

Cisco IOS Voice Command Reference - D through I

First Published: 2022-12-14

Last Modified: 2026-09-29

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 **default (auto-config application) through direct-inward-dial** 1

default (auto-config application) 3

default (MGCP profile) 4

default (SIP) 7

default-file vfc 8

define 9

delete vfc 11

description 12

description (ctl file) 15

description (dial peer) 16

description (DSP farm profile) 17

description (dspfarm) 18

description (media-profile) 19

description (phone proxy) 20

description (SCCP Cisco CallManager) 21

description (trunk group) 22

description (voice class) 23

description (voice source group) 24

destination e164-pattern-map 25

destination uri 26

destination-pattern 28

destination-pattern (interface) 32

destination route-string 33

detect v54 channel-group 34

detect-fax mode 35

device-id 36

dhcp interface 37
dial-control-mib 39
dial-peer cor custom 40
dial-peer cor list 42
dial-peer data 43
dial-peer hunt 45
dial-peer inbound selection creation-order 47
dial-peer inbound selection sip-trunk 48
dial-peer no-match disconnect-cause 50
dial-peer outbound status-check pots 51
dial-peer search type 54
dial-peer terminator 55
dial-peer video 56
dial-peer voice 57
dial-type 60
dialer extsig 62
dialer preemption level 63
dialer trunkgroup 65
digit 66
digit-strip 68
digital-filter 71
direct-inward-dial 72

CHAPTER 2 **disable-early-media through dualtone 73**
disable-early-media 180 74
disable service-settings 76
disc_pi_off 77
disconnect-ack 78
dnis (DNIS group) 79
dnis-map 81
dns-a-override 83
domain-name (annex G) 84
drop-last-conferee 85
ds0 busyout (voice) 87

ds0-group (E1) 89
ds0-group (T1) 95
ds0-num 102
dscp media 103
dscp-profile 107
dsn 108
dsp allocation signaling dspid 111
dsp services dspfarm 112
dspfarm (DSP farm) 114
dspfarm (voice-card) 116
dspfarm confbridge maximum 118
dspfarm connection interval 120
dspfarm profile 121
dspfarm rtp timeout 125
dspfarm transcoder maximum sessions 126
dspint dspfarm 128
dtmf-interworking 130
dtmf timer inter-digit 132
dtmf-relay (Voice over Frame Relay) 133
dtmf-relay (Voice over IP) 135
dualtone 139

CHAPTER 3

E 141
e164 143
e911 144
early-offer 145
early-media update block 147
echo-cancel comfort-noise 148
echo-cancel compensation 149
echo-cancel coverage 150
echo-cancel enable 152
echo-cancel enable (controller) 154
echo-cancel erl worst-case 155
echo-cancel loopback 156

echo-cancel mode 157
echo-cancel suppressor 158
element 159
emergency 160
emptycapability 161
emulate cisco h323 bandwidth 162
encap clear-channel standard 164
encapsulation atm-ces 166
encoding h450 call-identity 167
encoding h450 call-identity itu 169
encryption 170
endpoint alt-ep collect 172
endpoint alt-ep h323id 174
endpoint circuit-id h323id 176
endpoint max-calls h323id 177
endpoint naming 178
endpoint resource-threshold 179
endpoint ttl 180
erase vfc 181
error-category 182
error-code-override 184
error-correction 187
error-passthru 189
event-log 190
event-log (Privileged EXEC) 192
event-log dump ftp 194
event-log error-only 197
event-log max-buffer-size 198
expect-factor 200
extsig mgcp 202

CHAPTER 4 F 203

fax interface-type 205
fax protocol (dial peer) 207

fax protocol (voice-service) 209
fax protocol t38 (dial peer) 212
fax protocol t38 (voice-service) 215
fax rate (dial peer) 218
fax rate (pots) 221
fax rate (voice-service) 222
fax receive called-subscriber 224
fax-relay (dial peer) 225
fax-relay (voice-service) 228
fax send center-header 231
fax send coverpage comment 233
fax send coverpage e-mail-controllable 234
fax send coverpage enable 236
fax send coverpage show-detail 237
fax send left-header 239
fax send max-speed 241
fax send right-header 242
fax send transmitting-subscriber 244
file-acct flush 245
file-acct reset 246
filter voice 247
flush 248
fmtp 249
forward-alarms 251
forward-digits 252
forward-to-voicemail 254
frame-relay voice bandwidth 256
freq-max-delay 258
freq-max-deviation 260
freq-max-power 262
freq-min-power 264
freq-pair 266
freq-power-twist 268
frequency (cp-dualtone) 270

CHAPTER 5 G 271

g729 annexb-all 272

g729-annexb override 274

g732 ber 275

gatekeeper 276

gateway 277

gcid 278

global (application configuration) 280

groundstart auto-tip 281

group 282

group auto-reset 284

group cumulative-ack 286

group out-of-sequence 288

group receive 290

group retransmit 292

group set 294

group timer 296

group-params 298

gw-accounting 299

gw-type-prefix 303

CHAPTER 6 H 305

h225 alt-ep hunt 307

h225 connect-passthru 312

h225 display-ie 314

h225 h245-address 316

h225 h245-address on-connect (H.323 voice-class) 318

h225 h245-address on-connect (H.323 voice-service) 320

h225 h245-address setup 322

h225 id-passthru 324

h225 plus-digit passthru 325

h225 signal overlap 327

h225 start-h245 328

h225 timeout call-proceeding 329
h225 timeout keepalive 331
h225 timeout setup 332
h225 timeout t302 333
h225 timeout t304 334
h225 timeout tcp call-idle (H.323 voice service) 335
h225 timeout tcp establish 336
h225 timeut ntf 337
h245 address-check 339
h245 passthru 340
h245 timeout 341
h323 343
h323 asr 344
h323 call start 345
h323 gatekeeper 347
h323 h323-id 348
h323 interface 349
h323 qos 350
h323 t120 351
h323-annexg 352
h323-gateway voip bind srcaddr 354
h323-gateway voip h323-id 355
h323-gateway voip id 356
h323-gateway voip interface 358
h323-gateway voip tech-prefix 359
h323zone-id (voice source group) 361
h450 h450-3 timeout 362
handle-replaces 363
hangup-last-active-call 365
header-passing 367
history-info 369
history session event-log save-exception-only 370
history session max-records 371
history session retain-timer 372

hold-resume 373
hopcount 374
host (SIP URI) 375
host-registrar 377
http client cache memory 379
http client cache query 381
http client cache refresh 382
http client connection idle timeout 384
http client connection persistent 385
http client connection timeout 386
http client cookie 387
http client post-multipart 388
http client response timeout 389
http client secure-ciphersuite 390
http client secure-trustpoint 394
hunt-scheme least-idle 395
hunt-scheme least-used 397
hunt-scheme longest-idle 399
hunt-scheme random 401
hunt-scheme round-robin 402
hunt-scheme sequential 404
huntstop 406

CHAPTER 7 **icpif through irq global-request** 407
icpif 409
id 410
idle-voltage 411
ignore 412
ignore (interface) 414
image encoding 416
image resolution 418
impedance 420
inband-alerting 422
inbound ttl 424

incoming alerting 425
incoming called-number (call filter match list) 427
incoming called-number (dial peer) 429
incoming calling-number (call filter match list) 432
incoming dialpeer 434
incoming media local ipv4 435
incoming media remote ipv4 436
incoming port 437
incoming secondary-called-number 440
incoming signaling local ipv4 442
incoming signaling remote ipv4 443
incoming uri 444
index (voice class) 447
info-digits 449
information-type 451
inject guard-tone 453
inject pause 454
inject tone 455
input gain 457
intensity 459
interface (RLM server) 460
interface Dchannel 462
interface event-log dump ftp 463
interface event-log error only 466
interface event-log max-buffer-size 467
interface max-server-records 469
interface stats 470
interop-handling permit request-uri userid none 471
ip address trusted 472
ip circuit 474
ip dhcp-client forcerenew 476
ip precedence (dial-peer) 477
ip qos defending-priority 478
ip qos dscp 480

ip qos policy-locator 483
ip qos preemption-priority 486
ip rtcp report interval 488
ip rtcp sub-rtcp 489
ip udp checksum 490
ip vrf 491
ip vrf forwarding 492
irq global-request 493

CHAPTER 8 **isdn bind-l3 through ixi transport http 495**
isdn bind-l3 497
isdn bind-l3 (Interface BRI) 498
isdn bind-l3 ccm-manager 500
isdn bind-l3 iua-backhaul 501
isdn contiguous-bchan 503
isdn dpnss 504
isdn gateway-max-interworking 506
isdn global-disconnect 507
isdn gtd 509
isdn ie oli 510
isdn integrate calltype all 511
isdn network-failure-cause 513
isdn outgoing display-ie 516
isdn protocol-emulate 518
isdn rlm-group 520
isdn skipsend-idverify 522
isdn spoofing 525
isdn supp-service calldiversion 526
isdn supp-service mcid 527
isdn supp-service name calling 528
isdn supp-service tbct 530
isdn t-activate 532
isdn tei-negotiation (interface) 534
iua 537

ivr asr-server 539
ivr autoload mode 541
ivr prompt memory 543
ivr autoload url 545
ivr contact-center 547
ivr language link 550
ivr prompt cutoff-threshold 551
ivr prompt streamed 552
ivr record cpu flash 554
ivr record jitter 555
ivr record memory session 557
ivr record memory system 558
ivr tts-server 559
ivr tts-voice-profile 561
ixi application cme 562
ixi application mib 564
ixi transport http 566



default (auto-config application) through direct-inward-dial

- default (auto-config application), on page 3
- default (MGCP profile), on page 4
- default (SIP), on page 7
- default-file vfc, on page 8
- define, on page 9
- delete vfc, on page 11
- description, on page 12
- description (ctl file), on page 15
- description (dial peer), on page 16
- description (DSP farm profile), on page 17
- description (dspfarm), on page 18
- description (media-profile), on page 19
- description (phone proxy), on page 20
- description (SCCP Cisco CallManager), on page 21
- description (trunk group), on page 22
- description (voice class), on page 23
- description (voice source group), on page 24
- destination e164-pattern-map, on page 25
- destination uri, on page 26
- destination-pattern, on page 28
- destination-pattern (interface), on page 32
- destination route-string, on page 33
- detect v54 channel-group, on page 34
- detect-fax mode, on page 35
- device-id, on page 36
- dhcp interface, on page 37
- dial-control-mib, on page 39
- dial-peer cor custom, on page 40
- dial-peer cor list, on page 42
- dial-peer data, on page 43
- dial-peer hunt, on page 45

- dial-peer inbound selection creation-order, on page 47
- dial-peer inbound selection sip-trunk, on page 48
- dial-peer no-match disconnect-cause, on page 50
- dial-peer outbound status-check pots, on page 51
- dial-peer search type, on page 54
- dial-peer terminator, on page 55
- dial-peer video, on page 56
- dial-peer voice, on page 57
- dial-type, on page 60
- dialer extsig, on page 62
- dialer preemption level, on page 63
- dialer trunkgroup, on page 65
- digit, on page 66
- digit-strip, on page 68
- digital-filter, on page 71
- direct-inward-dial, on page 72

default (auto-config application)

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 an auto-config application configuration command to its default value, use the **default** command in auto-config application configuration mode.

default *command*

Syntax Description

command	One of the auto-config application configuration commands. Valid choices are as follows: • **retries** • **server** • **shutdown** • **timeout**

Command Default

No default behavior or values

Command Modes

Auto-config application configuration (auto-config-app)

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.

Examples

The following example shows the **default** command used to set the number of download retry attempts for an auto-config application to its default value:

```
Router(auto-config-app)#
default retries
```

Related Commands

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

default (MGCP profile)

To configure a Media Gateway Control Protocol (MGCP profile) command to its default value, use the **default**command inMGCP profile configuration mode. To disable the default command, use the **no** form of the command for that profile parameter.

default *command*
no default *command*

Syntax Description

command	One of the MGCP profile commands. Valid choices are as follows: • **call-agent** • **description** (MGCP profile) • **max1 lookup** • **max1 retries** • **max2 lookup** • **max2 retries** • **package persistent** • **timeout tcrit** • **timeout tdinit** • **timeout tdmax** • **timeout tdmin** • **timeout thist** • **timeout tone busy** • **timeout tone cot1** • **timeout tone cot2** • **timeout tone dial** • **timeout tone dial stutter** • **timeout tone mwi** • **timeout tone network congestion** • **timeout tone reorder** • **timeout tone ringback** • **timeout tone ringback connection** • **timeout tone ringing** • **timeout tone ringing distinctive** • **timeout tpar** • **timeout tsmax** • **voice-port** (MGCP profile)

Command Default

No default behaviors or values

Command Modes

MGCP profile configuration (config-mgcp-profile)

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 an MGCP profile.

The **default**(MGCP profile) command instructs the MGCP profile to use the default value of the specified command whenever the profile is called. This has the same effect as using the **no** form of the specified command, but the **default** command clearly specifies which commands are using their default values.

To use the default values for more than one command, enter each command on a separate line.

Examples

The following example shows how to configure the default values for three MGCP profile commands:

```
Router(config)# mgcp profile newyork
Router(config-mgcp-profile)# default max1 retries
Router(config-mgcp-profile)# default timeout tdinit
Router(config-mgcp-profile)# default timeout tone mwi
```

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.

default (SIP)

To reset a SIP command to its default value, use the **default** command in SIP configuration mode.

default *command*

Syntax Description

command	One of the SIP configuration commands. Valid choices are: • **bind** : Configures the source address of signaling and media packets to a specific interface's IP address. • **rel1xx** : Enables all SIP provisional responses (other than 100 Trying) to be sent reliably to the remote SIP endpoint. • **session-transport** : Configures the underlying transport layer protocol for SIP messages to TCP or UDP. • **url** : Configures URLs to either the SIP or TEL format for your voip sip calls.

Command Default

The default is that binding is disabled (**no bind**).

Command Modes

Voice service voip-sip configuration (conf-serv-sip)

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.
12.2(2)XB2	This command was implemented on the Cisco AS5850 platform.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and support was added for the Cisco 3700 series. Cisco AS5300, Cisco AS5350, Cisco AS5850, and Cisco AS5400 platforms were not supported in this release.
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Examples

The following example shows how to reset the value of the SIP **bind** command:

```
Router(config)# voice serv voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# default bind
```

Related Commands

Command	Description
sip	Enter SIP configuration mode from voice-service VoIP configuration mode.

default-file vfc

To specify an additional (or different) file from the ones in the default file list and stored in voice feature card (VFC) flash memory, use the **default file vfc**command in global configuration mode. To delete the file from the default file list, use the **no** form of this command.

default-file *filename* **vfc** *slot*
no default-file *filename* **vfc** *slot*

Syntax Description

filename	Indicates the file to be retrieved from VFC flash memory and used to boot up the system.
slot	Indicates the slot on the Cisco AS5300 in which the VFC is installed. Range is to 2. There is no default value.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(1)NA	This command was introduced on the Cisco AS5300.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

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 that are used to boot up the system.

Use the **default-file vfc**command to add a specified file to the default file list, replacing the existing default for that extension type.

Examples

The following example specifies that the bas-vfc-1.0.14.0.bin file, which is stored in VFC flash memory, be added to the default file list:

```
default-file bas-vfc-1.0.14.0.bin vfc 0
```

Related Commands

Command	Description
cap-list vfc	Adds a voice codec overlay file to the capability file list.
delete vfc	Deletes a file from VFC flash memory.

define

To define the transmit and receive bits for North American ear and mouth (E&M), E&M Mercury Exchange Limited Channel-Associated Signaling (MELCAS), and Land Mobile Radio (LMR) voice signaling, use the **define** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

define {**tx-bits** | **rx-bits**} {**seize** | **idle**} {**0000** | **0001** | **0010** | **0011** | **0100** | **0101** | **0110** | **0111** | **1000** | **1001** | **1010** | **1011** | **1100** | **1101** | **1110** | **1111**}
no define {**tx-bits** | **rx-bits**} {**seize** | **idle**} {**0000** | **0001** | **0010** | **0011** | **0100** | **0101** | **0110** | **0111** | **1000** | **1001** | **1010** | **1011** | **1100** | **1101** | **1110** | **1111**}

Syntax Description

tx-bits	The bit pattern applies to the transmit signaling bits.
rx-bits	The bit pattern applies to the receive signaling bits.
seize	The bit pattern defines the seized state.
idle	The bit pattern defines the idle state.
0000 through **1111**	Specifies the bit pattern.

Command Default

The default is to use the preset signaling patterns as defined in American National Standards Institute (ANSI) and European Conference of Postal and Telecommunications Administrations (CEPT) standards, as follows:

- For North American E&M:
  - tx-bits idle 0000 (0001 if on E1 trunk)
  - tx-bits seize 1111
  - rx-bits idle 0000
  - rx-bits seize 1111
- For E&M MELCAS:
  - tx-bits idle 1101
  - tx-bits seize 0101
  - rx-bits idle 1101
  - rx-bits seize 0101
- For LMR:
  - tx-bits idle 0000
  - tx-bits seize 1111
  - rx-bits idle 0000
  - rx-bits seize 1111

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
11.3(1)MA3	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.1(2)T	The command was integrated into Cisco IOS Release 12.1(2)T.
12.3(4)XD	The LMR signaling type was added to the signaling types to which this command applies.
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 **define** command applies to E&M digital voice ports associated with T1/E1 controllers.

Use the **define** command to match the E&M bit patterns with the attached telephony device. Be careful not to define invalid configurations, such as all 0000 on E1, or identical seized and idle states. Use this command with the **ignore** command.

In LMR signaling, the **define** command is used to define polarity on E&M analog and digital voice ports.

