voip-incoming translation-profile** command to globally assign a translation profile for all incoming VoIP calls. The translation profile was previously defined using the **voice translation-profile** command. The **voip-incoming translation-profile**command does not require additional steps to complete its definition.

If an H.323 call comes in and the call is associated with a source IP group that is defined with a translation profile, the source IP group translation profile overrides the global translation profile.

Examples

The following example assigns the translation profile named "global-definition" to all incoming VoIP calls:

```
Router(config)# voip-incoming translation-profile global-definition
```

Related Commands

Command	Description
show voice translation-profile	Displays the configurations for all voice translation profiles.
test voice translation-rule	Tests the voice translation rule definition.
voice translation-profile	Initiates a translation profile definition.

voip-incoming translation-rule

To set the incoming translation rule for calls that originate from H.323-compatible clients, use the **voip-incoming translation-rule** command in global configuration mode. To disable the incoming translation rule, use the **no** form of this command.

voip-incoming translation-rule {**calling** | **called**} **name-tag**
no voip-incoming translation-rule {**calling** | **called**} **name-tag**

Syntax Description

name-tag	Tag number by which the rule set is referenced. This is an arbitrarily chosen number. Range is from 1 to 2147483647. There is no default value.
calling	Automatic number identification (ANI) number or the number of the calling party.
called	Dial Number Information Service (DNIS) number or the number of the called party.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR1	This command was introduced for VoIP on the Cisco AS5300.
12.0(7)XK	This command was implemented for VoIP on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T and implemented for VoIP on the Cisco 1750, Cisco AS5300, Cisco 7200 series, and Cisco 7500 series platforms.
12.1(2)T	This command was implemented for VoIP on Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

With this command, all IP-based calls are captured and handled, depending on either the calling number or the called number to the specified tag name.

Examples

The following example identifies the rule set for calls that originate from H.323-compatible clients:

```
Router(config)# voip-incoming translation-rule called 5
```

Related Commands

Command	Description
numbering-type	Matches one number type for a dial-peer call leg.

Command	Description
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
show translation-rule	Displays the contents of all the rules that have been configured for a specific translation name.
test translation-rule	Tests the execution of the translation rules on a specific name-tag.
translate	Applies a translation rule to a calling party number or a called party number for incoming calls.
translate-outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls.
translation-rule	Creates a translation name and enters translation-rule configuration mode.

voip trunk group

To define or modify a VOIP trunk group and to enter trunk group configuration mode, use the **voip trunk group** command in global configuration mode. To delete the VOIP trunk group, use the **no** form of this command.

voip trunk group *name*
no voip trunk group *name*

Syntax Description

name	Name of the voip trunk group. Valid names contain a maximum of 63 alphanumeric characters.

Command Default

No voip trunk group is defined.

Command Modes

Global configuration

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use the **voip trunk group** command to define the VOIP trunk and extend serviceability to the trunk. By default, the session protocol of the IP trunk is h323. Up to 1000 trunk groups can be configured on the gateway provided that the gateway has sufficient memory to store the profiles

Examples

The following example enables creates a VOIP trunk group and enables monitoring.

```
Router(config)# voip trunk group siptrk1
Router(config-voip-trk)# session protocol sipv2
Router(config-voip-trk)# target ipv4: 10.1.1.15
Router(config-voip-trk)# xsvc
```

Related Commands

Command	Description
show voip trunk group	Displays internal list of voip trunk groups.
xsvc	Enables monitoring on the trunk.

volume

To set the receiver volume level for a POTS port on a router, use the **volume** command in dial-peer voice configuration mode. To reset to the default, use the **no** form of this command.

volume *number*
no volume *number*

Syntax Description

number	A number from 1 to 5 representing decibels (dB) of gain. Range is as follows: • 1: -11.99 dB • 2: -9.7dB • 3: -7.7dB • 4: -5.7dB • 5: -3.7dB Default is 3 (-7.7 dB gain).

Command Default

3 (-7.7 dB gain)

Command Modes

Dial-peer voice configuration

Command History

Release	Modification
12.2(8)T	This command was introduced on Cisco 803, Cisco 804, and Cisco 813 routers.

Usage Guidelines

Set the **volume** command for each POTS port separately. Setting the volume level affects only the port for which it has been set.



Note Only the receiver volume is set with this command.

Use the **show pots volume** command to check the volume status and level.

Examples

The following example shows a volume level of 4 for POTS port 1 and a volume level of 2 for POTS port 2.

```
dial-peer voice 1 pots
 destination-pattern 5551111
 port 1
 no call-waiting
 ring 0
 volume 4
dial-peer voice 2 pots
 destination-pattern 5552222
```

```
port 2
no call-waiting
ring 0
volume 2
```

Related Commands

Command	Description
show pots volume	Shows the receiver volume configured for each POTS port on a router.

vxml allow-star-digit

To configure a Voice Extensible Markup Language (VXML) interpreter to allow the star digit for built-in type digits, use the **vxml allow-star-digit** command in global configuration mode. To disable the configuration, use the **no** form of this command.

vxml allow-star-digit
no vxml allow-star-digit

Syntax Description

This command has no arguments or keywords.