Examples

To configure a voice port on a Cisco 2600 or Cisco 3600 series router that is sending traffic in North American E&M signaling format to convert the signaling to MELCAS format, enter the following commands:

```
voice-port 1/0/0
 define rx-bits idle 1101
 define rx-bits seize 0101
 define tx-bits idle 1101
 define tx-bits seize 0101
```

In this example, reverse polarity is configured on a voice port on a Cisco 3700 series router that is sending traffic in LMR signaling format:

```
voice-port 1/0/0
 define rx-bits idle 1111
 define rx-bits seize 0000
 define tx-bits idle 1111
 define tx-bits seize 0000
```

Related Commands

Command	Description
condition	Manipulates the signaling bit-pattern for all voice signaling types.
ignore	Configures a North American E&M or E&M MELCAS voice port to ignore specific receive bits.

delete vfc

To delete a file from voice feature card (VFC) flash memory, use the **delete vfc**command in privileged EXEC mode.

delete *filename* **vfc** *slot*

Syntax Description

filename	Specifies the file in VFC flash memory to be deleted.
slot	Specifies the slot on the Cisco AS5300 in which the specified VFC resides. Range is from 0 to 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(1)NA	This command was introduced on the Cisco AS5300.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

Use the **delete vfc**command to delete a specific file from VFC flash memory and to remove the file from the default list or capability list if the specified file is included in those lists.

Note Deleting a file from VFC flash memory does not free the VFC flash memory space that the file occupied. To free VFC flash memory space, use the **erase vfc** command.

Examples

The following example deletes the bas-vfc-1.0.14.0.bin file, which is stored in VFC flash memory of the VFC located in slot 0:

```
Router# delete bas-vfc-1.0.14.0.bin vfc 0
```

Related Commands

Command	Description
default-file vfc	Specifies an additional (or different) file from the ones in the default file list and stored in VFC flash memory.
erase vfc	Erases the flash memory of a specified VFC.
show vfc directory	Displays the list of all files that reside on this VFC.

description

To specify a description of the digital signal processor (DSP) interface, use the **description** command in voice-port or DSP farm interface configuration mode. To describe a MGCP profile that is being defined, use the **description** command in MGCP profile configuration mode. To specify the name or a brief description of a charging profile, use the **description** command in charging profile configuration mode. To delete a configured description, use the **no** form of the command in the appropriate configuration mode.

description *string*
no description

Syntax Description

string	Character string from 1 to 80 characters for DSP interfaces and MGCP profiles, or from 1 to 99 characters for charging profiles.

Command Default

Enabled with a null string. The MGCP profile has no default description. Charging profiles have no default description.

Command Modes

Voice-port configuration (config-voiceport)
DSP farm interface configuration (config-dspfarm-profile)
MGCP profile configuration (config-mgcp-profile)
Charging profile configuration (ch-prof-conf)

Usage Guidelines

The use of a special character such as '\'(backslash) and a three or more digit number for the character setting like **description**, results in incorrect translation.

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series and Cisco 7200.
11.3(1)MA	This command in voice-port configuration mode was implemented on the Cisco MC3810.
12.0(5)XE	This command in DSP farm interface configuration mode was modified.
12.1(1)T	The DSP farm interface configuration mode modification was integrated into Cisco IOS Release 12.1(1)T.
12.2(2)XA	This command was implemented on the Cisco AS5300.
12.2(11)T	This command was implimented on the Cisco AS5850 and integrated into Cisco IOS Release 12.2(11)T.
12.3(8)XU	This command was introduced in charging profile configuration mode.
12.3(11)YJ	This command in charging profile configuration mode was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command in charging profile configuration mode was integrated into Cisco IOS Release 12.3(14)YQ.
12.4(9)T	This was integrated into Cisco IOS Release 12.4(9)T.

Release	Modification
12.2(33)SXH	This command was changed to allow the description to contain spaces.

Usage Guidelines

Use the **description** command to describe the DSP interface connection or a defined MGCP profile. The information is displayed when a **show** command is used, and it does not affect the operation of the interface in any way.

In Release 12.2(33)SXH and later releases, you can enter spaces in the description.

Examples

The following example identifies voice port 1/0/0 as being connected to the purchasing department:

```
voice-port 1/0/0
 description purchasing-dept
```

The following example identifies DSP farm interface 1/0 as being connected to the marketing department:

```
dspint dspfarm 1/0
 description marketing-dept
```

The following example shows a description for an MGCP profile:

```
mgcp profile newyork
 description This is the head sales office in New York.
 dot ...(socket=0)
 S:.
 R:250 NAA09092 Message accepted for delivery
 S:QUIT
 R:221 madeup@abc.com closing connection
 Freeing SMTP ctx at 0x6121D454
 returned from work-routine, context freed
```

The following example describes a charging profile as APN-level default for home users:

```
gprs charging profile
 description APN-level_default_for_home_users
```

Related Commands

Command	Description
category	Identifies the subscriber category to which a charging profile applies.
cdr suppression	Specifies that CDRs be suppressed as a charging characteristic in a charging profile.
charging profile	Associates a default charging profile to an access point.
content dcca profile	Defines a DCCA client profile in a GGSN charging profile.
content postpaid time	Specifies, as a trigger condition for postpaid users in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.

Command	Description
content postpaid validity	Specifies, as a trigger condition in a charging profile, that the amount of time quota granted to a postpaid user is valid.
content postpaid volume	Specifies, as a trigger condition for postpaid users in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
content rulebase	Associates a default rule-base ID with a charging profile.
gprs charging characteristics reject	Specifies that create PDP context requests for which no charging profile can be selected be rejected by the GGSN.
gprs charging container time-trigger	Specifies a global time limit that when exceeded by a PDP context causes the GGSN to close and update the G-CDR for that particular PDP context.
gprs charging profile	Creates a new charging profile (or modifies an existing one) and enters charging profile configuration mode.
limit duration	Specifies, as a trigger condition in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
limit sgsn-change	Specifies, as a trigger condition in a charging profile, the maximum number of GGSN changes that can occur before closing and updating the G-CDR for a particular PDP context.
limit volume	Specifies, as a trigger condition in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
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.
tariff-time	Specifies that a charging profile use the tariff changes configured using the **gprs charging tariff-time**global configuration command.

description (ctl file)

To set a description for the Cisco Certificate Trust List (CTL) file, use the **description** command in CTL file configuration mode. To remove the description for the CTL file, use the **no** form of the command.

description *description*

Syntax Description

description	Description of the CTL file. The maximum length of the description is 100 characters.

Command Default

No description is set.

Command Modes

CTL file configuration mode (config-ctl-file)

Command History

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

Usage Guidelines

Example

The following example shows how to set a description for the CTL file instance:

```
Device(config)# voice-ctl-file myctl
Device(config-ctl-file)# description ctlfile1
```

description (dial peer)

To add a description to a dial peer, use the **description** command in dial peer configuration mode. To remove the description, use the **no** form of this command.

description *string*
no description

Syntax Description

string	Text string up to 64 alphanumeric characters.

Command Default

Disabled

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.2(2)T	This command was introduced.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

Use this command to include descriptive text about the dial peer. The description displays in **show** command output and does not affect the operation of the dial peer.

Examples

The following example shows a description included in a dial peer:

```
dial-peer voice 1 pots
 description inbound PSTN calls
```

Related Commands

Command	Description
dial-peer voice	Defines a dial peer.
show dial-peer voice	Displays configuration information for dial peers.

description (DSP farm profile)

To include a description about the digital signal processor (DSP) farm profile, use the **description** command in DSP farm profile configuration mode. To remove a description, use the **no** form of this command.

description *text*
no description *text*

Syntax Description

text	Character string from 1 to 80 characters.

Command Default

No default behavior or values

Command Modes

DSP farm profile configuration (config-dspfarm-profile)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use this command to include descriptive text about this DSP farm profile. This information displays in **show** commands and does not affect the operation of the interface.

Examples

The following example identifies the DSP farm profile as being designated to the art department:

```
Router(config-dspfarm-profile)# description art dept
```

Related Commands

Command	Description
codec (DSP farm 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 (DSP Farm profile)	Specifies the maximum number of sessions that need to be supported by the profile.
shutdown (DSP farm profile)	Allocates DSP farm resources and associates with the application.

description (dspfarm)

To include a specific description about the digital signal processor (DSP) interface, use the **description** command in DSP farm interface configuration mode. To disable this feature, use the **no** form of this command.

description *string*
no description *string*

Syntax Description

string	Character string from 1 to 80 characters.

Command Default

Enabled with a null string.

Command Modes

DSP farm interface configuration (config-dspfarm-profile)

Command History

Release	Modification
11.3(1)T	This command was introduced for the Cisco 7200 series routers.
12.0(5)XE	This command was modified to reduce the maximum number of allowable characters in a text string from 255 to 80.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Use the **description** command to include descriptive text about this DSP farm interface connection. This information is displayed when you issue a **show**command and does not affect the operation of the interface in any way.

Examples

The following example identifies DSP farm interface 1/0 on the Cisco 7200 series routers router as being connected to the marketing department:

```
dspint dspfarm 1/0
description marketing dept
```

description (media-profile)

To include a description specific to a media profile in CUBE, use the **description** command in media profile configuration mode. To remove the description, use the **no** form of this command.

connection description *string*
no connection description *string*

Syntax Description

string	A description specific to the media profile.

Command Default

Disabled by default.

Command Modes

Media Profile configuration mode (cfg-mediaprofile)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command was introduced on Cisco Unified Border Element.

Usage Guidelines

The **description** command provides details specific to a media profile.

Examples

The following is a sample configuration for **description (media-profile)** in CUBE:

```
router(cfg-mediaprofile)#description ?
WORD Specify hostname or IP address of proxy server

router(cfg-mediaprofile)#description <text>
```

Related Commands

Command	Description
media profile stream-service	Enables stream service on CUBE.
connection (media-profile)	Configures idle timeout and call threshold for a media profile.
proxy (media-profile)	Configures IP address or hostname of proxy in media profile.
source-ip (media-profile)	Configures local source IP address of a WebSocket connection.
media class	Applies the media class at the dial peer level.

description (phone proxy)

To specify a description for the phone proxy, use the **description** command in phone proxy configuration mode. To remove the description, use the **no** form of the command.

description*description*
no description

Syntax Description

This command has no arguments or keywords.

Command Default

No description is 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 create a phone proxy instance called first-pp, enter phone-proxy configuration mode, and set the description for this instance:

```
Device(config)# voice-phone-proxy first-pp
Device(config-phone-proxy)# description cluster-test
```

description (SCCP Cisco CallManager)

To include a description about the Cisco CallManager group, use the **description** command in SCCP Cisco CallManager configuration mode. To remove a description, use the **no** form of this command.

description *text*
no description

Syntax Description

text	Character string from 1 to 80 characters.

Command Default

No default behavior or values

Command Modes

SCCP Cisco CallManager configuration (config-sccp-ccm)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use this command to include descriptive text about a Cisco CallManager group. This information is displayed in **show** commands and does not affect the operation of the interface.

Examples

The following example identifies SCCP as being designated to the Boston office:

```
Router(config-sccp-ccm)# description boston office
```

Related Commands

Command	Description
associate ccm	Associates a Cisco CallManager with a Cisco CallManager group and establishes its priority within the group.
connect retries	Specifies the number of times that a DSP farm attempts to connect to a Cisco CallManager when the current Cisco CallManager connections fails.
sccp ccm group	Creates a Cisco CallManager group and enters SCCP Cisco CallManager configuration mode.

description (trunk group)

To add a description to a trunk group, use the **description** command in trunk group configuration mode. To delete the description, use the **no**form of this command.

description *string*
no description *string*

Syntax Description

string	Trunk group description. Maximum length is 63 alphanumeric characters.

Command Default

No default behavior or values

Command Modes

Trunk group configuration (config-trunk-group)

Command History

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

Examples

The following example shows a description for a trunk group:

```
Router(config)# trunk group alpha1
Router(config-trunk-group)# description carrierAgroup1
```

Related Commands

Command	Description
trunk group	Initiates the definition of a trunk group.

description (voice class)

To provide a TLS profile group description, and associate it to a TLS profile, use the command **description** in voice class configuration mode. To delete the TLS profile group description, use **no** form of this command.

description *tls-profile-group-label*
no description

Syntax Description

tls-profile-group-label	Allows you to provide a description for the TLS profile group.

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.

Usage Guidelines

The TLS profile group description is associated to a TLS profile through the command **voice class tls-profile** *tag*. The *tag* associates the TLS profile group description to the command **crypto signaling**.

Examples

The following example illustrates how to create a voice class tls-profile and associate a description TLS profile group:

```
Router(config)#voice class tls-profile 2
Router(config-class)#description tlsgroupname
```

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.

description (voice source group)

To add a description to a voice source group, use the **description** command in voice source-group configuration mode. To delete the description, use the **no**form of this command.

description *string*
no description *string*

Syntax Description

string	Describes a voice source group, Maximum length of the voice source group description is 63 alphanumeric characters.

Command Default

No default behavior or values

Command Modes

Voice source-group configuration (cfg-source-grp)

Command History

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

Examples

The following example shows a description for a voice source group:

```
Router(config)# voice source-group northern1
Router(cfg-source-grp)# description carrierBgroup3
```

Related Commands

Command	Description
voice source-group	Defines a source group for voice calls.

destination e164-pattern-map

To link an E.164 pattern map to a dial peer, use the **destination e164-pattern-map** command in dial peer configuration mode. To remove the link of an E.164 pattern map from a dial peer, use the **no** form of this command.

destination e164-pattern-map *tag*
no destination e164-pattern-map

Syntax Description

tag	A number that defines a destination E.164 pattern map. The range is from 1 to 10000.

Command Default

An E.164 pattern map is not linked to a dial peer.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

To support dial peer with multiple destination patterns, which involve massive dial peer configuration, use an E.164 destination pattern map. You can create a destination E.164 pattern map and then link it to one or more dial peers. Based on the validation of a pattern map, you can enable or disable one or more dial peers linked to the destination E.164 pattern map. To get the status of the configured E.164 pattern map, use the **show dial-peer voice** command in dial peer configuration mode.

Examples

The following example shows how to link an E.164 pattern map to a dial peer:

```
Device(config)# dial-peer voice 123 voip system

Device(config-dial-peer)# destination e164-pattern-map 2154
```

Related Commands

Command	Description
destination-pattern	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer
e164	Configures an E.164 entry on a destination E.164 pattern map.
show dial-peer voice	Displays configuration information and call statistics for dial peers.
url	Specifies the URL of a text file that has E.164 pattern entries configured on a destination E.164 pattern map.

destination uri

To specify the voice class used to match a dial peer to the destination uniform resource identifier (URI) of an outgoing call, use the **destination uri**command in dial peer configuration mode. To remove the URI voice class, use the **no** form of this command.

destination uri *tag*
no destination uri

Syntax Description

tag	Alphanumeric label that uniquely identifies the voice class. This tag must be configured with the **voice class uri** command.

Command Default

No default behavior or values

Command Modes

Dial peer configuration (config-dial-peer)

Command History

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

Usage Guidelines

Before you use this command, configure the voice class by using the **voice class uri** command.

This command applies new rules for dial-peer matching. The table below shows the rules and the order in which they are applied when the **destination uri** command is used. The gateway compares the dial-peer command to the call parameter in its search to match an outbound call to a dial peer. All dial peers are searched based on the first match criteria on . Only if no match is found does the gateway move on to the next criteria on.

Table 1: Dial-Peer Matching Rules for Outbound URI

Match Order	Cisco IOS Command	Outgoing Call Parameter
1	**destination uri** and **carrier-id target**	Application-provided URI and target carrier ID associated with the call
2	**destination-pattern** and **carrier-id target**	Called number and target carrier ID associated with the call
3	**destination uri**	Application-provided URI
4	**destination-pattern**	Called number
5	**carrier-id target**	Target carrier ID associated with the call

Note Calls whose destination is an E.164 number, rather than a URI, use the previously existing dial-peer matching rules. For information, see the *Dial Peer Configuration on Voice Gateway Routers* document, Cisco IOS Voice Library.

Examples

The following example matches the destination URI in the outgoing call by using voice class ab100:

```
dial-peer voice 100 voip
 destination uri ab100
```

Related Commands

Command	Description
answer-address	Specifies the calling number to match for a dial peer.
debug voice uri	Displays the debugging messages related to URI voice classes.
destination-pattern	Specifies the telephone number to match for a dial peer.
dial-peer voice	Enters dial peer configuration mode to create or modify a dial peer.
incoming uri	Specifies the voice class that a VoIP dial peer uses to match the URI of an incoming call.
pattern	Matches a call based on the entire SIP or TEL URI.
session protocol	Specifies a session protocol for calls between local and remote routers using the packet network.
show dialplan uri	Displays which outbound dial peer is matched for a specific destination URI.
voice class uri	Creates or modifies a voice class for matching dial peers to calls containing a SIP or TEL URI.

destination-pattern

To specify either the prefix or the full E.164 telephone number to be used for a dial peer, use the **destination-pattern** command in dial peer configuration mode. To disable the configured prefix or telephone number, use the **no** form of this command.

destination-pattern[**+**]*string*[**T**]
no destination-pattern[**+**]*string*[**T**]

Syntax Description

+	(Optional) Character that indicates an E.164 standard number.
string	Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: • The asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit (this character is used as a wildcard). • Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage. • Plus sign (+), which indicates that the preceding digit occurred one or more times. **Note** The plus sign used as part of a digit string is different from the plus sign that can be used preceding a digit string to indicate that the string is an E.164 standard number. • Circumflex (^), which indicates a match to the beginning of the string. • Dollar sign ($), which matches the null string at the end of the input string. • Backslash symbol (\), which is followed by a single character, and matches that character. Can be used with a single character with no other significance (matching that character). • Question mark (?), which indicates that the preceding digit occurred zero or one time. • Brackets ([ ]), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters from 0 to 9 are allowed in the range. • Parentheses (( )), which indicate a pattern and are the same as the regular expression rule.
T	(Optional) Control character that indicates that the **destination-pattern** value is a variable-length dial string. Using this control character enables the router to wait until all digits are received before routing the call.