Command Default

A VXML interpreter is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to configure a VXML interpreter to allow the star digit for built-in type digits:

```
Router# configure terminal
Router(config)# vxml allow-star-digit
```

Related Commands

Command	Description
vxml audioerror	Enables throwing an error event when audio playout fails.
vxml version pre2.0	Enables VoiceXML 2.0 features.

vxml logging-tag

To allow fetching logging tag header in Nuance ASR, use the **vxml logging-tag** command in global configuration mode. The **logging-tag** command helps in sending the logging-tag headers to Nuance ASR as part of a RECOGNIZE or SPEAK and SET-PARAM message. The command configuration is enabled by default. To disable the configuration, use the **no** form of this command.

vxml logging-tag
no vxml logging-tag

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.5(3)M7	This command was introduced in the Cisco IOS Release 15.0(3)M7.

Usage Guidelines

Enabling this command helps the gateway to send the logging-tag headers to Nuance ASR as part of a RECOGNIZE or SPEAK and SET-PARAM message. By default the command is in enable state. If you disable the command, the gateway will not send Logging-tag in RECOGNIZE or SPEAK. But, only SET-PARAM message carries Logging-Tag.

Examples

The following example disables the vxml logging-tag feature:

```
Router(config)#no vxml logging-tag
```

vxml audioerror

To enable throwing an error event when audio playout fails, use the **vxml audioerror** command in global configuration mode. To return to the default, use the **no** form of this command.

vxml audioerror
no vxml audioerror

Syntax Description

This command has no arguments or keywords.

Command Default

An audio error event, error.badfetch, is not thrown when an audio file cannot be played.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Entering this command causes an audio error event, error.badfetch, to be thrown when an audio file cannot be played, for instance, because the file is in an unsupported format, the src attribute references an invalid URI, or the expr attribute evaluates to an invalid URI.

The **vxml audioerror** command overrides the **vxml version 2.0** command, so that if both commands are entered, the audio error event will be thrown when an audio file cannot be played.

Examples

The following example enables the audio error feature:

```
Router(config)# vxml audioerror
```

Related Commands

Command	Description
vxml version pre2.0	Enables features compatible with versions earlier than VoiceXML 2.0.

vxml tree memory

To set the maximum memory size for the VoiceXML parser tree, use the **vxml tree memory** command in global configuration mode. To reset to the default, use the **no** form of this command.

vxml tree memory *size*
no vxml tree memory

Syntax Description

size	Maximum memory size, in kilobytes. Range is 64 to 100000. Default is 1000.

Command Default

1000 KB

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(15)T	The default was changed from 64 to 1000.

Usage Guidelines

This command limits the memory resources available for parsing VoiceXML documents, preventing large documents from consuming excessive system memory. Increasing the maximum memory size for the VoiceXML tree enables calls to use larger VoiceXML documents. If a VoiceXML document exceeds the limit, the gateway aborts the document execution and the **debug vxml error** command displays a "vxml malloc fail" error.



Note In Cisco IOS Release 12.3(4)T and later releases, less memory is consumed when parsing a VoiceXML document because the document is not stored by the VoiceXML tree.

Examples

The following example sets the maximum memory size to 128 KB:

```
vxml tree memory 128
```

Related Commands

Command	Description
debug vxml error	Displays VoiceXML application error messages.
ivr prompt memory	Sets the maximum amount of memory that dynamic audio files (prompts) occupy in memory.
ivr record memory system	Sets the maximum amount of memory for storing all voice recordings on the gateway.

vxml version 2.0

To enable VoiceXML 2.0 features, use the **vxml version 2.0** command in global configuration mode. To return to the default, use the **no** form of this command.

vxml version 2.0
no vxml version 2.0

Syntax Description

This command has no arguments or keywords.

Command Default

The default VoiceXML behavior is compatible with versions earlier than W3C VoiceXML 2.0 Specification .

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command enables the following VoiceXML features:

- An audio error event, error.badfetch, is not thrown when an audio file cannot be played, for instance, because the file is in an unsupported format, the src attribute references an invalid URI, or the expr attribute evaluates to an invalid URI.
- Support for the beep attribute of the <record> element.
- Blind transfer compliant with *W3C VoiceXML 2.0* and not the same as consultation transfer.
- Compatibility with W3C VoiceXML 2.0 Specification.
- A semantic error is generated if an undeclared variable is used. You must declare variables before using them.

Examples

The following example enables VoiceXML version 2.0 features:

```
Router(config)# vxml version 2.0
```



W

- watcher all, on page 504
- xsvc, on page 505

watcher all

To allow an external watcher to monitor an internal presentity, use the **watcher all**command in presence configuration mode. To disable monitoring by external watchers, use the **no** form of this command.

watcher all
no watcher all

Syntax Description

This command has no arguments or keywords.

Command Default

Only internal watchers are allowed when presence is enabled.

Command Modes

Presence configuration (config-presence)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command allows external watchers on a remote router connected through a SIP trunk to monitor internal directory numbers. You must enable the **allow watch** command on the internal directory numbers that are watched. To allow external watching from the remote router, you must enable the **allow subscribe** command on the remote router.

Examples

The following example shows how to enable external watching of an internal presentity:

```
Router(config)# presence
Router(config-presence)# watcher all
```

Related Commands

Command	Description
allow subscribe	Allows internal watchers to monitor external presentities.
allow watch	Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service.
presence	Enables presence service on the router and enters presence configuration mode.
presence enable	Allows incoming presence requests from SIP trunks.
server	Specifies the IP address of a presence server for sending presence requests from internal watchers to external presence entities.
show presence global	Displays configuration information about the presence service.
show presence subscription	Displays information about active presence subscriptions.

xsvc

To add support for extended serviceability (xsvc) on TDM, (ISDN-PRI/BRI, DS0-group, analog voice-port) voice interfaces, which are defined as a trunk group, use the**xsvc** command. To disable support for extended serviceability, use the**no** form of this command.

```
xsvc
no xsvc
```

Syntax Description

This command has no arguments or keywords.

Command Default

Extended serviceability is disabled on trunk groups.

Command Modes

Trunk group configuration

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use this command to add support for extended serviceability on voice interfaces which are defined as a trunk group.

Examples

The following example enables monitoring on a trunk group.

```
Router(config)# trunk group tdm-tg1
Router(config-trunk-group)# xsvc
```

Related Commands

Command	Description
provider	Enables a provider service.



X

- xfer target, on page 508

xfer target

To route the INVITE to the refer-to destination in the REFER consume case, use the command **xfer target refer-to**. The routing decision is made based on the xfer target destination. If the target is set to dial-peer, CUBE routes the invite to the dial-peer session target. If the target is set to refer-to, CUBE routes the invite to refer-to host in the REFER message. To disable **xfer target refer-to** and set it to the default **xfer target dial-peer**, use the **no** form of this command.

xfer target refer-to
no xfer target refer-to

Syntax Description

This command has no arguments or keywords.

Command Default

Dial-peer is looked up for session target to route the INVITE to refer-to target.

Command Modes

SIP UA configuration (config-sip-ua)

Voice class tenant configuration (config-class)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.6	This command was introduced.
Cisco IOS XE Bengaluru 17.4.1a	The default value is **xfer target dial-peer**.This command was modified to include the **xfer target refer-to** to route the INVITE to the refer-to host address. This command is available in Cisco IOS XE Fuji 16.9.6, Cisco IOS XE Amsterdam 17.3.1a, and Cisco IOS XE Bengaluru 17.4.1a in sip-ua and voice class tenants.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

By default, in the REFER consume case, the CUBE performs the dial-peer look up to route INVITE to dial-peer session target with the command **xfer target dial-peer**. To change this behavior, you can use the command **xfer target refer-to** in SIP user-agent configuration mode or voice class tenant configuration mode to route the INVITE to refer-to host address.

Examples

The following example shows how to enable xfer target refer-to on the CUBE:

```
Router(config)# sip-ua
Router(config-sip-ua)# xfer target refer-to
```

The following example shows how to enable xfer target refer-to on the CUBE in the voice class tenant configuration mode:

```
Router(config)#voice class tenant 1
Router(config-class)# xfer target refer-to
```



Z

- zone access, on page 510
- zone bw, on page 512
- zone circuit-id, on page 513
- zone cluster local, on page 515
- zone cluster remote, on page 516
- zone qos, on page 518
- zone local, on page 520
- zone prefix, on page 522
- zone remote, on page 526
- zone subnet, on page 529

zone access

To configure the accessibility of your local zone, use the **zone access** command in gatekeeper configuration mode. To remove any accessibility configurations, use the **no** form of this command.

zone access *local-zone-name* {**default** | **remote-zone** *remote-zone-name*} {**direct** | **proxied**}
no zone access *local-zone-name* **remote-zone** *remote-zone-name*

Syntax Description

local -zone-name	Name of local zone (synonymous with local gatekeeper).
default	Use with the **direct** or **proxied** keyword to define the mode of behavior for all remote zones that have not been specially named using the **remote-zone** *remote-zone-name* keyword and argument combination.
remote -zone *remote-zone-name*	Name of remote zone (synonymous with remote gatekeeper) for which a special mode of behavior is defined.
direct	Configures direct calls (without use of proxies) between endpoints. The local zone (or gatekeeper) offers the local endpoint IP address instead of the IP address of a local proxy.
proxied	Configures calls using proxies between endpoints. The local zone (or gatekeeper) offers the IP address of a local proxy instead of the local endpoint address.

Command Default

The local zone allows proxied access for all remote zones.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2500 series and Cisco 3600 series.

Usage Guidelines

By default, a gatekeeper offers a local proxy IP address when queried by a remote gatekeeper about a target local endpoint. This is considered proxied access. By using the **zone access** command, you can configure the local gatekeeper to offer the local endpoint address instead of the local proxy address. This is considered direct access.



Note The **zone access** command, configured on your local gatekeeper, affects only the use of proxies for incoming calls (that is, it does not affect the use of local proxies for outbound calls). When originating a call, a gatekeeper uses a proxy only if the remote gatekeeper offers a proxy at the remote end. A call between two endpoints in the same zone is always a direct (nonproxied) call.

You can define the accessibility behavior of a local zone relative to certain remote zones using the **remote-zone** *remote-zone-name* keyword and argument combination with the **direct** or **proxied** keyword. You can define the default behavior of a local zone relative to all other remote zones using the **default** keyword with the

direct or **proxied** keywords. To remove an explicitly named remote zone so that it is governed by the default-behavior rule, use the **no zone access** command.