Command Default

The command is enabled with a null string.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA	This command was implemented on the Cisco MC3810.
12.0(4)XJ	This command was modified for store-and-forward fax.
12.1(1)	The command was integrated into Cisco IOS Release 12.1(1).
12.0(7)XR	This command was implemented on the Cisco AS5300 and modified to support the plus sign, percent sign, question mark, brackets, and parentheses symbols in the dial string.
12.0(7)XK	This command was modified. Support for the plus sign, percent sign, question mark, brackets, and parentheses in the dial string was added to 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 Cisco 1750, Cisco 7200 series, and Cisco 7500 series. The modifications for the Cisco MC3810 in Cisco IOS Release12.0(7)XK are not supported in this release.
12.1(2)T	The modifications made in Cisco IOS Release 12.0(7)XK for the Cisco MC3810 were integrated into Cisco IOS Release 12.1(2)T.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series and Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented on the Cisco 2600XM, the Cisco ICS7750, and the Cisco VG200.
12.4(22)T	Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)M	This command was modified. With CSCub65380, behavior of dial peers with destination-patterns configured with + symbol was rectified. The + symbol is no longer dropped from the dial peers and matching occurs as expected
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

Use the **destination-pattern** command to define the E.164 telephone number for a dial peer.

The pattern you configure is used to match dialed digits to a dial peer. The dial peer is then used to complete the call. When a router receives voice data, it compares the called number (the full E.164 telephone number) in the packet header with the number configured as the destination pattern for the voice-telephony peer. The router then strips out the left-justified numbers that correspond to the destination pattern. If you have configured a prefix, the prefix is prepended to the remaining numbers, creating a dial string that the router then dials. If all numbers in the destination pattern are stripped out, the user receives a dial tone.

There are areas in the world (for example, certain European countries) where valid telephone numbers can vary in length. Use the optional control character **T**to indicate that a particular **destination-pattern** value is

a variable-length dial string. In this case, the system does not match the dialed numbers until the interdigit timeout value has expired.



Note Cisco IOS software does not verify the validity of the E.164 telephone number; it accepts any series of digits as a valid number.

Examples

The following example shows configuration of the E.164 telephone number 555-0179 for a dial peer:

```
dial-peer voice 10 pots
 destination-pattern +5550179
```

The following example shows configuration of a destination pattern in which the pattern "43" is repeated multiple times preceding the digits "555":

```
dial-peer voice 1 voip
 destination-pattern 555(43)+
```

The following example shows configuration of a destination pattern in which the preceding digit pattern is repeated multiple times:

```
dial-peer voice 2 voip
 destination-pattern 555%
```

The following example shows configuration of a destination pattern in which the possible numeric values are between 5550109 and 5550199:

```
dial-peer voice 3 vofr
 destination-pattern 55501[0-9]9
```

The following example shows configuration of a destination pattern in which the possible numeric values are between 5550439, 5553439, 5555439, 5557439, and 5559439:

```
dial-peer voice 4 voatm
 destination-pattern 555[03579]439
```

The following example shows configuration of a destination pattern in which the digit-by-digit matching is prevented and the entire string is received:

```
dial-peer voice 2 voip
 destination-pattern 555T
```

Related Commands

Command	Description
answer-address	Specifies the full E.164 telephone number to be used to identify the dial peer of an incoming call.
dial-peer terminator	Designates a special character to be used as a terminator for variable-length dialed numbers.
incoming called-number (dial peer)	Specifies a digit string that can be matched by an incoming call to associate that call with a dial peer.

Command	Description
prefix	Specifies the prefix of the dialed digits for a dial peer.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.

destination-pattern (interface)

To specify the ISDN directory number for the telephone interface, use the **destination-pattern** command in interface configuration mode. To disable the specified ISDN directory number, use the **no** form of this command.

destination-pattern *isdn*
no destination-pattern

Syntax Description

isdn	Local ISDN directory number assigned by your telephone service provider.

Command Default

A default ISDN directory number is not defined for this interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series.

Usage Guidelines

This command is applicable to the Cisco 800 series routers.

You must specify this command when creating a dial peer. This command does not work if it is not specified within the context of a dial peer. For information on creating a dial peer, refer to the *Cisco 800 Series Routers Software Configuration Guide*.

Do not specify an area code with the local ISDN directory number.

Examples

The following example specifies 555-0101 as the local ISDN directory number:

```
destination-pattern 5550101
```

Related Commands

Command	Description
dial-peer voice	Enters dial peer configuration mode, defines the type of dial peer, and defines the tag number associated with a dial peer.
no call-waiting	Disables call waiting.
port (dial peer)	Enables an interface on a PA-4R-DTR port adapter to operate as a concentrator port.
ring	Sets up a distinctive ring for telephones, fax machines, or modems connected to a Cisco 800 series router.
show dial-peer voice	Displays configuration information and call statistics for dial peers.

destination route-string

To configure a destination route string, use the **destination route-string** command in dial peer configuration mode. To remove the destination route string, use the **no** form of this command.

destination route-string *tag*
no destination route-string

Syntax Description

tag	The route string tag defined by the route string class. The range is from 1 to 10000.

Command Default

No destination route string is configured.

Command Modes

Dial peer configuration (config-dial-peer)

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 **destination route-string** command to configure a voice class to match a destination route string. The destination route string defined in dial-peer voice configuration mode is used to match an outbound dial peer.

Example

The following example shows how to match the destination route string:

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 100 voip
Device(config-dial-peer)# destination route-string 2
```

Related Commands

Command	Description
voice class route-string	Assigns a unique identifier tag to a route string.

detect v54 channel-group

To enable V.54 loopback detection for the command sent from the remote device, use the **detect v54 channel-group**command in controller configuration mode. To disable the V.54 loopback detection, use the **no** form of this command.

detect v54 channel-group *channel-number*
no detect v54 channel-group *channel-number*

Syntax Description

channel-number	Channel number from 1 to 24 (T1) or from 1 to 31 (E1).

Command Default

V.54 loopback detection is disabled.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Use the **detect v54 channel-group** controller configuration command to enable V.54 loopback detection. The remote device sends a loopup inband payload command sequence in fractional T1 (FT1).

Examples

The following example sets the loopback detection for channel-group 1; then the loopback detection is disabled for channel-group 1:

```
detect v54 channel-group 1
no detect v54 channel-group 1
```

Related Commands

Command	Description
loopback remote v54 channel-group	Activates a remote V.54 loopback for the channel group on the far end.

detect-fax mode

To define fax detection and redirect as local or refer mode, use the **detect-fax** [**mode {refer | local}**] *number* command in dial peer configuration mode. To disable the mode of fax detection and redirect, use the **no** form of this command.

detect-fax [**mode {refer | local}**] *number*
no detect-fax [**mode {refer | local}**] *number*

Syntax Description

number	The directory number of the fax machine.

Command Default

Fax mode detection is disabled.

Command Modes

Dial Peer configuration (config-dial-peer)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1r	This command was introduced for Unified Border Element.

Usage Guidelines

Use the **detect-fax** [**mode {refer | local}**] *number* configuration command to enable detection of fax mode. Also, it refers to the directory number of the fax machine for redirect.

Examples

The following is a sample configuration of local redirect mode for fax detection in Unified Border Element:

```
dial-peer voice 410 voip
 description "Incoming dial-peer to CUBE for fax"
 session protocol sipv2
 incoming called-number 903309
 codec g711ulaw
 detect-fax mode local 12101 12102

dial-peer voice 411 voip
 description "Outgoing dial-peer to VVB"
 destination-pattern 309903
 session protocol sipv2
 session target ipv4:9.42.25.148 //VVB IP Address
 codec g711ulaw

dial-peer voice 412 voip
 description "Incoming dial-peer for VVB"
 session protocol sipv2
 incoming called-number 309903
 codec g711ulaw
```

Related Commands

Command	Description
fax-relay (dial peer)	Enables the suppression of call menu (CM) tones or answer (ANS) tones from reaching the Super Group 3 (SG3) fax machines.

device-id

To identify a gateway associated with a settlement provider, use the **device-id** command in settlement configuration mode. To reset to the default value, use the **no** form of this command.

device-id *number*
no device-id *number*

Syntax Description

number	Device ID number as provided by the settlement server. Range is from 0 to 2147483647.

Command Default

The default device ID is 0.

Command Modes

Settlement configuration (config-settlement)

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Identifying a gateway associated with a settlement provider is optional.

Examples

The following example sets the device ID to 1000:

```
settlement 0
 device-id 1000
```

Related Commands

Command	Description
customer-id	Identifies a carrier or Internet service provider with the settlement provider.
settlement	Enters settlement configuration mode.

dhcp interface

To configure an interface type for Dynamic Host Configuration Protocol (DHCP) provisioning of Session Initiation Protocol (SIP) parameters, use the **dhcp interface** command in SIP user-agent configuration mode.

dhcp interface *type number*

Syntax Description

type	Type of interface to be configured.
number	Port, connector, or interface card number. **Note** The number format varies depending on the network module or line card type and the router's chassis slot it is installed in. The numbers are assigned at the factory at the time of installation or when they are added to a system; they can be displayed with the **show interfaces** command.

Command Default

No interface type is configured for DHCP provisioning of SIP parameters.

Command Modes

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated in Cisco IOS Release 15.0(1)M.

Usage Guidelines

Multiple interfaces on the Cisco Unified Border Element can be configured with DHCP. The **dhcp interface** command specifies which one is the DHCP interface used with SIP.

This command does not have a **no** form.

The table below displays the keywords that represent the types of interfaces that can be configured with the **dhcp interface** command. Replace the *type* argument with the appropriate keyword from the table.

Table 2: Interface Type Keywords

Keyword	Interface Type
ethernet	Ethernet IEEE 802.3 interface.
fastethernet	100-Mbps Ethernet interface. In RITE configuration mode, specifies the outgoing (monitored) interface for exported IP traffic.
gigabitethernet	1000-Mbps Ethernet interface.
tengigabitethernet	10-Gigabit Ethernet interface.

Examples

The following example configures the Gigabit Ethernet interface of slot 0 port 0 as the DHCP interface for DHCP provisioning of SIP parameters:

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0/0
Router(config-if)# ip address dhcp
Router(config-if)# sip-ua
Router(sip-ua)# dhcp interface gigabitethernet 0/0
```

Related Commands

Command	Description
show interfaces	Displays information about interfaces.
sip-ua	Enters SIP user-agent configuration mode.

dial-control-mib

To specify attributes for the call history table, use the **dial-control-mib** command in global configuration mode. To restore the default maximum size or retention time of the call history table, use the **no** form of this command.

dial-control-mib {**max-size** *table-entries* | **retain-timer** *minutes*}
no dial-control-mib {**max-size** *table-entries* | **retain-timer** *minutes*}

Syntax Description

max-size *table-entries*	Maximum number of table entries in the call history table. Range is from 0 to 3000. **Note** Specifying a value of 0 prevents any further entries from being added to the table. Any existing table entries will be preserved for the duration specified with the **retain-timer** keyword.
retain-timer *minutes*	Duration, in minutes, for entries to remain in the call history table. Range is from 0 to 35791. **Note** Specifying a value of 0 prevents any further table entries from being retained, but does not affect any timer currently in effect. Therefore, any existing table entries will remain for the duration previously specified with the **retain-timer** keyword.

Command Default

The default call history table length is 500 table entries. The default retain timer is 15 minutes.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series routers.
12.0(1)XA	This command was first applied to the CDR feature on the Cisco MC3810.
12.0(2)T	The command was integrated into Cisco IOS Release 12.0(2)T.
12.3T	The maximum value for the *table-entries* argument following the **max-size** keyword was increased to 1200 entries.
12.3(8)T	The maximum value of the *minutes* argument following the **retain-timer** keyword was decreased to 35791 minutes.

Examples

The following example configures the call history table to hold 400 entries, with each entry remaining in the table for 10 minutes:

```
dial-control-mib max-size 400
dial-control-mib retain-timer 10
```

dial-peer cor custom

To specify that named class of restrictions (COR) apply to dial peers, use the **dial-peer cor custom** command in global configuration mode.

dial-peer cor custom

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or keywords.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
Cisco IOS XE Bengaluru 17.6.1a	Introduced support for YANG models.

Usage Guidelines

You must use the **dial-peer cor custom**command and the **name** command to define the names of capabilities before you can specify COR rules and apply them to specific dial peers.

Examples of possible names might include the following: call1900, call527, call9, and call911.

Note You can define a maximum of 64 COR names.

Examples

The following example defines two COR names:

```
dial-peer cor custom
 name samplegroup32
 name samplegroup12
```

The following example defines Webex Calling COR names:

```
dial-peer cor custom
 name wx-calling_Internal
 name wx-calling_Toll-fre
 name wx-calling_National
 name wx-calling_International
 name wx-calling_Operator_Assistance
 name wx-calling_chargeable_Directory_Assistance
 name wx-calling_Special_Sevices1
 name wx-calling_Special_Sevices2
 name wx-calling_Premium_Sevices1
 name wx-calling_Premium_Sevices2
```

Related Commands

Command	Description
name (dial peer cor custom)	Provides a name for a custom COR.

dial-peer cor list

To define a class of restrictions (COR) list name, use the **dial-peer cor list** command in global configuration mode. To remove a previously defined COR list name, use the **no** form of this command.

dial-peer cor list *list-name*
no dial-peer cor list *list-name*

Syntax Description

list-name	List name that is applied to incoming or outgoing calls to specific numbers or exchanges.

Command Default

No default behavior or keywords.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
Cisco IOS XE Bengaluru 17.6.1a	Introduced support for YANG models.

Usage Guidelines

A COR list defines a capability set that is used in the COR checking between incoming and outgoing dial peers.

Examples

The following example adds two members to the COR list named list1:

```
dial-peer cor list list1
 member 900block
 member 800call
```

Related Commands

Command	Description
dial-peer cor custom	Specifies that named COR apply to dial peers.
member (dial peer cor list)	Adds a member to a dial peer COR list.
name (dial peer cor custom)	Provides a name for a custom COR.

dial-peer data

To create a data dial peer and to enter dial-peer configuration mode, use the **dial-peer data** command in global configuration mode. To remove a data dial peer, use the **no** form of this command.

dial-peer data *tag* **pots**
no dial-peer data *tag*

Syntax Description

tag	Specifies the dial-peer identifying number. Range is from 1 to 2147483647.
pots	Specifies an incoming POTS dial peer.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.4(4)XC	This command was implemented on the Cisco 2600XM series, Cisco 2800 series, Cisco 3700 series, and Cisco 3800 series.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

A data dial peer should be defined only for incoming data calls. The **incoming called-number** and **shutdown** commands on the data dial peer are allowed. However, the following POTS dial-peer commands are disabled on a data dial peer:

- **answer-address**
- **carrier-id**
- **destination-pattern**
- **information-type**
- **port**
- **trunk-group-label**

Examples

The following example is a data dial-peer configuration:

```
dial-peer data 100 pots
 incoming called-number 100
```

The following example is a voice dial-peer configuration:

```
dial-peer voice 2001 pots
 destination-pattern 2001
```

```
no digit-strip
port 3/1:1
```

Related Commands

Command	Description
dial-peer search	Optimizes voice or data dial-peer searches.
incoming called-number	Specifies an incoming called number of an MMoIP or POTS dial peer.
shutdown (dial peer)	Changes the administrative state of a selected dial peer from up to down.

dial-peer hunt

To specify a hunt selection order for dial peers, use the **dial-peer hunt** command in global configuration mode. To restore the default selection order, use the **no** form of this command.

dial-peer hunt *hunt-order-number*
no dial-peer hunt

Syntax Description

hunt-order-number	A number from 0 to 7 that selects a predefined hunting selection order: • 0--Longest match in phone number, explicit preference, random selection. This is the default hunt order number. • 1--Longest match in phone number, explicit preference, least recent use. • 2--Explicit preference, longest match in phone number, random selection. • 3--Explicit preference, longest match in phone number, least recent use. • 4--Least recent use, longest match in phone number, explicit preference. • 5--Least recent use, explicit preference, longest match in phone number. • 6--Random selection. • 7--Least recent use.

Command Default

The default is the longest match in the phone number, explicit preference, random selection (hunt order number 0).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XK	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco MC3810, and Cisco AS5300.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use the **dial-peer hunt** dial peer configuration command if you have configured hunt groups. "Longest match in phone number" refers to the destination pattern that matches the greatest number of the dialed digits. "Explicit preference" refers to the **preference** command setting in the dial-peer configuration. "Least recent use" refers to the destination pattern that has waited the longest since being selected. "Random selection" weights all of the destination patterns equally in a random selection mode.

This command applies to POTS, VoIP, Voice over Frame Relay (VoFR), Voice over ATM (VoATM), and Multimedia Mail over Internet Protocol (MMOIP) dial peers.

Examples

The following example configures the dial peers to hunt in the following order: (1) longest match in phone number, (2) explicit preference, (3) random selection.

```
dial-peer hunt 0
```

Related Commands

Command	Description
destination-pattern	Specifies the prefix or the complete telephone number for a dial peer.
preference	Specifies the preferred selection order of a dial peer within a hunt group.
show dial-peer voice	Displays configuration information for dial peers.

dial-peer inbound selection creation-order

To enable incoming dial-peer selection without changing the creation order when sorting the longest matched numbers, use **dial-peer inbound selection creation-order** command. To revert to the default behavior, use the **no** form of this command

dial-peer inbound selection creation-order
no dial-peer inbound selection creation-order

Syntax Description

This command has no arguments or keywords.

Command Default

The default behavior does not guarantee that the creation order would be retained for multiple dial-peers with the same number of matched digits due to the unstable heap sorting algorithm.