Examples

The following example allows direct access to the local zone eng.xyz.com from remote zones within xyz corporation. All other remote locations will have proxied access to eng.xzy.com.

```
zone local eng.xyz.com xyz.com
zone access eng.xyz.com remote-zone mfg.xyz.com direct
zone access eng.xyz.com remote-zone mktg.xyz.com direct
zone access eng.xyz.com remote-zone sales.xyz.com direct
zone access eng.xyz.com default proxied
```

The following example supposes that only local gatekeepers within xyz.com have direct access to each other because your corporation has firewalls or you do not advertise your gatekeepers externally. You have excellent Quality of Service (QoS) within your corporate network, except for a couple of foreign offices. In this case, use proxies with the foreign offices (in Milan and Tokyo) and nowhere else.

```
zone local sanjose.xyz.com xyz.com
zone access sanjose.xyz.com default direct
zone access sanjose.xyz.com remote-zone milan.xyz.com proxied
zone access sanjose.xyz.com remote-zone tokyo.xyz.com proxied
```

Related Commands

Command	Description
show proxy h323 calls	Displays a list of each active call on the proxy.
zone local	Specifies a zone controlled by a gatekeeper.

zone bw

To set the maximum bandwidth allowed in a gatekeeper zone at any one time, use the **zone bw** command in gatekeeper configuration mode. To remove the maximum bandwidth setting and make the bandwidth unlimited, use the **no** form of this command.

zone bw *gatekeeper-name max-bandwidth*
no zone bw *gatekeeper-name max-bandwidth*

Syntax Description

gatekeeper -name	Name of the gatekeeper that controls the zone.
max -bandwidth	Maximum bidirectional bandwidth, in kbps, allowed in the zone at any one time.

Command Default

Bandwidth is unlimited.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500 series and Cisco 3600 series.

Examples

The following example sets the maximum bandwidth to 1000 kbps for zone gk1:

```
zone bw gk1
1000
```

Related Commands

Command	Description
show proxy h323 calls	Displays a list of each active call on the proxy.

zone circuit-id

To associate a remote zone with a circuit, use the **zone circuit-id** command in gatekeeper configuration mode. To delete the circuit ID for a zone, use the **no** form of this command.

zone circuit-id *remote-zone-name circuit-id* [**override-source-circuitid**]
no zone circuit-id *remote-zone-name circuit-id*

Syntax Description

remote -zone-name	Name of the remote zone.
circuit -id	ID of the circuit to be associated with the remote zone.
override-source-circuitid	(Optional) Specifies whether the source circuit ID of the incoming location request (LRQ) message needs to be overridden with this keyword.

Command Default

The override flag is disabled and the incoming source circuit ID is used if present.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.3(14)T	The **override-source-circuitid**keyword was added.

Usage Guidelines

VoIP calls with an LRQ message that come to a gatekeeper from a non-cisco gatekeeper in a remote zone (for example, from an Internet telephony service provider [ITSP]), the LRQ message does not include a source circuit identifier. This command allows the gatekeeper to assign a circuit identifier to the zone and an IP address of the call origination. If the source circuit ID is already present then the configured value will not be used. To enforce the usage of configured source circuit ID, even if the incoming LRQ has a value, configure the **override-source-circuitid** keyword. The Gatekeeper Transaction Message Protocol (GKTMP) server application uses this data to determine a route for the call.

Examples

The following example configures the remote zone GKout1 with a circuit ID CarrierA:

```
Router(config)# gatekeeper
Router(config-gk)# zone circuit-id GKout1 CarrierA
```

The following example configures the remote zone GKout2 with a circuit ID CarrierB and overrides the incoming LRQ source circuit-id value:

```
Router(config)# gatekeeper
Router(config-gk)# zone circuit-id GKout2 CarrierB override-source-circuitid
```

Related Commands

Command	Description
endpoint circuit-id h323id	Assigns a circuit to a non-Cisco endpoint.

Command	Description
show gatekeeper circuits	Displays circuit information on the gatekeeper.
show gatekeeper endpoint circuits	Displays information for all registered endpoints and carriers for the gatekeeper.

zone cluster local

To define a local grouping of gatekeepers, including the gatekeeper that you are configuring, use the **zone cluster local**command in gatekeeper configuration mode. To disable the local grouping of gatekeepers, use the **no** form of this command.

zone cluster local *cluster-name local-zone-name*
no zone cluster local

Syntax Description

cluster -name	Cluster name.
local -zone-name	Local zone name.

Command Default

No default behavior or values

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on Cisco AS5850.

Usage Guidelines

Use this command to define a local cluster of gatekeepers that are alternates of each other. Each of these gatekeepers must be configured in a compatible manner for the cluster to work effectively.

Examples

The following example defines a local grouping of gatekeepers named EuropeCluster in the ParisGK time zone:

```
zone cluster local EuropeCluster ParisGK
```

Related Commands

Command	Description
element	Defines component elements of local or remote clusters.
zone cluster remote	Defines a remote grouping of gatekeepers, including the gatekeeper that you are configuring.

zone cluster remote

To define a remote grouping of gatekeepers, including the gatekeeper that you are configuring, use the **zone cluster remote command in**gatekeeper configuration mode. To disable the remote grouping of gatekeepers, use the **no** form of this command.