Command Modes

Global configuration (config)

Command History

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

Example

```
Device(config)# dial-peer inbound selection creation-order
```

dial-peer inbound selection sip-trunk

To enable incoming SIP line-side calls to use the same dial-peer matching rules as SIP trunk-side calls, use the **dial-peer inbound selection sip-trunk** command in global configuration mode. To revert to the default behavior, use the **no** form of this command.

dial-peer inbound selection sip-trunk
no dial-peer inbound selection sip-trunk

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled (SIP line-side and SIP trunk-side calls use different dial-peer matching rules).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)T2	This command was introduced.

Usage Guidelines

This command applies the same dial-peer matching rules used for calls from SIP trunks to incoming calls from SIP phones (line side). The first table below shows the rules and the order in which they are applied by default to SIP line-side calls. The second table below shows the rules and the order in which they are applied to SIP trunk-side calls and to SIP line-side calls when the **dial-peer inbound selection sip-trunk** command is used.

The router compares the dial-peer configuration to the call parameter in its search to match an inbound call to a dial peer. All dial peers are searched based on the first match criteria. The router moves on to the next criteria only if no match is found.

Table 3: Dial-Peer Matching Rules for Inbound Calls from SIP Phones (Line Side)

Match Order	Cisco IOS Command	Incoming Call Parameter
1	**destination-pattern**	Calling number
2	**answer-address**	Calling number
3	**incoming called-number**	Called number
4	**incoming uri request**	Request-URI
5	**incoming uri to**	To URI
6	**incoming uri from**	From URI
7	**carrier-id source**	Carrier-is associated with the call

Table 4: Dial-Peer Matching Rules for Inbound Calls from SIP Trunks

Match Order	Cisco IOS Command	Incoming Call Parameter
1	**incoming uri request**	Request-URI
2	**incoming uri to**	To URI
3	**incoming uri from**	From URI
4	**incoming called-number**	Called number
5	**answer-address**	Calling number
6	**destination-pattern**	Calling number
7	**carrier-id source**	Carrier-is associated with the call

Examples

The following example shows SIP line-side calls use the same matching rules as trunk-side calls:

```
dial-peer inbound selection sip-trunk
```

Related Commands

Command	Description
answer-address	Specifies calling number to match for a dial peer.
destination-pattern	Specifies telephone number to match for a dial peer.
dial-peer voice	Defines a specific dial peer.
incoming called-number	Incoming called number matched to a dial peer.
incoming uri	Specifies the voice class used to match a VoIP dial peer to the uniform resource identifier (URI) of an incoming call.
show dial-peer voice	Displays configuration information for voice dial peers.

dial-peer no-match disconnect-cause

To disconnect the incoming ISDN or channel associated signaling (CAS) call when no inbound voice or modem dial peer is matched, use the **dial-peer no-match disconnect-cause**command in global configuration mode. To restore the default incoming call state (call is forwarded to the dialer), use the **no** form of this command.

dial-peer no-match disconnect-cause *cause-code-number*
no dial-peer no-match disconnect-cause *cause-code-number*

Syntax Description

cause-code-number	An ISDN cause code number. Range is from 1 to 127.

Command Default

The call is forwarded to the dialer to handle as a modem call.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

By default, calls are forwarded to the dialer to handle as a modem call when no inbound dial peer is matched. The **dial-peer no-match disconnect-cause**command changes that behavior to disconnect the incoming ISDN or CAS calls when no inbound voice or modem dial peer is matched.

Refer to the ISDN Cause Values table in the *Cisco IOS Debug Command Reference* for a list of ISDN cause codes.

Examples

The following example shows that ISDN cause code 47 has been specified to match inbound voice or modem dial peers:

```
dial-peer no-match disconnect-cause 47
```

Related Commands

Command	Description
show dial-peer voice	Displays configuration information for dial peers.

dial-peer outbound status-check pots

To check the status of outbound POTS dial peers during call setup and to disallow, for that call, any dial peer whose status is down, use the **dial-peer outbound status-check pots**command in privileged EXEC mode. To disable status checking, use the **no** form of this command.

dial-peer outbound status-check pots
no dial-peer outbound status-check pots

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3	This command was introduced.

Usage Guidelines

Use this command to disallow, during call setup, outbound POTS dial peers (except those for e-phones) whose endpoints (voice ports or trunk groups) are down.

When the **dial-peer outbound status-check pots**command is configured, if the voice-port configured under an outbound POTS dial-peer is down, that dial-peer is excluded while matching the corresponding destination-pattern. Therefore, if there are no other matching outbound POTS dial-peers for the specified destination-pattern, the gateway will disconnect the call with a cause code of 1 (Unallocated/unassigned number), which is mapped to the "404 Not Found" SIP response by default. When the **no** form of this command is configured, the outbound POTS dial-peer is matched even if the voice-port configured under is down and the gateway disconnects the call with a cause code of 34 (No circuit/channel available), which is mapped to the "503 Service Unavailable" SIP response by default.

Note "503 Service Unavailable" was the default behavior before the **dial-peer outbound status-check pots**command was introduced. Users who need the original behavior should configure the **no** form of this command.

The table below shows conditions under which an outbound POTS dial peer may be up or down.

Table 5: Conditions Under Which an Outbound POTS Dial Peer Is Up or Down

If a Dial Peer's...	And If...	Then the Dial Peer Is...
Operational state is up	Its voice port is up	Up
	Its trunk groups and any associated trunks are up	

If a Dial Peer's...	And If...	Then the Dial Peer Is...
Operational state is down	--	Down
Voice port is down		
Trunk groups are down	All associated trunks are down	

To show or verify the status (up or down) of all or selected dial peers, use the **show dial-peer voice** command.

Examples

The following examples of output for the related **show dial-peer voice** command show the status of all or selected dial peers. You can use the **dial-peer outbound status-check pots**command to disallow the outbound POTS dial peers that are down.

The following example shows a short summary status for all dial peers. Outbound status is displayed in the OUT STAT field. POTS dial peers 31 and 42 are shown as down.

```
Router# show dial-peer voice summary
dial-peer hunt 0
              AD                                      PRE PASS                 OUT
TAG    TYPE  MIN  OPER PREFIX    DEST-PATTERN      FER THRU SESS-TARGET    STAT PORT
444    voip  up   up                                 0
22     voip  up   up                                 0  syst
12     pots  up   up             5550123 0                       up   4/0:15
311    voip  up   up                                 0  syst
31     pots  up   up             5550111             0                      down 4/1:15
421    voip  up   up             5550199 0  syst ipv4:1.8.56.2
42     pots  up   up                                 0                      down
```

The following example shows the status for dial peer 12. Outbound status is displayed in the Outbound state field. The dial peer is shown as up.

```
Router# show dial-peer voice 12
VoiceEncapPeer12
        peer type = voice, information type = voice,
        description = `',
        tag = 12, destination-pattern = `5550123',
        answer-address = `', preference=0,
        CLID Restriction = None
        CLID Network Number = `'
        CLID Second Number sent
        source carrier-id = `', target carrier-id = `',
        source trunk-group-label = `',  target trunk-group-label = `',
        numbering Type = `unknown'
        group = 12, Admin state is up, Operation state is up,
        Outbound state is up,                                  <------- display status
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        huntstop = disabled,
        in bound application associated: 'DEFAULT'
        out bound application associated: ''
        dnis-map =
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        Translation profile (Incoming):
  .
  .
  .
```

The following example shows the status for dial peer 31. Outbound status is displayed in the Outbound state field. The dial peer is listed as down.

```
Router# show dial-peer voice 31
VoiceEncapPeer31
        peer type = voice, information type = voice,
        description = `',
        tag = 31, destination-pattern = `5550111',
        answer-address = `', preference=0,
        CLID Restriction = None
        CLID Network Number = `'
        CLID Second Number sent
        source carrier-id = `', target carrier-id = `',
        source trunk-group-label = `',  target trunk-group-label = `',
        numbering Type = `unknown'
        group = 31, Admin state is up, Operation state is up,
        Outbound state is down,                          <--------- display status
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        huntstop = disabled,
        in bound application associated: 'DEFAULT'
        out bound application associated: ''
        dnis-map =
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        Translation profile (Incoming):
  .
  .
  .
```

For descriptions of other significant fields shown in these outputs, see the **show dial-peer voice** command.

Related Commands

Command	Description
show dial-peer voice	Displays information for voice dial peers.

dial-peer search type

To optimize voice or data dial-peer searches, use the **dial-peer search type** command in global configuration mode. To disable the search parameters, use the **no** form of this command.

dial-peer search type {**data voice** | **data voice** | **none**}
no dial-peer search type

Syntax Description

data	Searches for data dial peers.
none	Searches for all dial peers by order of input.
voice	Searches for voice dial peers.

Command Default

data and **voice**

Command Modes

Global configuration (confing)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.4(4)XC	This command was implemented on the Cisco 2600XM series, Cisco 2800 series, Cisco 3700 series, and Cisco 3800 series.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

The search defines the search preference explicitly. If the **data** and **voice** keywords are specified, data dial peers are searched first. If no data dial peers are found, the voice dial peers are searched.

Examples

The following is sample output that shows that data dial peers are searched first. Then voice dial peers are searched if no data dial peers can be matched for an incoming call:

```
dial-peer search type data voice
```

The following is sample output that shows that voice dial peers are searched first. Then data dial peers are searched if no voice dial peers can be matched for an incoming call:

```
dial-peer search type voice data
```

Related Commands

Command	Description
dial-peer data	Enable a gateway to process incoming data calls first by assigning the POTS dial peer as data.

dial-peer terminator

To change the character used as a terminator for variable-length dialed numbers, use the **dial-peer terminator** command in global configuration mode. To restore the default terminating character, use the **no** form of this command.

dial-peer terminator *character*
no dial-peer terminator

Syntax Description

character	Designates the terminating character for a variable-length dialed number. Valid numbers and characters are **#**, *****, **0**, **1**, **2**, **3**, **4**, **5**, **6**, **7**, **8**, **9**, **a**, **b**, **c**, and **d**. The default is **#**.

Command Default

The default terminating character is #.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0	This command was introduced.
12.0(7)XK	Usage was restricted to variable-length dialed numbers. The command was implemented on the Cisco 2600 series and Cisco 3600 series, and Cisco MC3810.
12.1(2)T	The command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

There are certain areas in the world (for example, in certain European countries) where telephone numbers can vary in length. When a dialed-number string has been identified as a variable length dialed number, the system does not place a call until the configured value for the **timeouts interdigit**command has expired or until the caller dials the terminating character. Use the **dial-peer terminator** global configuration command to change the terminating character.

Examples

The following example shows that "9" has been specified as the terminating character for variable-length dialed numbers:

```
dial-peer terminator 9
```

Related Commands

Command	Description
answer-address	Specifies the full E.164 telephone number to be used to identify the dial peer of an incoming call.
destination-pattern	Specifies the prefix or the complete telephone number for a dial peer.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.
show dial-peer voice	Displays configuration information for dial peers.

dial-peer video

To define a video ATM dial peer for a local or remote video codec, to specify video-related encapsulation, and to enter dial peer configuration mode, use the **dial-peer video** command in global configuration mode. To remove the video dial peer, use the **no** form of this command.

dial-peer video *tag* {**videocodec** | **videoatm**}
no dial-peer video *tag* {**videocodec** | **videoatm**}

Syntax Description

tag	Digits that define a particular dial peer. Defines the dial peer and assigns the protocol type to the peer. Range is from 1 to 10000. The tag must be unique on the router.
videocodec	Specifies a local video codec connected to the router.
videoatm	Specifies a remote video codec on the ATM network.

Command Default

No video dial peer is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)XK	This command was introduced for ATM interface configuration on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

The *tag* value must be unique to the device.

Examples

The following example sets up a local video dial peer designated as 10:

```
dial-peer video 10 videocodec
```

Related Commands

Command	Description
show dial-peer video	Displays dial-peer video configuration.

dial-peer voice

To define a particular dial peer, to specify the method of voice encapsulation, and to enter dial peer configuration mode, use the **dial-peer voice**command in global configuration mode. To delete a defined dial peer, use the **no** form of this command.

Cisco 1750 and Cisco 1751 Modular Access Routers
dial-peer voice *tag* {**pots** | **vofr** | **voip** **system**}
no dial-peer voice *tag* {**pots** | **vofr** | **voip** **system**}

Cisco 2600 Series, Cisco 2600XM, Cisco 3600 Series, Cisco 3700 Series, Cisco 7204VXR and Cisco 7206VXR
dial-peer voice *tag* {**pots** | **voatm** | **vofr** | **voip** **system**}
no dial-peer voice *tag* {**pots** | **voatm** | **vofr** | **voip** **system**}

Cisco 7200 Series
dial-peer voice *tag* **vofr**
no dial-peer voice *tag* **vofr**

Cisco AS5300
dial-peer voice *tag* {**mmoip** | **pots** | **vofr** | **voip** **system**}
no dial-peer voice *tag* {**mmoip** | **pots** | **vofr** | **voip** **system**}

Syntax Description

tag	Digits that define a particular dial peer. Range is from 1 to 2147483647.
pots	Indicates that this is a POTS peer that uses VoIP encapsulation on the IP backbone.
vofr	Specifies that this is a Voice over Frame Relay (VoFR) dial peer that uses FRF.11 encapsulation on the Frame Relay backbone network.
voip	Indicates that this is a VoIP peer that uses voice encapsulation on the POTS network.
system	Indicates that this is a system that uses VoIP.
voatm	Specifies that this is a Voice over ATM (VoATM) dial peer that uses real-time ATM adaptation layer 5 (AAL5) voice encapsulation on the ATM backbone network.
mmoip	Indicates that this is a multimedia mail peer that uses IP encapsulation on the IP backbone.

Command Default

No dial peer is defined. No method of voice encapsulation is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA	This command was implemented on the Cisco MC3810, with support for the **pots**, **voatm**, **vofr**, and **vohdlc** keywords.

Release	Modification
12.0(3)T	This command was implemented on the Cisco AS5300, with support for the **pots** and **voip** keywords.
12.0(3)XG	The **vofr** keyword was added for the Cisco 2600 series and Cisco 3600 series.
12.0(4)T	The **vofr** keyword was added for the Cisco 7200 series.
12.0(4)XJ	The **mmoip** keyword was added for the Cisco AS5300. The **dial-peer voice**command was implemented for store-and-forward fax.
12.0(7)XK	The **voip** keyword was added for the Cisco MC3810, and the **voatm** keyword was added for the Cisco 3600 series. Support for the **vohdlc** keyword on the Cisco MC3810 was removed.
12.1(1)	The **mmoip** keyword addition in Cisco IOS Release 12.0(4)XJ was integrated into Cisco IOS Release 12.1(1). The **dial-peer voice** implementation for store-and-forward fax was integrated into Cisco IOS Release 12.1(1).
12.1(2)T	The keyword changes in Cisco IOS Release 12.0(7)XK were integrated into Cisco IOS Release 12.1(2)T.
12.1(5)T	This command was implemented on the Cisco AS5300 and integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(2)XN	Support for enhanced Media Gateway Control Protocol (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(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2. This command was implemented on the Cisco IAD2420 series.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented on the Cisco 2600XM, Cisco ICS7750, and Cisco VG200.
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 **dial-peer voice** global configuration command to switch to dial peer configuration mode from global configuration mode and to define a particular dial peer. Use the **exit**command to exit dial peer configuration mode and return to global configuration mode.

A newly created dial peer remains defined and active until you delete it with the **no** form of the **dial-peer voice** command. To disable a dial peer, use the **no shutdown** command in dial peer configuration mode.

In store-and-forward fax on the Cisco AS5300, the POTS dial peer defines the inbound faxing line characteristics from the sending fax device to the receiving Cisco AS5300 and the outbound line characteristics from the sending Cisco AS5300 to the receiving fax device. The Multimedia Mail over Internet Protocol (MMoIP) dial peer defines the inbound faxing line characteristics from the Cisco AS5300 to the receiving Simple Mail Transfer Protocol (SMTP) mail server. This command works with both on-ramp and off-ramp store-and-forward fax functions.

Note On the Cisco AS5300, MMoIP is available only if you have modem ISDN channel aggregation (MICA) technologies modems.

Examples

The following example shows how to access dial peer configuration mode and configure a POTS peer identified as dial peer 10 and an MMoIP dial peer identified as dial peer 20:

```
dial-peer voice 10 pots
dial-peer voice 20 mmoip
```

The following example deletes the MMoIP peer identified as dial peer 20:

```
no dial-peer voice 20 mmoip
```

The following example shows how the **dial-peer voice** command is used to configure the extended echo canceller. In this instance, **pots** indicates that this is a POTS peer using VoIP encapsulation on the IP backbone, and it uses the unique numeric identifier tag 133001.

```
Router(config)# dial-peer voice 133001 pots
```

Related Commands

Command	Description
codec (dial-peer)	Specifies the voice coder rate of speech for a VoFR dial peer.
destination-pattern	Specifies the prefix, the full E.164 telephone number, or an ISDN directory number to be used for a dial peer.
dtmf-relay (Voice over Frame Relay)	Enables the generation of FRF.11 Annex A frames for a dial peer.
preference	Indicates the preferred order of a dial peer within a rotary hunt group.
sequence-numbers	Enables the generation of sequence numbers in each frame generated by the DSP for VoFR applications.
session protocol	Establishes a session protocol for calls between the local and remote routers via the packet network.
session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
shutdown	Changes the administrative state of the selected dial peer from up to down.

dial-type

To specify the type of out-dialing for voice port interfaces, use the **dial-type** command in voice-port configuration mode. To disable the selected type of dialing, use the **no** form of this command.

dial-type {**dtmf** | **pulse** | **mf**}
no dial-type

Syntax Description

dtmf	Dual tone multifrequency (DTMF) touch-tone dialing.
pulse	Pulse (rotary) dialing.
mf	Multifrequency tone dialing.

Command Default

DTMF touch-tone dialing

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA3	This command was implemented on the Cisco MC3810, and the **pulse**keyword was added.
12.0(7)XK	The **mf** keyword was added.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(5)XM	This command was extended to the merged SGCP/MGCP software image.
12.2(2)T	This command was implemented on the Cisco 7200 series and integrated into Cisco IOS Release 12.2(2)T.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

Use the **dial-type** command to specify an out-dialing type for a Foreign Exchange Office (FXO) or E&M voice port interface. This command specifies the tone type for digit detection and out-pulsing. This command is not applicable to Foreign Exchange Station (FXS) voice ports because the ports do not generate out-dialing. This command also specifies the detection direction. Multifrequency tone dialing is not supported for FXS and FXO.

Voice ports can always detect DTMF and pulse signals. This command does not affect voice port dialing detection.

The **dial - type** command affects out-dialing as configured for the dial peer.

If you are using the **dial-type** command with E&M wink-start signaling, use the **dtmf** or **mf** option.

SGCP 1.1+ does not support pulse dialing.

Examples

The following example shows a voice port configured to support a rotary (pulse tone) dialer:

```
Router(config)# voice-port 1/1
Router(config-voice-port)# dial-type pulse
```

The following example shows a voice port configured to support a DTMF (touch-tone) dialer:

```
Router(config)# voice-port 1/1
Router(config-voice-port)# dial-type dtmf
```

The following example shows a voice port configured to support a multifrequency tone dialer:

```
Router(config)# voice-port 1/1
Router(config-voice-port)# dial-type mf
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.

dialer extsig

To configure an interface to initiate and terminate calls using an external signaling protocol, use the **dialer extsig** command in interface configuration mode. To discontinue control of the interface by the external signaling protocol, use the **no** form of this command.

dialer extsig
no dialer extsig

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

This command is used with the Network Access Server Package for Media Gateway Control Protocol feature. Configuring the **dialer in-band**command is a prerequisite to using this command. The configuration is blocked for profile dialers.

Examples

The following example shows an interface to initiate and terminate calls using an external signaling protocol being configured:

```
Router(config)# interface Dialer1
Router(config-if)# dialer extsig
```

Related Commands

Command	Description
debug dialer	Provides debugging information for two types of dialer information: dial-on-demand events and dial-on-demand traffic.
dialer in-band	Specifies that DDR is to be supported.
extsig mgcp	Configures external signaling control by MGCP for a T1 or E1 trunk controller card.
show dialer	Displays dialer-related information for DNIS, interface, maps, and sessions.

dialer preemption level

To set the precedence for voice calls to be preempted by a dial-on demand routing (DDR) call for the dialer map, use the **dialer preemption level** command in map-class dialer configuration mode. To remove the preemption setting, use the **no** form of this command.

dialer preemption level {**flash-override** | **flash** | **immediate** | **priority** | **routine**}
no dialer preemption level {**flash-override** | **flash** | **immediate** | **priority** | **routine**}

Syntax Description

flash-override	Sets the precedence for DDR calls to preemption level 0 (highest).
flash	Sets the precedence for DDR calls to preemption level 1.
immediate	Sets the precedence for DDR calls to preemption level 2.
priority	Sets the precedence for DDR calls to preemption level 3.
routine	Sets the precedence for DDR calls to preemption level 4 (lowest). This is the default.

Command Default

The preemption level default is **routine** (lowest).

Command Modes

Map-class dialer configuration (config-map-class)

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Examples

The following example sets a preemption level of *priority* (level 3) for the dialer map-class *dial1*.

```
Router(config)# map-class dialer dial1
Router(config-map-class)# dialer preemption level priority
```

Related Commands

Command	Description
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
dialer trunkgroup	Defines the dial-on-demand trunk group label for the dialer interface.
map-class dialer	Defines a class of shared configuration parameters associated with the **dialer map** command for outgoing calls from an ISDN interface and for PPP callback.
preemption enable	Enables preemption capabilities on a trunk group.
preemption level	Sets the preemption level of the selected outbound dial peer. Voice calls can be preempted by a DDR call with higher preemption level.

preemption tone timer	Defines the expiry time for the preemption tone for the outgoing call being preempted by a DDR backup call.

dialer trunkgroup

To define the dial-on-demand trunk group label for the dialer interface, use the **dialer trunkgroup**command in map-class dialer configuration mode. To remove the trunk group label, use the **no** form of this command.

dialer trunkgroup *label*
no dialer trunkgroup *label*

Syntax Description

label	Unique name for the dialer interface trunk group. Valid names contain a maximum of 63 alphanumeric characters.

Command Default

No dialer trunk group is defined.

Command Modes

Map-class dialer configuration (config-map-class)

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Examples

The following example creates a trunk group named 20 for dialer map-class *dial1*.

```
Router(config)# map-class dialer dial1
Router(config-map-class)# dialer trunkgroup 20
```

Related Commands

Command	Description
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
map-class dialer	Defines a class of shared configuration parameters associated with the **dialer map** command for outgoing calls from an ISDN interface and for PPP callback.
show dialer	Displays general diagnostic information for interfaces configured for dial-on-demand routing (DDR).
trunk group	Defines a trunk group (global configuration) and enters trunk group configuration mode.

digit

To designate the number of digits for SCCP telephony control (STC) application feature speed-dial codes, use the **digit** command in STC application feature speed-dial configuration mode. To reset to the default, use the **no** form of this command.

digit *number*
no digit

Syntax Description

number	Number of digits for speed-dial codes. Values are 1 or 2. Default is 1.

Command Default

The default number of digits is 1.

Command Modes

STC application feature speed-dial configuration (stcapp-fsd

Command History

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

Usage Guidelines

This command is used with the STC application, which enables features on analog FXS endpoints that use Skinny Client Control Protocol (SCCP) for call control.

This command determines the number of digits that can be configured for speed-dial codes using the **speed dial** and **voicemail** commands. Use this command only if you want to change the number of digits from its default, which is 1. If you modify the value of this command, the **speed dial** and **voicemail** commands are reset to their defaults. If you set the value to 2 and then try to configure a single-digit speed-dial code, the system converts the speed-dial code into two digits.

Note that the phone numbers that are stored with various speed-dial codes are configured on the call-control device, such as Cisco CallManager or a Cisco CallManager Express router.

Examples

The following example sets the number of digits for speed-dial codes to two. It also sets a speed-dial prefix of one pound sign (#) and a speed-dial code range from 5 to 25. After these values are configured, a phone user presses #10 on the keypad to dial the number that was stored with code 10.

```
Router(config)# stcapp feature speed-dial
Router(stcapp-fsd)# prefix #
Router(stcapp-fsd)# digit 2
Router(stcapp-fsd)# speed dial from 5 to 25
```

Related Commands

Command	Description
prefix (stcapp-fsd)	Designates a prefix to precede the dialing of an STC application feature speed-dial code.
show stcapp feature codes	Displays configured and default STC application feature access codes.
speed dial	Designates a range of STC application feature speed dial codes.

Command	Description
voicemail	Designates an STC application feature speed-dial code to dial the voice-mail number.

digit-strip

To enable digit stripping on a POTS dial-peer call leg, use the **digit - strip command in**dial peer configuration mode. To disable digit stripping on the dial-peer call leg, use the **no** form of this command.

digit-strip
no digit-strip

Syntax Description

This command has no arguments or keywords.

Command Default

Digit stripping is enabled.

Command Modes

Dial peer configuration (config-dial-peer)

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 supported for the following voice technologies on the following platforms: • VoIP--(Cisco 2600 series, Cisco 3600 series, Cisco MC3810) • Voice over Frame Relay (VoFR)--Cisco 2600 series, Cisco 3600 series, Cisco MC3810 • Voice over ATM (VoATM)--Cisco 3600 series and Cisco MC3810
12.1(1)T	This command was integrated in Cisco IOS Release 12.1(1)T.
12.1(2)T	This command was integrated into 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, Cisco MC3810)

Usage Guidelines

The **digit-strip** command is supported on POTS dial peers only.

When a called number is received and matched to a POTS dial peer, the matched digits are stripped and the remaining digits are forwarded to the voice interface.

The table below lists a series of dial peers configured with a specific destination pattern and shows the longest matched number after the digit is stripped based on the dial string 408 555-0148.

Table 6: Dial-Peer Configurations with Longest Matched Number

Dial Peer	Destination Pattern	Preference	Session Target	Longest Matched Number
	4085550148	0 (highest)	100-voip	10
	408[0-9]550148	0	200-voip	9

Dial Peer	Destination Pattern	Preference	Session Target	Longest Matched Number
	408555	0	300-voip	6
	408555	1(lower)	400-voip	6
	408%	1	500-voip	3
	.....	0	600-voip	0
	.....	1	1:D (interface)	0

The table below lists a series of dial peers configured with a specific destination pattern and shows the number after the digit strip based on the dial string 408 555-0148 and the different dial-peer symbols applied.

Table 7: Dial-Peer Configurations with Digits Stripped

Dial Peer	Destination Pattern	Number After the Digit Strip
1	408555....	0148
2	408555.%	0148
3	408525.+	0148
4	408555.?	0148
5	408555+	0148
6	408555%	50148
7	408555?	50148
8	408555[0-9].%	30148
9	408555(30).%	30148
10	408555(30)%	30148
11	408555..48	30148

Examples

The following example disables digit stripping on a POTS dial peer:

```
dial-peer voice 100 pots
 no digit-strip
```

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.

Command	Description
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.
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.

digital-filter

To specify the digital filter to be used before the voice packet is sent from the digital signal processor (DSP) to the network, use the **digital-filter** command in voice-class configuration mode. To remove the digital filter, use the **no** form of this command.

digital-filter {**1950hz** | **2175hz**}
no digital-filter {**1950hz** | **2175hz**}

Syntax Description

1950hz	Filter out 1950 Hz frequency.
2175hz	Filter out 2175 Hz frequency.

Command Default

Digital filtering is disabled.

Command Modes

Voice-class configuration (config-voice-class)

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 **digital-filter** 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). The digital filter improves voice quality by preventing transmission of the guard tone with the voice packet from the LMR system to the VoIP network. The guard tone is configured with the **inject guard-tone**command. The digital filter can be configured to filter out either 2175 Hz or 1950 Hz. Only one of these frequencies can be filtered out at a time. Filtering is performed by the DSP.

Examples

The following example specifies that 1950 Hz guard tone be filtered out of the voice packet before it is sent from the DSP to the network:

```
voice class tone-signal mytones
 digital-filter 1950hz
```

Related Commands

Command	Description
inject guard-tone	Plays out a guard tone with the voice packet.

direct-inward-dial

To enable the direct inward dialing (DID) call treatment for an incoming called number, use the **direct-inward-dial** command in dial peer configuration mode. To disable DID on the dial peer, use the **no** form of this command.

direct-inward-dial
no direct-inward-dial

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)NA	This command was introduced.
12.0(4)T	This command was modified for store-and-forward fax.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Use the **direct-inward-dial** command to enable the DID call treatment for an incoming called number. When this feature is enabled, the incoming call is treated as if the digits were received from the DID trunk. The called number is used to select the outgoing dial peer. No dial tone is presented to the caller.

Use the no form of this command to disable DID on the dial peer. When the command is disabled, the called number is used to select the outgoing dial peer. The caller is prompted for a called number via dial tone.

This command is applicable only to plain old telephone service (POTS) dial peers for on-ramp store-and-forward fax functions.

Examples

The following example enables DID call treatment for the incoming called number:

```
dial-peer voice 10 pots
 direct-inward-dial
```



disable-early-media through dualtone

- disable-early-media 180, on page 74
- disable service-settings, on page 76
- disc_pi_off, on page 77
- disconnect-ack, on page 78
- dnis (DNIS group), on page 79
- dnis-map, on page 81
- dns-a-override, on page 83
- domain-name (annex G), on page 84
- drop-last-conferee, on page 85
- ds0 busyout (voice), on page 87
- ds0-group (E1), on page 89
- ds0-group (T1), on page 95
- ds0-num, on page 102
- dscp media, on page 103
- dscp-profile, on page 107
- dsn, on page 108
- dsp allocation signaling dspid, on page 111
- dsp services dspfarm, on page 112
- dspfarm (DSP farm), on page 114
- dspfarm (voice-card), on page 116
- dspfarm confbridge maximum, on page 118
- dspfarm connection interval, on page 120
- dspfarm profile, on page 121
- dspfarm rtp timeout, on page 125
- dspfarm transcoder maximum sessions, on page 126
- dspint dspfarm, on page 128
- dtmf-interworking, on page 130
- dtmf timer inter-digit, on page 132
- dtmf-relay (Voice over Frame Relay), on page 133
- dtmf-relay (Voice over IP), on page 135
- dualtone, on page 139

disable-early-media 180

To specify which call treatment, early media or local ringback, is provided for 180 responses with 180 responses with Session Description Protocol (SDP), use the **disable-early-media 180** command in sip-ua configuration mode or voice class tenant configuration mode. To enable early media cut-through for 180 messages with SDP, use the **no** form of this command.

disable-early-media 180 system
no disable-early-media 180

Syntax Description

system	Specifies that the disable-early-media method 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

Early media cut-through for 180 responses with SDP is enabled.

Command Modes

SIP UA configuration (config-sip-ua)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.2(13)T	This command was introduced.
IOS Release XE 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

This command provides the ability to enable or disable early media cut-through on Cisco IOS gateways for SIP 180 responses with SDP. Use the **disable-early-media 180** command to configure the gateway to ignore the SDP message and provide local ringback. To restore the default treatment, early media cut-through, use the **no disable-early-media 180** command.

Examples

The following example disables early media cut-through for SIP 180 responses with SDP:

```
Router(config-sip-ua)# disable-early-media 180
```

The following example shows how to disable early media cut-through for SIP 180 responses in the voice class tenant configuration mode:

```
Router(config-class)# disable-early-media 180 system
```

Related Commands

Command	Description
show sip-ua retry	Displays SIP retry statistics.
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.

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

disable service-settings

To disable the service settings configured on a Cisco Unified Communications Manager (CUCM), use the **disable service-settings** command in phone proxy configuration mode. To enable the service settings configured on a CUCM, use the **no** form of the command.

disable service-settings
no disable service-settings

Syntax Description

This command has no arguments or keywords.

Command Default

The service settings on a CUCM are enabled.

Command Modes

Phone proxy configuration mode (config-phone-proxy)

Command History

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

Usage Guidelines

The **disable service-setting** command disables the service settings configured on a CUCM. PC Port, Gratuitous ARP, Voice VLAN access, Web access, and Span to PC Port are the services enabled by default on a CUCM.

Example

```
Device(config)# voice-phone-proxy first-pp
Device(config-phone-proxy)# disable service-settings
```

disc_pi_off

To enable an H.323 gateway to disconnect a call when it receives a disconnect message with a progress indicator (PI) value, use the **disc_pi_off** command in voice-port configuration mode. To restore the default state, use the **no**form of this command.

disc_pi_off
no disc_pi_off

Syntax Description

This command has no arguments or keywords.

Command Default

The gateway does not disconnect a call when it receives a disconnect message with a PI value.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(5)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco 7500 series, Cisco AS5300, Cisco AS5800, and Cisco MC3810.
12.2(2)XA	This command was implemented on the Cisco AS5400 and Cisco AS5350.
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

The **disc_pi_off** voice-port command is valid only if the disconnect with PI is received on the inbound call leg. For example, if this command is enabled on the voice port of the originating gateway, and a disconnect message with PI is received from the terminating switch, the disconnect message is converted to a disconnect message. But if this command is enabled on the voice port of the terminating gateway, and a disconnect message with PI is received from the terminating switch, the disconnect message is not converted to a standard disconnect message because the disconnect message is received on the outbound call leg.



Note The **disc_pi_off** voice-port configuration command is valid only for the default session application; it does not work for interactive voice response (IVR) applications.

Examples

The following example handles a disconnect message with a PI value in the same way as a standard disconnect message for voice port 0:23:

```
voice-port 0:D
 disc_pi_off
```

Related Commands

Command	Description
isdn t306	Sets a timer for disconnect messages.

disconnect-ack

To configure a Foreign Exchange Station (FXS) voice port to return an acknowledgment upon receipt of a disconnect signal, use the **disconnect-ack** command in voice-port configuration mode. To disable the acknowledgment, use the **no** form of this command.

disconnect-ack
no disconnect-ack

Syntax Description

This command has no arguments or keywords.

Command Default

FXS voice ports return an acknowledgment upon receipt of a disconnect signal

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the 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 **disconnect-ack** command configures an FXS voice port to remove line power if the equipment on an FXS loop-start trunk disconnects first.

Examples

The following example, which begins in global configuration mode, disables the disconnect acknowledgment signal on voice port 1/1/0:

```
voice-port 1/0/0
 no disconnect-ack
```

Command History

Command	Description
show voice port	Displays voice port configuration information.

dnis (DNIS group)

To add a dialed number identification service (DNIS) number to a DNIS map, use the **dnis** command in DNIS-map configuration mode. To delete a DNIS number, use the **no** form of this command.

dnis *telephone-umber* [**url** *url*]
no dnis

Syntax Description

telephone-umber	Adds a user-selected DNIS number to a DNIS map.
url *url*	(Optional) URL that links a DNIS number to a specific VoiceXML document. If a URL is not entered, the DNIS number is linked to the VoiceXML application in the dial peer, which must be configured using the **application** command. This keyword is not valid for Tool Command Language (TCL) applications.

Command Default

If no URL is entered, the DNIS number links to the VoiceXML application that is configured in the dial peer with the **application** command.

Command Modes

DNIS-map configuration

Command History

Release	Modification
Cisco IOS XE 26.2.1	This command was modified to display warning message for insecure protocol usage.
12.2(11)T	This command was implemented on the Cisco 3640 and Cisco 3660.
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

To enter DNIS-map configuration mode for the **dnis** command, use the **voice dnis-map** command.

Enter the **dnis** command once for each telephone number that you want to map to a voice application. A separate entry must be made for each telephone number in a DNIS map. Wildcards are not supported.

URLs in DNIS entries are used only by VoiceXML applications. When an incoming called number matches a DNIS entry, it loads the VoiceXML document that is specified by the URL, provided that a VoiceXML application is configured in the dial peer with the **application** command configured.

Non-VoiceXML applications, such as TCL applications, ignore the URLs in DNIS maps and link a call to the TCL application that is configured in the dial peer using the **application** command.

For a DNIS map to be applied to an outbound dial peer, a VoiceXML application must be configured with the **application out-bound** command. Otherwise, the call is not handed off to the application that is specified in the URL of the DNIS map.

The number of allowable DNIS entries is limited by the amount of available configuration memory on the gateway. As a general rule, DNIS maps that contain more than several hundred DNIS entries should be maintained in an external text file.

To associate a DNIS map with a dial peer, use the **dnis-map** command.

Warning Starting with Cisco IOS XE 26.2.1, a warning message is displayed when insecure protocols such as HTTP, FTP, or TFTP are used, as they do not provide encryption or authentication. Use secure alternatives such as HTTPS, SFTP, or SCP instead.

Examples

The first line in the following example shows how the **voice dnis-map** command is used to create a DNIS map named dmap1. The last two lines show how the dnis command is used to enter DNIS entries.

The first DNIS entry specifies the location of a VoiceXML document. The second DNIS entry does not specify a URL. A DNIS number without a URL is, by default, matched to the URL of the application that is configured in the dial peer by the configured application command.