{**zone cluster remote** *cluster name* [**cost** *cost-value* [**priority** *priority-value*]] [**foreign-domain**] [**invia** *inbound gatekeeper*] | [**outvia** *outbound gatekeeper*]}
no zone cluster remote

Syntax Description

cluster name	Cluster name.
cost	(Optional) Cost.
cost -value	(Optional) Cost value. Range is from 1 to 100. The default is L50.
priority	(Optional) Priority.
priority -value	(Optional) Priority value. Range is from 1 to 100. The default is 50.
foreign -domain	(Optional) Cluster is in a different administrative domain.
invia	Specifies gatekeeper for calls entering this zone.
inbound gatekeeper	Name of gatekeeper.
outvia	Specifies gatekeeper for calls leaving this zone.
outbound gatekeeper	Name of gatekeeper.

Command Default

No default behavior or values

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	The **foreign-domain** keyword was added.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on Cisco AS5850.
12.2(13)T3	The **invia** and **outvia** keywords were added.

Usage Guidelines

Use this command to define a set of remote gatekeepers that act as alternates to each other and that form a local cluster. This command causes the gatekeeper to optimize these remote gatekeepers by round-robin sending of Location Request (LRQ) messages.

Examples

The following example shows how to define a remote grouping of gatekeepers:

```
zone cluster remote AsiaCluster cost 70 priority 10
```

Related Commands

Command	Description
element	Defines component elements of local or remote clusters.
zone cluster local	Defines a local grouping of gatekeepers, including the gatekeeper that you are configuring.
zone local	Specifies a zone controlled by a gatekeeper.

zone qos

To configure the Differentiated Services Code Point (DSCP) value for a specific zone or a common DSCP value for all zones in Quality of Service (QoS) configurations on a Cisco router, use the **zone qos**command in gatekeeper configuration mode. To remove the DSCP configuration, use the **no** form of this command.

zone qos {*gatekeeper-name* | **global**} **dscp** *dscp-value*
no zone qos {*gatekeeper-name* | **global**} **dscp dscp-value**

Syntax Description

gatekeeper-name	The gatekeeper name to be configured.
global	Configures the DSCP value globally.
dscp	Specifies the DSCP to be configured.
dscp-value	The predefined DSCP keyword or its equivalent numeric value. Refer to the table below for more details.

Command Default

This command is disabled by default.

Command Modes

Gatekeeper configuration (conf-gk)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

To configure a common DSCP value for all local and remote zones, use the **global** keyword and then specify the **dscp** keyword and its value. To change a globally configured DSCP value for a zone-specific DSCP value, the globally configured value should be removed first using the **no** form of the command. If not, a warning message will be displayed. Use the gatekeeper name and the **dscp** keyword with the specific value to configure a zone-based DSCP value.

DSCP can be configured using the predefined DSCP keywords or its equivalent numeric value. For example, to configure the DSCP value of a zone, the **cs1** keyword can be replaced with the numeric value 8. However, the **show gatekeeper zone status** output displays the configured DSCP as cs1. The table below provides the predefined DSCP keywords and their equivalent numeric values. The hexadecimal value is the number that is displayed in the QOS field of the IP header.

Table 8: Predefined DSCP Keywords and Numeric Values

Keyword	Numeric Value	Hexadecimal Value
default	0	0x00
cs1	8	0x20
af11	10	0x28
af12	12	0X30

Keyword	Numeric Value	Hexadecimal Value
af13	14	0x38
cs2	16	0x40
af21	18	0x48
af22	20	0x50
af23	22	0x58
cs3	24	0x60
af31	26	0x68
af32	28	0x70
af33	30	0x78
cs4	32	0x80
af41	34	0x88
af42	36	0x90
af43	38	0x98
cs5	40	0xA0
ef	46	0xB8
cs6	48	0xC0
cs7	56	0xE0

Examples

The following example shows how to configure the DSCP value for a specific zone using the **zone qos** *gatekeeper-name* **dscp** *dscp-value*command:

```
Router(config)# gatekeeper
Router(conf-gk)# zone qos GK-08 dscp cs3
```

The following example shows how to configure the global DSCP value using the **zone qos global dscp** *dscp-value*command:

```
Router(config)# gatekeeper
Router(conf-gk)# zone qos global dscp af11
```

Related Commands

Command	Description
show gatekeeper zone status	Displays the status of the zones related to the gatekeeper.

zone local

To specify a zone controlled by a gatekeeper, use the **zone local** command in gatekeeper configuration mode. To remove a zone controlled by a gatekeeper, use the **no** form of this command.

zone local *gatekeeper-name domain-name* [*ras-IP-address*] [**invia** *inbound gatekeeper* | **outvia** *outbound gatekeeper* [**enable-intrazone**]]
no zone local *gatekeeper-name domain-name* [**invia** *inbound gatekeeper* | **outvia** *outbound gatekeeper* [**enable-intrazone**]]

Syntax Description

gatekeeper-name	Gatekeeper name or zone name. This is usually the fully domain-qualified host name of the gatekeeper. For example, if the *domain-name* is cisco.com, the *gatekeeper-name* might be gk1.cisco.com. However, if the gatekeeper is controlling multiple zones, the *gatekeeper-name* for each zone should be some unique mnemonic string.
domain-name	The domain name served by this gatekeeper.
ras-IP-address	(Optional) IP address of one of the interfaces on the gatekeeper. When the gatekeeper responds to gatekeeper discovery messages, it signals the endpoint or gateway to use this address in future communications. **Note** Setting this address for one local zone makes it the address used for all local zones.
invia	Specifies gatekeeper for calls entering this zone.
inbound gatekeeper	Name of gatekeeper.
outvia	Specifies gatekeeper for calls leaving this zone.
outbound gatekeeper	Name of gatekeeper.
enable-intrazone	Forces all intrazone calls to use the via gatekeeper.