```
voice dnis-map dmap1
 dnis 5550105 url tftp://blue/sky/test.vxml
 dnis 5550188
```

The following example shows the warning message displayed for the usage of insecure HTTP protocol:

```
Device(config)#voice dnis-map dmapname
Device(config-dnis-map)#dnis 123456 url tftp://blue/sky/test.vxml
SECURITY WARNING - Module: VOICE_DNISMAPS, Command: dnis 123456 url tftp://blue/sky/test.vxml,

Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of
encryption and authentication,
Description: voice dnis maps configured with FTP/HTTP/TFTP URL protocol,
Remediation: Use secure protocols such as HTTPS, SFTP, or SCP instead of insecure HTTP,
FTP, or TFTP
Device(config-dnis-map)#
```

Related Commands

Command	Description
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 dnis -map load	Reloads a DNIS map that has changed since the previous load.

dnis-map

To associate a dialed number identification service (DNIS) map with a dial peer, use the **dnis-map** command in dial peer configuration mode. To remove a DNIS map from the dial peer, use the **no** form of this command.

dnis-map *map-name*
no dnis-map

Syntax Description

map -name	Name of the configured DNIS map.

Command Default

No default behavior or values

Command Modes

Dial peer 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 implemented on the Cisco 3640 and Cisco 3660.

Usage Guidelines

A DNIS map is a table of destination numbers with optional URLs that link to specific VoiceXML documents. When configured in a dial peer, a DNIS map enables you to link multiple called numbers to a single Tool Command Language (TCL) application or to individual VoiceXML documents.

The **dnis-map**command must be used with the **application** command.

Only one DNIS map can be configured in each dial peer.

To create a DNIS map, use the **voice dnis-map** command to enter DNIS-map configuration mode, and then use the **dnis** command to add entries to the DNIS map. Or you can create an external text file of DNIS entries and link to its URL by using the **voice dnis-map** command.

To display the configuration information for DNIS maps, use the **show voice dnis-map** command.

A URL configured for a DNIS number is ignored by a TCL application; the TCL script that is configured for the application is used instead.



Note For a DNIS map to be applied to an outbound dial peer, the call application must be configured as an outbound application. That is, a VoiceXML application must be configured by with the **application out-bound** command. Otherwise, the call is not handed off to the application that is specified in the URL of the DNIS map.

Examples

In the following example the DNIS map named "dmap1" is associated with the VoIP dial peer 3. The outbound application "vapptest1" is associated through this dial peer with DNIS map "dmap1."

```
dial-peer voice 3 voip
 dnis-map dmap1
 application vapptest1 outbound
```

Related Commands

Command	Description
dnis	Adds a DNIS number to a DNIS map.
show voice dnis -map	Displays configuration information about DNIS maps.
voice dnis -map	Enters DNIS-map configuration mode to create a DNIS map.
voice dnis -map load	Reloads a DNIS map that has changed since the previous load.

dns-a-override

To skip querying Domain Name System (DNS) IPv4 and IPv6 address records (A and AAAA) if a service record (SRV) query times out, use the **dns-a-override** command in voice service SIP configuration mode or voice class tenant configuration mode. To disable this functionality, use the **no** form of this command.

dns-a-override system
no dns-a-override

Command Default

If an SRV query times out, DNS IPv4 and IPv6 records are queried.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

Command History

Release	Modification
15.3(1)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.

Usage Guidelines

Use the**dns-a-override** command if you do not want the Cisco Unified Border Element (Cisco UBE) to query the A and AAAA records on the DNS server when the SRV query times out.

Example

The following example shows how to skip querying the DNS A and AAAA records when an SRV query times out:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# dns-a-override
```

The following example shows how to skip querying in the voice class tenant configuration mode:

```
Router(config-class)# dns-a-override system
```

domain-name (annex G)

To set the domain name that is reported in service relationships, use the **domain name**command in annex G neighbor configuration mode. To remove the domain name, use the **no** form of this command.

domain-name *id*
no domain-name *id*

Syntax Description

id	Domain name that is reported in service relationships.

Command Default

No default behavior or values

Command Modes

Annex G neighbor configuration mode

Command History

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

Usage Guidelines

Use this command to set the domain name that is reported in service relationships.

Examples

The following example shows how to set a domain name to "boston1":

```
Router(config-annexg-neigh)# domain-name sample1
```

Related Commands

Command	Description
access -policy	Requires that a neighbor be explicitly configured.

drop-last-conferee

To define a Feature Access Code (FAC) to access the Drop Last Conferee feature in feature mode on analog phones controlled by Cisco Unified Communications Manager Express (CME), use the **drop-last-conferee** command in STC application feature-mode call-control configuration mode. To return the code to its default, use the **no** form of this command.

drop-last-conferee *keypad-character*
no drop-last-conferee

Syntax Description

keypad-character	Character string of one to four characters that can be dialed on a telephone keypad (0-9, *, #). Default is #4.

Command Default

The default value is #4.

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 the Drop Last Conferee feature from the default (#4) 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.

Note This command does not change the user experience for Drop Last Conferee if the Cisco call-control system is Cisco Unified Communications Manager.

Examples

The following example shows how to change the value of the feature code for the Drop Last Conferee feature from the default (#4). With this configuration, a phone user in a three-party conference on an analog phone controlled by Cisco Unified CME presses hook flash to get the feature tone and then dials 44 to drop the last active party. The conference becomes a basic call to the second call party.

```
Router(config)# stcapp call-control mode feature
Router(config-stcapp-fmcode)# drop-last-conferee 44
Router(config-stcapp-fmcode)# exit
```

Related Commands

Command	Description
conference	Defines FAC in Feature Mode to initiate 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.
transfer	Defines FAC in feature mode to connect a call to a third party that the phone user dials.

ds0 busyout (voice)

To force a DS0 time slot on a controller into the busyout state, use the **ds0 busyout** command in controller configuration mode. To remove the DS0 time slot from the busyout state, use the **no** form of this command.

ds0 busyout *ds0-time-slot*
no ds0 busyout *ds0-time-slot*

Syntax Description

ds0 -time-slot	DS0 time slots to be forced into the busyout state. Range is from 1 to 24 and can include any combination of time slots.

Command Default

DS0 time slots are not in the busyout state.

Command Modes

Controller configuration

Command History

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

Usage Guidelines

The **ds0 busyout**command affects only DS0 time slots that are configured into a DS0 group and that function as part of a digital voice port. If multiple DS0 groups are configured on a controller, any combination of DS0 time slots can be busied out, provided that each DS0 time slot to be busied out is part of a DS0 group.

If a DS0 time slot is in the busyout state, only the **no ds0 busyout** command can restore the DS0 time slot to service.

To avoid conflicting interaction of command-line interface (CLI) commands, do not use the **ds0 busyout** command and the **busyout forced** command on the same controller.

Examples

The following example configures DS0 time slot 6 on controller T1 0 to be forced into the busyout state:

```
controller t1 0
 ds0 busyout 6
```

The following example configures DS0 time slots 1, 3, 4, 5, 6, and 24 on controller E1 1 to be forced into the busyout state:

```
controller e1 1
 ds0 busyout 1,3-6,24
```

Related Commands

Command	Description
busyout seize	Changes the busyout seize procedure for a voice port.

Command	Description
show running configuration	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or virtual circuit (VC) class.

ds0-group (E1)

To specify the DS0 time slots that make up a logical voice port on an E1 controller, specify the signaling type by which the router communicates with the PBX or PSTN, and define E1 channels for compressed voice calls and the channel-associated signaling (CAS) method by which the router connects to the PBX or PSTN, use the **ds0-group** command in controller configuration mode. To remove the group and signaling setting, use the **no** form of this command.

Cisco IOS Release 12.2 and Later Releases-Cisco 1750 and Cisco 1751
ds0-group *ds0-group-number* **timeslots** *timeslot-list* {**service** *service-type* | [**type e&m-fgb** | **e&m-fgd** | **e&m-immediate-start** | **fgd-eana** | **fgd-os** | **fxs-ground-start** | **fxs-loop-start** | **none** | **r1-itu** | **r1-modified** | **r1-turkey**]}
no ds0-group *ds0-group-number*

Cisco IOS Release 12.1 and Earlier Releases- Cisco 1750 and Cisco 1751
ds0-group *ds0-group-number* **timeslots** *timeslot-list* {[**service** *service-type*] | [**type e&m-fgb** | **e&m-fgd** | **em-immediate-start** | **fgd-eana** | **fgd-os** | **fxs-ground-start** | **fxs-loop-start** | **none** | **r1-itu** | **r1-modified** | **r1-turkey** | **sas-ground-start** | **sas-loop-start**]}
no ds0-group *ds0-group-number*

Cisco 2600 Series (Except Cisco 2691), Cisco 3600 Series (Except Cisco 3660)
ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type** {**e&m-delay-dial** | **&em-immediate-start** | **e&m-melcas-delay** | **e&m-melcas-immed** | **e&m-melcas-wink** | **e&m-wink-start** | **ext-sig** | **fgd-eana** | **fxo-ground-start** | **fxo-loop-start** | **fxo-melcas** | **fxs-ground-start** | **fxs-loop-start** | **fxs-melcas** | **r2-analog** | **r2-digital** | **r2-pulse**}
no ds0-group *ds0-group-number*

Cisco 2691, Cisco 2600XM Series, Cisco 2800 Series (Except Cisco 2801), Cisco 3660, Cisco 3700 Series, Cisco 3800 Series
ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type** {**e&m-delay-dial** | **e&m-immediate-start** | **e&m-lmr** | **e&m-melcas-delay** | **e&m-melcas-immed** | **e&m-melcas-wink** | **e&m-wink-start** | **ext-sig** | **fgd-eana** | **fxo-ground-start** | **fxo-loop-start** | **fxo-melcas** | **fxs-ground-start** | **fxs-loop-start** | **fxs-melcas** | **r2-analog** | **r2-digital** | **r2-pulse**}
no ds0-group *ds0-group-number*

Cisco 7200 Series and Cisco 7500 Series Voice Ports
ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type** {**e&m-delay-dial** | **e&m-fgd** | **e&m-immediate-start** | **e&m-wink-start** | **fxo-ground-start** | **fxo-loop-start** | **fxs-ground-start** | **fxs-loop-start**}
no ds0-group *ds0-group-number*

Cisco 7700 Series Voice Ports
ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type** {**e&m-delay-dial** | **e&m-immediate-start** | **e&m-wink-start** | **fxs-ground-start** | **fxs-loop-start** | **fxo-ground-start** | **fxo-loop-start**}
no ds0-group *ds0-group-number*

Cisco AS5300 and Cisco AS5400
ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type** {**none** | **p7** | **r2-analog** | **r2-digital** | **r2-lsv181-digital** | **r2-pulse**}

no ds0-group *ds0-group-number*

Syntax Description

ds0 -group-number	A value that identifies the DS0 group. Range is from 0 to 14 and 16 to 30; 15 is reserved.
timeslots *timeslot -list*	Lists time slots in the DS0 group. The *timeslot-list* argument is a single time-slot number, a single range of numbers, or multiple ranges of numbers separated by commas. Range is from 1 through 31. Examples are as follows: • 2 • 1-15,17-24 • 1-23 • 2,4,6-12
type	Specifies the type of signaling for the DS0 group. The signaling method selection for the type keyword depends on the connection that you are making. The ear and mouth (E&M) interface allows connection for PBX trunk lines (tie lines) and telephone equipment. The Foreign Exchange Station (FXS) interface allows connection of basic telephone equipment and a PBX. The Foreign Exchange Office (FXO) interface is for connecting the central office (CO) to a standard PBX interface where permitted by local regulations; it is often used for off-premise extensions (OPXs). Types are as follows: • **e&m -delay-dial**--The originating endpoint sends an off-hook signal and then waits for an off-hook signal followed by an on-hook signal from the destination. • e&m-fgb--E&M Type II Feature Group B. • e&m-fgd--E&M Type II Feature Group D. • **e&m -immediate-start**--E&M immediate start. • **e&m-lmr** --E&M Land Mobile Radio (LMR). • **e&m -melcas-delay**--E&M MELCAS delay-start signaling support. • **e&m -melcas-immed**--E&M MELCAS immediate-start signaling support.

	• **e&m -melcas-wink**--E&M MELCAS wink-start signaling support. • **e&m -wink-start**--The originating endpoint sends an off-hook signal and waits for a wink-start from the destination. • **fgd -eana--Feature Group D exchange access North American.** • fgd-os--Feature Group D operator services. • **fxo -ground-start--FXO ground-start signaling.** • **fxo -loop-start--FXO loop-start signaling.** • **fxo -melcas--FXO MELCAS signaling.** • **fxs -ground-start--FXS ground-start signaling.** • **fxs -loop-start--FXS loop-start signaling.** • **fxs -melcas--FXS MELCAS signaling.** • **none** --Null signaling for external call control. • p7--Specifies the p7 switch type. • r1-itu--Line signaling based on international signaling standards. • r1-modified--An international signaling standard that is common to channelized T1/E1 networks. • **r1 -turkey**--A signaling standard used in Turkey. • **r2 -analog--R2 analog line signaling.** • **r2 -digital--R2 digital line signaling.** • r2-lsv181-digital--Specifies a specific R2 digital line. • **r2 -pulse--7-pulse line signaling, a transmitted pulse that indicates a change in the line state.** • **sas-ground-start --Single attachment station (SAS) ground-start.** • **sas-loop-start --SAS loop-start.**
service *service -type*	(Optional) Specifies the type of service • **data** --data service • **fax** -- store-and-forward fax service • **voice** --voice service (for FGD-OS service) • **mgcp** --Media Gateway Control Protocol (MGCP) service

Command Default

There is no DS0 group. Calls are allowed in both directions.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
11.2	This command was introduced for the Cisco AS5300 as the **cas-group** command.
11.3(1)MA	The command was introduced as the voice-group command for the Cisco MC3810.
12.0(1)T	This command was integrated into Cisco IOS Release 12.0(1)T, and the cas-group command was implemented on the Cisco 3600 series routers.
12.0(5)T	The command was renamed ds0-group on the Cisco AS5300 and Cisco 2600 series and Cisco 3600 series routers. Some keyword modifications were implemented.
12.0(5)XE	This command was implemented on the Cisco 7200 series.
12.0(7)XK	Support for this command was implemented on the Cisco MC3810. When the ds0-group command became available on the Cisco MC3810, the voice-group command was removed and no longer supported.
12.0(7)XR	The mgcp service type was added.
12.1(2)XH	The e&m-fgd and fgd-eana keywords were added for Feature Group D signaling.
12.1(5)XM	The **sgcp** keyword was removed.
12.1(3)T	This command was modified for Cisco 7500 series routers. The fgd-os signaling type and the voice service type were added.
12.2	The command was modified to exclude sas keywords. The Single Attachment Station (SAS) CAS options of sas-loop-start and sas-ground-start are not supported as a type of signaling for the DS0 group.
12.2(2)XA	This command was implemented on the Cisco AS5300.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
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(4)XM	This command was implemented on Cisco 1750 and Cisco 1751 routers. Support for other Cisco platforms is not included in this release.
12.2(2)XN	Support for the **mgcp** keyword was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
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.
12.2(11)T	This command was supported with Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2. This command is supported on the Cisco IAD2420 series, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5850 in this release.

Release	Modification
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. The Cisco 1750 and Cisco 1751 do not support T1 and E1 voice and data cards in Cisco IOS Release 12.2(13)T. The Cisco 17xx platforms can support only HC DSP firmware images in this release.
12.3(8)T	Documentation of the **ds0-group** command was divided into the individual **ds0-group (E1)** and **ds0-group (T1)** commands.
12.4(2)T1	Support was added for the **e&m-lmr** signaling type on the Cisco 2691, Cisco 2600XM series, Cisco 2800 series (except Cisco 2801), Cisco 3660, Cisco 3700 series, and Cisco 3800 series.

Usage Guidelines

The **ds0-group** command automatically creates a logical voice port that is numbered as follows:

Note This command does not support the extended echo canceller (EC) feature on the Cisco AS5x00 series.

Although only one voice port is created for each group, applicable calls are routed to any channel in the group.

Be sure you take the following into account when you are configuring DS0 groups:

- Channel groups, CAS voice groups, DS0 groups, and time-division multiplexing (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.
- The keywords available for the **ds0-group** command are dependent upon the Cisco IOS software release that you are using. For the most current information, go to the Cisco Feature Navigator home page at the following URL: http://www.cisco.com/go/fn
- When you are using command-line interface (CLI) help, the keywords for the **ds0-group** command are configuration specific. For example, if MGCP is configured, you see the **mgcp** keyword. If you are not using MGCP, you do not see the **mgcp** keyword.
- Cisco IOS Releases later than 12.2 do not support the Single Attachment Station (SAS) CAS options of sas-loop-start and sas-ground-start.

Examples

The following example shows ranges of E1 controller time slots configured for FXS ground-start and FXO loop-start signaling:

```
E1 1/0
 framing esf
 linecode b8zs
 ds0-group 1 timeslots 1-10 type fxs-ground-start
 ds0-group 2 timeslots 11-24 type fxo-loop-start
```

The following example shows ranges of T1 controller time slots configured for FXS ground-start signaling:

```
controller E1 1/0
 ds0-group 1 timeslots 1-4 type fxs-ground-start
```

The following example illustrates setting the E1 channels for Signaling System 7 (SS7) service on any trunking gateway using the **mgcp** keyword:

```
Router(config-controller)# ds0-group 0 timeslots 1-24 type none service mgcp
```

In the following example, the time slot maximum is 12 and the time slot is 1, so two voice-ports are created successfully.

```
controller E1 0/0
 ds0-group 0 timeslots 1-4 type e&m-immediate-start
 ds0-group 1 timeslots 6-12 type e&m-immediate-start
```

If a third DS0 group is added, the voice-port is rejected even though the total number of voice channels is fewer than 16.

```
ds0-group 2 timeslots 17-18 type e&m-immediate-start
```

In the following example, the signaling type is set to E&M-LMR:

```
ds0-group 0 timeslots 1-10 type e&m-lmr
```

Related Commands

Command	Description
cas-group	Configures channelized T1 time slots with robbed bit signaling.
codec	Specifies the voice coder rate of speech for a dial peer.
codec complexity	Specifies call density and codec complexity based on the codec standard that you are using.

ds0-group (T1)

To specify the DS0 time slots that make up a logical voice port on a T1 controller, to specify the signaling type by which the router communicates with the PBX or PSTN, and to define T1 channels for compressed voice calls and the channel-associated signaling (CAS) method by which the router connects to the PBX or PSTN, use the **ds0-group** command in controller configuration mode. To remove the group and signaling setting, use the **no** form of this command.

Cisco IOS Release 12.2 and Later Releases- Cisco 1750 and Cisco 1751
ds0-group *ds0-group-number* **timeslots** *timeslot-list* [**service** *service-type*] **type** {**e&m-fgb** | **e&m-fgd** | **e&m-immediate-start** | **fgd-eana** | **fgd-os** | **fxs-ground-start** | **fxs-loop-start** | **none** | **r1-itu** | **r1-modified** | **r1-turkey**}
no ds0-group *ds0-group-number*

Cisco IOS Release 12.1 and Earlier Releases - Cisco 1750 and Cisco 1751
ds0-group *ds0-group-number* **timeslots** *timeslot-list* [**service** *service-type*] **type** {**e&m-fgb** | **e&m-fgd** | **e&m-immediate-start** | **fgd-eana** | **fgd-os** | **fxs-ground-start** | **fxs-loop-start** | **none** | **r1-itu** | **r1-modified** | **r1-turkey** | **sas-ground-start** | **sas-loop-start**}
no ds0-group *ds0-group-number*

Cisco 2600 Series (Except Cisco 2691), Cisco 3600 Series (Except Cisco 3660), and Cisco VG 200
ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type** {**e&m-delay-dial** | **em-fgd** | **e&m-immediate-start** | **e&m-wink-start** | **ext-sig** | **fgd-eana** | **fxo-ground-start** | **fxo-loop-start** | **fxs-ground-start** | **fxs-loop-start**}
no ds0-group *ds0-group-number*

Cisco 2691, Cisco 2600XM Series, Cisco 2800 Series (Except Cisco 2801), Cisco 3660, Cisco 3700 Series, Cisco 3800 Series
ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type** {**em-delay-dial** | **em-fgd** | **e&m-immediate-start** | **e&m-lmr** | **e&m-wink-start** | **ext-sig** | **fgd-eana** | **fgd-emf** [**mf**] [**ani-pani**] [**ani**] | **fxo-ground-start** | **fxo-loop-start** | **fxs-ground-start** | **fxs-loop-start**}
no ds0-group *ds0-group-number*

Cisco 7200 Series and Cisco 7500 Series
ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type** {**e&m-delay-dial** | **e&m-fgd** | **e&m-immediate-start** | **e&m-wink-start** | **fxo-ground-start** | **fxo-loop-start** | **fxs-ground-start** | **fxs-loop-start**}
no ds0-group *ds0-group-number*

Cisco 7700 Series Voice Ports
ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type** {**e&m-delay-dial** | **e&m-immediate-start** | **e&m-wink-start** | **fxo-ground-start** | **fxo-loop-start** | **fxs-ground-start** | **fxs-loop-start**}
no ds0-group *ds0-group-number*

Cisco IOS Release 12.2 and Later Releases for Cisco AS5300, Cisco AS5350, and Cisco AS5400
ds0-group *ds0-group-number* **timeslots** *timeslot-list* [**service** *service-type*] [**type e&m-fgd** [**dtmf** | **mf** [**dnis** | **ani-dnis** [**info-digits-no-strip**] | **fgd-emf** [**ani-pani**] [**ani**] | **service** *service-type*] | **e&m-immediate-start** | **fxs-ground-start** | **fxs-loop-start** | **fgd-eana** [**ani-dnis** | **mf**] | **fgd-os** [**dnis-ani** | **mf**] | **none**]]

no ds0-group *ds0-group-number*

Cisco AS5850
ds0-group *ds0-group-number* **timeslots** *timeslot-list* [**service** *service-type*] [**type e&m-fgd** [**dtmf** | **mf** [**dnis** | **ani-dnis** [**info-digits-no-strip**] | **fgd-emf** [**ani-pani**] [**ani**] | **service** *service-type*] | **e&m-immediate-start** | **fxs-ground-start** | **fxs-loop-start** | **fgd-eana** [**ani-dnis** | **mf**] | **fgd-os** [**dnis-ani** | **mf**] | **r1-itu** [**dnis**] | **none**]]
no ds0-group *ds0-group-number*

Cisco IOS Release 12.1 and Earlier Releases - Cisco AS5300, Cisco AS5350, and Cisco AS5400
ds0-group *ds0-group-number* **timeslots** *timeslot-list* [**service** *service-type*] [**type e&m-fgd** [**dtmf** | **mf** [**dnis** | **ani-dnis** [**info-digits-no-strip**] | **fgd-emf** [**ani-pani**] [**ani**] | **service** *service-type*] | **e&m-immediate-start** | **fxs-ground-start** | **fxs-loop-start** | **fgd-eana** [**ani-dnis** | **mf**] | **fgd-os** [**dnis-ani** | **mf**] | **sas-ground-start** | **sas-loop-start** | **none**]]
no ds0-group *ds0-group-number*

Cisco AS5850
ds0-group *ds0-group-number* **timeslots** *timeslot-list* [**service** *service-type*] [**type e&m-fgd** [**dtmf** | **mf** [**dnis** | **ani-dnis** [**info-digits-no-strip**] | **fgd-emf** [**ani-pani**] [**ani**] | **service** *service-type*] | **e&m-immediate-start** | **fxs-ground-start** | **fxs-loop-start** | **fgd-eana** [**ani-dnis** | **mf**] | **fgd-os** [**dnis-ani** | **mf**] | **sas-ground-start** | **sas-loop-start** | **none**]]
no ds0-group *ds0-group-number*

Syntax Description

ds0 -group-number	A value that identifies the DS0 group. Range is from 0 to 23.
timeslots *timeslot-list*	Lists time slots in the DS0 group. The *timeslot-list* argument is a single time-slot number, a single range of numbers, or multiple ranges of numbers separated by commas. Range is from 1 to 24. Examples are as follows: • 2 • 1-15,17-24 • 1-23 • 2,4,6-12

typenone	Specifies the type of signaling for the DS0 group. The signaling method selection for the type keyword depends on the connection that you are making. The ear and mouth (E&M) interface allows connection for PBX trunk lines (tie lines) and telephone equipment. The Foreign Exchange Station (FXS) interface allows connection of basic telephone equipment and a PBX interface. The Foreign Exchange Office (FXO) interface is for connecting the central office (CO) to a standard PBX interface where permitted by local regulations; it is often used for off-premise extensions (OPXs). Types are as follows: • **e&m-delay-dial** --The originating endpoint sends an off-hook signal and then waits for an off-hook signal followed by an on-hook signal from the destination. • **e&m-fgb** --E&M Type II Feature Group B. • **e&m-fgd** --E&M Type II Feature Group D. • **e&m-immediate-start** --E&M immediate start. • **e&m-lmr** --E&M Land Mobile Radio (LMR). • **e&m-wink-start** --The originating endpoint sends an off-hook signal and waits for a wink-start from the destination. • **ext-sig** --The external signaling interface specifies that the signaling traffic comes from an outside source. • **fgd-eana --Feature Group D exchange access North American.** • **fgd-emf--** FGD Enhanced MF. • **fgd-os** --Feature Group D operator services. • **fxo-ground-start --FXO ground-start signaling.** • **fxo-loop-start --FXO loop-start signaling.** • **fxs-ground-start --FXS ground-start signaling.** • **fxs-loop-start --FXS loop-start signaling.** • **none** --Null signaling for external call control. • **r1-itu** --Line signaling based on international signaling standards. (This signaling type is not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.) • **r1-modified** --An international signaling standard that is common to channelized T1/E1 networks.
	• **r1-turkey** --A signaling standard used in Turkey. • **sas-ground-start** --Single attachment station (SAS) ground-start. • **sas-loop-start** --SAS loop-start.

service *service-type*	(Optional) Specifies the type of service: • **data** --Data service. • **fax** -- Store-and-forward fax service. • **mgcp** --Media Gateway Control Protocol (MGCP) service. Used only with the type none keywords on the Cisco AS5x00 platforms. • **sccp** --Simple Gateway Control Protocol (SCCP) service. • **voice** --Voice service (for FGD-OS service).
dtmf	(Optional) Specifies dual tone multifrequency (DTMF) tone signaling.
mf	(Optional) Specifies multifrequency (MF) tone signaling
ani	(Optional) Provisions ANI address information.
ani-dnis	(Optional) Specifies automatic number identification (ANI) and dialed number identification service (DNIS) address information provisioning for FGD OS.
ani-pani	(Optional) Provisions ANI and PANI address information.
dnis-ani	(Optional) Specifies ANI and DNIS address information provisioning for FGD EANA.
dnis	(Optional) Specifies DNIS address information provisioning.
info-digits-no-strip	(Optional) Retains information digits on the Cisco AS5x00 platforms.

Command Default

There is no DS0 group. Calls are allowed in both directions.

Command Modes

Controller configuration

Command History

Release	Modification
11.2	This command was introduced for the Cisco AS5300 as the **cas-group** command.
11.3(1)MA	The command was introduced as the **voice-group** command for the Cisco MC3810.
12.0(1)T	This command was integrated into Cisco IOS Release 12.0(1)T, and the **cas-group** command was implemented on the Cisco 3600 series routers.
12.0(5)T	The command was renamed **ds0-group** on the Cisco AS5300 and Cisco 2600 series and Cisco 3600 series routers. Some keyword modifications were implemented.
12.0(5)XE	This command was implemented on the Cisco 7200 series.
12.0(7)XK	Support for this command was implemented on the Cisco MC3810. When the **ds0-group** command became available on the Cisco MC3810, the **voice-group** command was removed and no longer supported. The **ext-sig** keyword replaced the **ext-sig-master** and **ext-sig-slave** keywords that were available with the **voice-group** command.
12.0(7)XR	The **mgcp** service type was added.

Release	Modification
12.1(2)XH	The **e&m-fgd** and **fgd-eana** keywords were added for Feature Group D signaling.
12.1(5)XM	The **sgcp** keyword was removed.
12.1(3)T	This command was modified for Cisco 7500 series routers. The **fgd-os** signaling type and the **voice** service type were added.
12.2(2)XA	This command was implemented on the Cisco AS5300.
12.2	The command was modified to exclude sas keywords. The Single Attachment Station (SAS) CAS options of sas-loop-start and sas-ground-start are not supported as a type of signaling for the DS0 group.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
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(4)XM	This command was implemented on Cisco 1750 and Cisco 1751 routers. Support for other Cisco platforms is not included in this release.
12.2(2)XN	Support for the **mgcp** keyword was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
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.
12.2(11)T	This command was supported in Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2. This command is supported on the Cisco IAD2420 series, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5850 in this release.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. The Cisco 1750 and Cisco 1751 do not support T1 and E1 voice and data cards in Cisco IOS Release 12.2(13)T. The Cisco 17xx platforms can support only HC DSP firmware images in this release.
12.2(15)T	This command was implemented on the Cisco 2600XM, Cisco 3725, and Cisco 3745.
12.3(4)XD	This command was modified for the Cisco 3725 and Cisco 3745. The **e&m-lmr** signaling type was added.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(8)T	Documentation of the **ds0-group** command was divided into the individual **ds0-group**(E1) and **ds0-group**(T1) commands.
12.3(10)	The **info-digits-no-strip** keyword was added for use on the Cisco AS5x00 platforms.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T. The **fgd-emf**, **ani-pani**, and **ani** keywords were added for the Cisco 2800 and Cisco AS5x00 platforms.

Usage Guidelines

The **ds0-group** command automatically creates a logical voice port that is numbered as follows:

- Cisco 2600 series, Cisco 2600XM, Cisco 3660, Cisco 3725, Cisco 3745, and Cisco 7200 series:
  - *slot*/*port* **:** *ds0-group-number*
- Cisco AS5300, Cisco AS5350, and Cisco AS5400 with a T1 controller:
  - *slot*/*port*
- Cisco AS5850 with a T1 controller:
  - *slot*/*port* **:** *ds0-group-number*

Although only one voice port is created for each group, applicable calls are routed to any channel in the group.

Be sure that you take the following into account when you are configuring DS0 groups:

- Channel groups, CAS voice groups, DS0 groups, and time-division multiplexing (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.
- The keywords available for the **ds0-group** command are dependent upon the Cisco IOS software release that you are using. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

- When you are using command-line interface (CLI) help, the keywords for the **ds0-group** command are configuration specific. For example, if MGCP is configured, you see the **mgcp** keyword. If you are not using MGCP, you do not see the **mgcp** keyword.



Note This command does not support the extended echo canceller (EC) feature on the Cisco AS5x00 series.



Note The signaling type R1-ITU is not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.

Examples

The following example shows ranges of T1 controller time slots configured for FXS ground-start and FXO loop-start signaling:

```
controller T1 1/0
 framing esf
 linecode b8zs
 ds0-group 1 timeslots 1-10 type fxs-ground-start
 ds0-group 2 timeslots 11-24 type fxo-loop-start
```

The following example shows ranges of T1 controller time slots configured for FXS ground-start signaling:

```
controller T1 1/0
 ds0-group 1 timeslots 1-4 type fxs-ground-start
```

The following example illustrates setting the T1 channels for Signaling System 7 (SS7) service on any trunking gateway using the **mgcp** keyword:

```
ds0-group 0 timeslots 1-24 service mgcp type none
```

In the following example, the time slot maximum is 12 and the time slot is 1, so two voice ports are created successfully:

```
controller T1 0/0
 ds0-group 0 timeslots 1-4 type e&m-immediate-start
 ds0-group 1 timeslots 6-12 type e&m-immediate-start
```

If a third DS0 group is added, the voice port is rejected even though the total number of voice channels is fewer than 16.

```
ds0-group 2 timeslots 17-18 type e&m-immediate-start
```

In the following example, the signaling type is set to E&M LMR:

```
ds0-group 0 timeslots 1-10 type e&m-lmr
```

You have the option to retain info digits when you are configuring E&M Type II Feature Group D with MF signaling and ANI/DNIS for calls being sent over IP. Info digits denote the subscriber type, and the **info-digits** keyword prepends info digits to the calling number.

On inbound calls from a T1 FGD voice-port with MF ANI/DNIS, when ANI information is obtained, it is passed unaltered to the next matching dial peer, either POTS or VoIP. The addition of the **info-digits-no-strip** keyword allows you to retain the info digits portion of the ANI information; the modified ANI is then passed to the next matching dial peer. Ordinarily, info digits are not valid for calls going over IP and are, therefore, stripped off. The ability to retain info digits is particularly useful for calls that are not leaving the PSTN network and are just being hairpinned back.

In the following example, the E&M Type II Feature Group D is configured with MF signaling and ANI/DNIS over IP while retaining info digits:

```
 ds0-group 0 timeslots 1-24 type e&m-fgd mf ani-dnis info-digits-no-strip
```

The following example enables FGD EMF:

```
 ds0-group 11 timeslots 11 type fgd-emf ani
 ds0-group 11 timeslots 11 type fgd-emf ani-pani
```

Related Commands

Command	Description
cas-group	Configures channelized T1 time slots with robbed bit signaling.
codec	Specifies the voice coder rate of speech for a dial peer.
codec complexity	Specifies call density and codec complexity based on the codec standard that you are using.

ds0-num

To add B-channel information in outgoing Session Initiation Protocol (SIP) messages, use the **ds0-num**command in SIP voice service configuration mode. To return to the default setting, use the **no** form of this command.

ds0-num
no ds0-num

Syntax Description

This command has no arguments or keywords.