Command Default

No local zone is defined.

Note The gatekeeper cannot operate without at least one local zone definition. Without local zones, the gatekeeper goes to an inactive state when the **no shutdown** command is issued.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500 and Cisco 3600 series routers.
12.2(11)T	This command was implemented on the Cisco MC3810 and Cisco 7200 series.

Release	Modification
12.3(4)T	The **invia**, **outvia**, and **enable-intrazone** keywords were added.

Usage Guidelines

Multiple local zones can be defined. The gatekeeper manages all configured local zones. Intrazone and interzone behavior remains the same (zones are controlled by the same or different gatekeepers).

Only one *ras-IP-address* argument can be defined for all local zones. You cannot configure each zone to use a different RAS IP address. If you define this in the first zone definition, you can omit it for all subsequent zones, which automatically pick up this address. If you set it in a subsequent **zone local** command, it changes the RAS address of all previously configured local zones as well. Once defined, you can change it by reissuing any **zone local** command with a different *ras-IP-address* argument.

If the *ras-IP-address* argument is a Hot Standby Router Protocol (HSRP) virtual address, it automatically puts the gatekeeper into HSRP mode. In this mode, the gatekeeper assumes STANDBY or ACTIVE status according to whether the HSRP interface is on STANDBY or ACTIVE status.

You cannot remove a local zone if there are endpoints or gateways registered in it. To remove the local zone, shut down the gatekeeper first, which forces unregistration.

Multiple zones are controlled by multiple logical gatekeepers on the same Cisco IOS platform.

The maximum number of local zones defined in a gatekeeper should not exceed 100.

This command can also be used to change the IP address used by the gatekeeper.

Examples

The following example creates a zone controlled by a gatekeeper in the domain called "cisco.com":

```
Router(config)# gatekeeper
Router(config-gk)# zone local easterngk.cisco.com cisco.com
```

Related Commands

Command	Description
show proxy h323 calls	Displays a list of each active call on the proxy.
zone subnet	Specifies a zone controlled by a gatekeeper.

zone prefix

To add a prefix to the gatekeeper zone list, use the **zone prefix** command in gatekeeper configuration mode. To remove knowledge of a zone prefix, use the **no** form of this command with the gatekeeper name and prefix. To remove the priority assignment for a specific gateway, use the **no** form of this command with the **gw-priority** option.

zone prefix*gatekeeper-name e164 prefix*[**blast** | **sequence**] {**gw-priority***priority-gw-alias*[*gw-alias..*]}
zone prefix*gatekeeper-name e164 prefix*[**blast** | **sequence**] {**gw-priority***priority-gw-alias*[*gw-alias..*]}

Syntax Description

gatekeeper -name	Name of a local or remote gatekeeper, which must have been defined by using the **zone local** or **zone remote** command.
e164 -prefix	E.164 prefix in standard form followed by dots (.). Each dot represents a number in the E.164 address. For example, 212..... is matched by 212 and any seven numbers. **Note** Although a dot representing each digit in an E.164 address is the preferred configuration method, you can also enter an asterisk (*) to match any number of digits.
blast	(Optional) If you list multiple hopoffs, this indicates that the LRQs should be sent simultaneously to the gatekeepers based on the order in which they were listed. The default is **seq**.
seq	(Optional) If you list multiple hopoffs, this indicates that the LRQs should be sent sequentially to the gatekeepers based on the order in which they were listed. The default is **seq**.
gw -priority *pri-0-to-10 gw-alias*	(Optional) Defines how the gatekeeper selects gateways in its local zone for calls to numbers beginning with prefix *e164-prefix*. Do not use this option to set priority levels for a prefix assigned to a remote gatekeeper. Range is from 0 to 10, where 0 prevents the gatekeeper from using the gateway *gw-alias* for that prefix and 10 places the highest priority on gateway *gw-alias*. The default is 5. To assign the same priority value for one prefix to multiple gateways, list all the gateway names after the *pri-0-to-10*value. *gw-alias* name is the H.323 ID of a gateway that is registered or will register with the gatekeeper. This name is set on the gateway with the **h323-gateway voip h.323-id** command.

Command Default

No knowledge of the gatekeeper zone prefix or the prefix of any other zone is defined. Gateway priority is 5.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
11.3(6)Q	This command was introduced.

Release	Modification
11.3(7)NA	This command was modified for H.323 Version 1.
12.0(5)T	The display format was modified for H.323 Version 2.
12.1(5)XM	The command was implemented on Cisco AS5350 and Cisco AS5400.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Usage Guidelines

A gatekeeper can handle more than one zone prefix, but a zone prefix cannot be shared by more than one gatekeeper. If you have defined a zone prefix as being handled by a gatekeeper and now define it as being handled by a second gatekeeper, the second assignment cancels the first.

If you need a gatekeeper to handle more than one prefix, but for cost reasons you want to be able to group its gateways by prefix usage, there are two ways to do it.

The first method is simpler, has less overhead, and is recommended if your gateways can be divided into distinct groups, in which each group is to be used for a different set of prefixes. For instance, if a group of gateways is used for calling area codes 408 and 650, and another group is used for calling area code 415, you can use this method. In this case, you define a local zone for each set of prefixes and have the group of gateways to be used for that set of prefixes register with that specific local zone. Do not define any gateway priorities. All gateways in each local zone are treated equally in the selection process.

However, if your gateways cannot be cleanly divided into nonintersecting groups (for instance, if one gateway is used for calls to 408 and 415 and another gateway is used for calls to 415 and 650), you can put all these gateways in the same local zone and use the **gw-priority** option to define which gateways will be used for which prefixes.

When choosing a gateway, the gatekeeper first looks for the longest zone prefix match; then it uses the priority and the gateway status to select from the gateways.

If all gateways are available, the gatekeeper chooses the highest-priority gateway. If all the highest-priority gateways are busy (see the gateway **resource threshold** command), a lower-priority gateway is selected.



Note The **zone prefix** command matches a prefix to a gateway. It does not register the gateway. The gateway must register with the gatekeeper before calls can be completed through that gateway.

Examples

The following example shows how you can define multiple local zones for separating your gateways:

```
Router(config-gk)# zone local gk408or650 xyz.com
Router(config-gk)# zone local gk415 xyz.com
Router(config-gk)# zone prefix gk408or650 408.......Router(config-gk)# zone prefix
gk408or650 650.......Router(config-gk)# zone prefix gk415 415.......
```

Now you need to configure all the gateways to be used for area codes 408 or 650 to register with gk408or650 and all gateways to be used for area code 415 to register with gk415. On Cisco voice gateways, you configure the gateways to register with the appropriate gatekeepers by using the **h323 voip id** command.

The following example shows how you can put all your gateways in the same zone but use the **gw-priority** keyword to determine which gateways are used for calling different area codes:

```
Router(config-gk)# zone local localgk xyz.com
Router(config-gk)# zone prefix localgk 408.......
Router(config-gk)# zone prefix localgk 415....... gw-priority 10 gw1 gw2
Router(config-gk)# zone prefix localgk 650....... gw-priority 0 gw1
```

The commands shown accomplish the following tasks:

- Domain xyz.com is assigned to gatekeeper localgk.
- Prefix 408..... is assigned to gatekeeper localgk, and no gateway priorities are defined for it; therefore, all gateways registering to localgk can be used equally for calls to the 408 area code. No special gateway lists are built for the 408..... prefix; selection is made from the primary list for the zone.
- Prefix 415..... is added to gatekeeper localgk, and priority 10 is assigned to gateways gw1 and gw2.
- Prefix 650..... is added to gatekeeper localgk, and priority 0 is assigned to gateway gw1.

A priority 0 is assigned to gateway gw1 to exclude it from the gateway pool for prefix 650. When gateway gw2 registers with gatekeeper localgk, it is added to the gateway pool for each prefix as follows:

- For gateway pool for 415, gateway gw2 is set to priority 10.
- For gateway pool for 650, gateway gw2 is set to priority 5.

The following example changes gateway gw2 from priority 10 for zone 415..... to the default priority 5:

```
Router(config)# gatekeeper
Router(config-gk)# no zone prefix localgk 415....... gw-priority 10 gw2
```

The following example changes both gateways gw1 and gw2 from priority 10 for zone 415..... to the default priority 5:

```
Router(config)# gatekeeper
Router(config-gk)# no zone prefix localgk 415....... gw-priority 10 gw1 gw2
```

In this example, the prefix 415..... remains assigned to gatekeeper localgk. All gateways that do not specify a priority level for this prefix are assigned a default priority of 5. The following example removes the prefix and all associated gateways and priorities from this gatekeeper:

```
Router(config)# gatekeeper
Router(config-gk)# no zone prefix localgk 415.......
```

Related Commands

Command	Description
register	Configures a gateway to register or deregister a fully qualified dial-peer E.164 address with a gatekeeper.
resource threshold	Configures a gateway to report H.323 resource availability to the gatekeeper of the gateway.
show call resource voice threshold	Displays the threshold configuration settings and status for an H.323 gateway.
show gateway	Displays the current gateway status.
zone local	Specifies a zone controlled by a gatekeeper.
zone remote	Statically specifies a remote zone if DNS is unavailable or undesirable.

zone remote

To statically specify a remote zone if domain name service (DNS) is unavailable or undesirable, use the **zone remote**command in gatekeeper configuration mode. To remove the remote zone, use the **no** form of this command.

{**zone remote** *other-gatekeeper-name other-domain-name other-gatekeeper-ip-address* [*port-number*] [**cost** *cost-value* [**priority** *priority-value*]] [**foreign-domain**] [**invia** *inbound gatekeeper*] | [**outvia** *outbound gatekeeper*]}
{**no zone remote** *other-gatekeeper-name other-domain-name other-gatekeeper-ip-address* [*port-number*] [**cost** *cost-value* [**priority** *priority-value*]] [**foreign-domain**] [**invia** *inbound gatekeeper*] | [**outvia** *outbound gatekeeper*]}

Syntax Description

other -gatekeeper-name	Name of the remote gatekeeper.
other -domain-name	Domain name of the remote gatekeeper.
other -gatekeeper-ip-address	IP address of the remote gatekeeper.
port-number	(Optional) RAS signaling port number for the remote zone. Range is from 1 to 65535. If the value is not set, the default is the well-known RAS port number 1719.
cost *cost -value*	(Optional) Cost of the zone. Range is from 1 to 100. The default is 50.
priority *priority-value*	(Optional) Priority of the zone. Range is from 1 to 100. The default is 50.
foreign -domain	(Optional) Cluster is in a different administrative domain.
invia	Specifies gatekeeper for calls entering this zone.
inbound gatekeeper	Name of gatekeeper.
outvia	Specifies gatekeeper for calls leaving this zone.
outbound gatekeeper	Name of gatekeeper.

Command Default

No remote zone is defined. DNS will locate the remote zone. Default RAS port is 1719. Cost value is 50. Priority value is 50.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500 and Cisco 3600 series routers.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.1(5)XM	The **cost** and **priority** keywords were added.

Release	Modification
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	The **foreign-domain** keyword was added.
12.2(4)T	The command was integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on Cisco AS5850 universal gateways.
12.2(8)T	Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and was implemented on the Cisco 7200 series. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(13)T3	The **invia** and **outvia** keywords were added.

Usage Guidelines

Not all gatekeepers have to be in the DNS. For those that are not, use the **zone remote** command so that the local gatekeeper knows how to access them. In addition, you may wish to improve call response time slightly for frequently accessed zones. If the **zone remote** command is configured for a particular zone, you do not need to make a DNS lookup transaction.

The maximum number of zones defined on a gatekeeper varies depending on the mode or the call model or both. For example, a directory gatekeeper may be in the mode of being responsible for forwarding Location Request (LRQ) messages and not handling any local registrations and calls; the call model might be E.164 addressed calls instead of H.323-ID addressed calls.

For a directory gatekeeper that does not handle local registrations and calls, the maximum remote zones defined should not exceed 10,000; an additional 4 MB of memory is required to store this maximum number of remote zones.

For a gatekeeper that handles local registrations and only E.164 addressed calls, the number of remote zones defined should not exceed 2000.

For a gatekeeper that handles H.323-ID calls, the number of remote zones defined should not exceed 200.

When there are several remote zones configured, they can be ranked by cost and priority value. A zone with a lower cost value and a higher priority value is given preference over others.

Examples

The following example configures the local gatekeeper to reach targets of the form *xxx*.cisco.com by sending queries to the gatekeeper named "sj3.cisco.com" at IP address 10.1.1.12.

```
Router(config)# gatekeeper
Router(config-gk)# zone remote sj3.cisco.com cisco.com 10.1.1.12
```

The following example shows how to configure the cost and priority for the gatekeeper "GK10" that serves zone 1.

```
Router(config)# gatekeeper
Router(config-gk)#  zone remote GK10 Zone1 209.165.200.224 cost 20 priority 5
```

Related Commands

Command	Description
show proxy h323 calls	Lists each active call on the proxy.
zone local	Specifies a zone controlled by a gatekeeper.

zone subnet

To configure a gatekeeper to accept discovery and registration messages sent by endpoints in designated subnets, use the **zone subnet**command in gatekeeper configuration mode. To disable the gatekeeper from acknowledging discovery and registration messages from subnets or to remove subnets entirely, use the **no** form of this command.

zone subnet *local-gatekeeper-name* {**default** | *subnet-address* {*/bits-in-maskmask-address*}} **enable**
no zone subnet *local-gatekeeper-name* {**default** | *subnet-address* {*/bits-in-maskmask-address*}} **enable**

Syntax Description

local -gatekeeper-name	Name of the local gatekeeper.
default	Applies to all other subnets that are not specifically defined by the **zone subnet** command.
subnet -address	Address of the subnet being defined.
/ *bits -in-mask*	Number of bits of the mask to be applied to the subnet address.
mask -address	Mask (in dotted string format) to be applied to the subnet address.
enable	Gatekeeper accepts discovery and registration from the specified subnets.

Command Default

The local gatekeeper accepts discovery and registration requests from all subnets. If the request specifies a gatekeeper name, it must match the local gatekeeper name or the request is not accepted.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500 series and Cisco 3600 series.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

You can use the **zone subnet** command more than once to create a list of subnets controlled by a gatekeeper. The subnet masks do not have to match actual subnets in use at your site. For example, to specify a particular endpoint, you can supply its address with a 32-bit netmask.

Examples

The following example starts by disabling the gatekeeper, gk1.cisco.com, from accepting discovery and registration messages from all subnets. Next, gk1.cisco.com is configured to accept discovery and registration messages from all H.323 nodes on the subnet 172.21.127.0.

In addition, gk1.cisco.com is configured to accept discovery and registration messages from a particular endpoint with the IP address 172.21.128.56.

```
no zone subnet gk1.cisco.com default enable
zone subnet gk1.cisco.com 172.21.127.0/24 enable
zone subnet gk1.cisco.com 172.21.128.56/32 enable
```

Related Commands

Command	Description
show gatekeeper zone status	Displays the status of zones related to a gatekeeper.
zone local	Specifies a zone controlled by a gatekeeper.