Command Default

B channel information is disabled.

Command Modes

SIP voice service configuration (conf-serv-sip)

Command History

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

Usage Guidelines

This command enables the SIP application to receive B-channel information of incoming ISDN calls. The B-channel information appears in the Via header of an Invite request. Information acquired from the Via header can be used during call transfer or to route a call.

Examples

The following example adds B-channel information to outgoing SIP messages:

```
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# ds0-num
```

Related Commands

Command	Description
sip	Enables SIP voice service configuration commands.
voice service voip	Specifies the voice encapsulation type as VoIP.

dscp media

To specify the resource priority header (RPH) to differentiated services code point (DSCP) mapping, use the **dscp media** command in voice class configuration mode. To disable the configuration, use the **no** form of this command.

dscp media {**audio** | **video**} {**flah-override-override** | **flash-override** | **flsh** | **immediate** | **priority** | **routine**} {*dscp-valueset-afset-cs* | **ef** | **zero**}
no dscp media {**audio** | **video**} {**flah-override-override** | **flash-override** | **flsh** | **immediate** | **priority** | **routine**} {*dscp-valueset-afset-cs* | **ef** | **zero**}

Syntax Description

audio	Applies DSCP to audio payload packets.
video	Applies DSCP to video payload packets.
flah-override-override	Applies flash-override-override RPH priority.
flash-override	Applies flash-override RPH priority.
flsh	Applies flash RPH priority.
immediate	Applies immediate RPH priority.
priority	Applies priority RPH priority.
routine	Applies routine RPH priority.
dscp-value	DSCP value. Valid values are from 0 to 63.

set-af	An assured forwarding bit pattern as the DSCP value: • **af11** —bit pattern 001010 • **af12** —bit pattern 001100 • **af13** —bit pattern 001110 • **af21** —bit pattern 010010 • **af22** —bit pattern 010100 • **af23** —bit pattern 010110 • **af31** —bit pattern 011010 • **af32** —bit pattern 011100 • **af33** —bit pattern 011110 • **af41** —bit pattern 100010 • **af42** —bit pattern 100100 • **af43** —bit pattern 100110
set-cs	Class-selector code point as the DSCP value: • **cs1** —code point 1 (precedence 1) • **cs2** —code point 2 (precedence 2) • **cs3** —code point 3 (precedence 3) • **cs4** —code point 4 (precedence 4) • **cs5** —code point 5 (precedence 5) • **cs6** —code point 6 (precedence 6) • **cs7** —code point 7 (precedence 7)
ef	Specifies the expedited forwarding bit pattern 101110 as the DSCP value.
zero	Specifies the default bit pattern 000000 as the DSCP value.

Command Default

See the Usage Guidelines section.

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 **dscp media** command to configure RPH to DSCP mapping for audio and video calls.

The following table lists the default values for the **dscp media** command:

Granular Service Class	Priority or Precedence	DSCP Base10 Value	DSCP Binary Value
Voice	Audio Call	46	101110
	Flash	43	101011
	Flash Override	41	101001
	Flash Override Override	40	101000
	Immediate	45	101101
	Priority	47	101111
	Routine	49	110001
Video	Flash Override	33	100001
	Flash	35	100011
	Flash Override Override	32	100000
	Immediate	37	100101
	Priority	39	100111
	Routine	51	110011
	Video Call	34	100111

Examples

The following example shows how to specify RPH to DSCP mapping after you configure the DSCP profile:

```
Router> enable
Router# configure terminal
Router(config)# voice class dscp-profile 1
Router(config-class)# dscp media audio routine ef
```

Related Commands

Command	Description syslog
violation	Specifies the action that needs to be performed on any violation in the DSCP policy.

dscp-profile

To apply a differentiated services code point (DSCP) profile globally, use the **dscp-profile** command in voice service SIP configuration mode or voice class tenant configuration mode. To disable the configuration, use the **no** form of this command.

dscp-profile *tag*
no dscp-profile

Syntax Description

tag	DSCP profile tag. The range is from 1 to 10000.

Command Default

A DSCP profile is not applied.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.6(2)T and IOS XE Denali 16.3.1	This command is now available under voice class tenants.

Usage Guidelines

You can use the **dscp-profile** command to apply a DSCP profile that is configured using the **dscp media** command at the global level.

Examples

The following example shows how to configure a DSCP profile at the global level:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# dscp-profile 1
```

Related Commands

Command	Description
dscp media	Specifies the RPH to DSCP mapping.
voice service voip	Enters voice service configuration mode.
sip	Enters service SIP configuration mode.

dsn

To specify that a delivery status notice (DSN) be delivered to the sender, use the **dsn** command in dial-peer configuration mode. To cancel a specific DSN option, use the **no** form of this command.

dsn {**delay** | **failure** | **success**}
no dsn {**delay** | **failure** | **success**}

Syntax Description

delay	Defines the delay for each mailer.
failure	Requests that a failed message be sent to the FROM address. This is the default.
success	Requests that a message be sent to the FROM address saying that the mail message was delivered successfully to the recipient.

Command Default

The default is to send a nondelivery message in the event of a failure.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series and Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

When the delay keyword is selected, the next-hop mailer sends a message to the FROM address saying that the mail message was delayed. The definition of the delay keyword is made by each mailer and is not controlled by the sender. Each mailer in the path to the recipient that supports the DSN extension receives the same request.

When the failure keyword is selected, the next-hop mailer sends a message to the FROM address that the mail message delivery failed. Each mailer in the path to the recipient that supports the DSN extension receives the same request.

When the success keyword is selected, the next-hop mailer sends a message to the FROM address saying that the mail message was successfully delivered to the recipient. Each mailer in the path to the recipient that supports the DSN extension receives the same request.

Note In the absence of any other DSN settings (for example, no dsn, or a mailer in the path that does not support the DSN extension), a failure to deliver message always causes a nondelivery message to be generated. This nondelivery message is called a bounce.

This command is applicable to Multimedia Mail over Internet Protocol (MMoIP) dial peers.

DSNs are messages or responses that are automatically generated and sent to the sender or originator of an e-mail message by the Simple Mail Transfer Protocol (SMTP) server, notifying the sender of the status of the e-mail message. Specifications for DSN are described in RFC 1891, RFC 1892, RFC 1893, and RFC 1894.

The on-ramp DSN request is included as part of the fax-mail message sent by the on-ramp gateway when the matching MMoIP dial peer has been configured. The on-ramp DSN response is generated by the SMTP server when the fax-mail message is accepted. The DSN is sent back to the user defined by the **mta send mail-from** command. The off-ramp DSN is requested by the e-mail client. The DSN response is generated by the SMTP server when it receives a request as part of the fax-mail message.

Note DSNs are generated only if the mail client on the SMTP server is capable of responding to a DSN request.

Because the SMTP server generates the DSNs, you need to configure both mail from: and rcpt to: on the server for the DSN feature to work. For example:

```
mail from: <user@mail-server.sample.com>
rcpt to: <fax=555-0112@sample.com> NOTIFY=SUCCESS,FAILURE,DELAY
```

Three different states can be reported back to the sender:

- Delay--Indicates that the message was delayed in being delivered to the recipient or mailbox.
- Success--Indicates that the message was successfully delivered to the recipient or mailbox.
- Failure--Indicates that the SMTP server was unable to deliver the message to the recipient or mailbox.

Because these delivery states are not mutually exclusive, you can configure store-and-forward fax to generate these messages for all or any combination of these events.

DSN messages notify the sender of the status of a particular e-mail message that contains a fax TIFF image. Use the **dsn** command to specify which notification messages are sent to the user.

The **dsn** command allows you to select more than one notification option by reissuing the command and specifying a different notification option each time. To discontinue a specific notification option, use the **no** form of the command for that specific keyword.

If the **failure** keyword is not included when DSN is configured, the sender receives no notification of message delivery failure. Because a failure is usually significant, care should be taken to always include the **f ailure keyword**as part of the **dsn** command configuration.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example specifies that a DSN message be returned to the sender when the e-mail message that contains the fax has been successfully delivered to the recipient or if the message that contains the fax has failed to be delivered:

```
dial-peer voice 10 mmoip
 dsn success
 dsn failure
```

Related Commands

Command	Description
mta send mail -from hostname	Specifies the originator (host-name portion) of the e-mail fax message.
mta send mail -from username	Specifies the originator (username portion) of the e-mail fax message.

dsp allocation signaling dspid

To change the digital signal processor (DSP) selection for signaling channel allocation from the default (DSP weight-based) to the DSP ID number, use the **dsp allocation signaling dspid** command in voice-card configuration mode. To return to the default behavior, use the **no** form of this command.

dsp allocation signaling dspid
no dsp allocation signaling dspid

Syntax Description

This command has no arguments or keywords.

Command Default

Selection of a DSP for signaling channel allocation is based on the internal weighted value assigned to the DSPs.

Command Modes

Voice-card configuration (config-voicecard)

Command History

Release	Modification
12.4(15)T9	This command was introduced.

Usage Guidelines

The **dsp allocation signaling dspid** command takes effect only after a reload of the router. The command should be enabled and saved into the startup-config file.

The default signal channel allocation method (by weight) may not be suitable for some network implementations. The default allocation method selects the DSPs based on the DSP weight, and you cannot control the selection of the DSP for specific configuration even if the order of the packet voice data modules (PVDMs) is changed. Enable the **dsp allocation signaling dspid** command to change the selection order to the DSP ID number. This command is more useful when there is a PVDM2-8 module in the network configuration.

Examples

The following example shows how to change the default for DSP allocation from the DSP weight to the DSP ID number:

```
voice card 1
 dsp allocation signaling dspid
```

Related Commands

Command	Description
show voice dsp	Displays the current status or selective statistics of DSP voice channels.
voice-card	Enters voice-card configuration mode.

dsp services dspfarm

To enable digital-signal-processor (DSP) farm services for a particular voice network module, use the **dsp services dspfarm** command in voice card configuration mode. To disable services, use the **no** form of this command.

dsp services dspfarm
no dsp services dspfarm

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Voice-card configuration (config-voicecard)

Command History

Release	Modification
12.2(13)T	This command was introduced.
Cisco IOS XE Release 3.2S	Support for this command was added on Cisco ASR 1000 Series Routers.

Usage Guidelines

The router must be equipped with one or more voice network modules that provide DSP resources. DSP resources are used only if this command is configured under the particular voice card.

The number of voice network modules that must be enabled for DSP-farm services depends on the number of DSPs on the module and on the maximum number of transcoding and conferencing sessions configured for the DSP farm.

Note Use this command before enabling DSP-farm services with the **dspfarm** command for an NM-HDV or NM-HDV-FARM.

Cisco ASR 1000 Series Router

The SPA-DSPs on a Cisco ASR 1000 Series Routers are installed in a subslot on a SIP. Hence, when referring to a SPA-DSP the **voice-card** command is used.

Examples

The following example enables DSP-farm services on an NM-HDV2 or NM-HD-1V/2V/2VE:

```
Router(config)# voice-card 2
Router(config-voicecard)# dsp services dspfarm
Router(config-voicecard)# exit
```

The following example enables DSP-farm services on an NM-HDV or NM-HDV-FARM:

```
Router(config)# voice-card 2
Router(config-voicecard)# dsp services dspfarm
Router(config-voicecard)# exit
```

The following example enables DSP-farm services on SPA-DSP for a Cisco ASR 1000 Series Router:

```
Router(config)# voice-card 1/1
Router(config-voicecard)# dsp services dspfarm
Router(config-voicecard)# exit
```

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 voice dsp (SPA-DSP)	Displays the DSP current status or the selective statistics of the DSP voice channels.

dspfarm (DSP farm)

To enable digital signal processor (DSP) farm service, use the **dspfarm** command in global configuration mode. To disable the service, use the **no** form of this command.

dspfarm
no dspfarm

Syntax Description

This command has no arguments or keywords.

Command Default

DSP-farm service is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.

Usage Guidelines

The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide DSP resources.

Before enabling DSP-farm services, you must configure the NM-HDV or NM-HDV-FARM on which DSP-farm services are to be enabled using the **dsp services dspfarm** command. You must also specify the maximum number of transcoding sessions to be supported by the DSP farm using the **dspfarm transcoder maximum sessions** command.

This command causes the system to download new firmware into the DSPs, start up the required subsystems, and wait for a service request from the transcoding and conferencing applications.

Examples

The following example configures an NM-HDV or NM-HDV-FARM, specifies the maximum number of transcoding sessions, and enables DSP-farm services:

```
Router# configure terminal
Router(config)# no dspfarm
Router(config)# voice-card 2
Router(config-voicecard)# dsp services dspfarm
Router(config-voicecard)# exit
Router(config)# dspfarm transcoder maximum sessions 15
Router(config)# dspfarm
```

Related Commands

Command	Description
dsp services dspfarm	Specifies the NM-HDV or NM-HDV-FARM on which DSP-farm services are to be enabled.

Command	Description
dspfarm transcoder maximum sessions	Specifies the maximum number of transcoding sessions to be supported by a DSP farm.
show dspfarm	Displays summary information about DSP resources.

dspfarm (voice-card)

To add a specified voice card to those participating in a digital signal processor (DSP) resource pool, use the **dspfarm** command in voice-card configuration mode. To remove the specified card from participation in the DSP resource pool, use the **no** form of this command.

dspfarm
no dspfarm

Syntax Description

This command has no arguments or keywords.

Command Default

A card participates in the DSP resource pool.

Command Modes

Voicecard configuration (config-voicecard)

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 3660.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB	This command was implemented on the Cisco 2600 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(15)T	This command was implemented on the Cisco 2600XM, Cisco 3725, and Cisco 3745.

Usage Guidelines

DSP mapping occurs when DSP resources on one AIM or network module are available for processing of voice time-division multiplexing (TDM) streams on a different network module or on a voice/WAN interface card (VWIC). This command is used on Cisco 3660 routers with multiservice interchange (MIX) modules installed or on Cisco 2600 series routers with AIMs installed.

To reach voice-card configuration mode for a particular voice card, from global configuration mode enter the **voice-card** command and the slot number for the AIM or network module that you want to add to the pool. See the **voice-card** command page for details on slot numbering.

The assignment of DSP pool resources to particular TDM streams is based on the order in which the streams are configured with the **ds0-group** command for T1/E1 channel-associated signaling (CAS) or with the **pri-group** command for ISDN PRI.

The assignment of DSP pool resources does not occur dynamically during call signaling.

Examples

The following example adds to the DSP resource map the DSP resources on the network module in slot 5 on a Cisco 3660 with a MIX module:

```
voice-card 5
 dspfarm
```

The following example makes available the DSP resources on an AIM on a modular access router:

```
voice-card 0
 dspfarm
```

Related Commands

Command	Description
ds0-group	Specifies the DS0 time slots that make up a logical voice port on a T1 or E1 controller, Specifies the signaling type by which the router communicates with the PBX or PSTN, Defines T1or E1 channels for compressed voice calls and the CAS method by which the router connects to the PBX or PSTN.
pri-group	Specifies ISDN PRI on a channelized T1 or E1 controller.
voice-card	Enters voice-card configuration mode.

dspfarm confbridge maximum

To specify the maximum number of concurrent conference sessions for which digital signal processor (DSP) farm resources should be allocated, use the **dspfarm confbridge maximum**command in global configuration mode. To reset to the default, use the **no** form of this command.

dspfarm confbridge maximum {**mixed-mode sessions** | **sessions**} *number*
no dspfarm confbridge maximum {**mixed-mode sessions** | **sessions**} *number*

Syntax Description

mixed-mode	Specifies the maximum number of transcoding sessions for mixed-mode conferencing.
sessions	Specifies the conferencing maximum sessions parameter value.
number	Number of conference sessions. A single DSP supports one conference session with up to six participants.

Command Default

No DSP farm resources are allocated for the sessions.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was modified. This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.
15.0(1)M	This command was modified. The **mixed-mode** keyword was added.

Usage Guidelines

The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide DSP resources.

Before using this command, you must disable DSP-farm service using the **no dspfarm** command.

The maximum number of conference sessions depends upon DSP availability in the DSP farm. A single DSP supports one conference session with up to six participants. However, you may need to allocate additional DSP resources for transcoding to support conferences. If all participants use G.711 or G.729 codecs, you need not allocate any additional DSP resources because transcoding is done in the conferencing DSP.

When you use this command, take into consideration the number of DSPs allocated for transcoding services with the **dspfarm transcoder maximum sessions**command.

Examples

The following example sets the maximum number of transcoding sessions for mixed-mode conferencing to 8:

```
Router# dspfarm confbridge maximum mixed-mode sessions 8
```

Related Commands

Command	Description
dspfarm (DSP farm)	Enables DSP-farm service.
dspfarm transcoder maximum sessions	Specifies the maximum number of transcoding sessions to be supported by a DSP farm.
show dspfarm	Displays summary information about DSP resources.

dspfarm connection interval

To specify the time interval during which to monitor Real-Time Transport Protocol (RTP) inactivity before deleting an RTP stream, use the **dspfarm connection interval**command in global configuration mode. To reset to the default, use the **no** form of this command.

dspfarm connection interval *seconds*
no dspfarm connection interval *seconds*

Syntax Description

seconds	Interval, in seconds, during which to monitor RTP inactivity. Range is from 60 to 10800. Default is 600.

Command Default

600 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.

Usage Guidelines

The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide digital signal processor (DSP) resources.

After each interval, RTP streams are checked for inactivity. If all RTP streams for a particular call are inactive, the RTP timer, as set with the **dspfarm rtp timeout** command, is started. When the RTP timer expires, the call is deleted.

Examples

The following example sets the connection interval to 60 seconds:

```
Router(config)# dspfarm connection interval 60
```

Related Commands

Command	Description
dspfarm rtp timeout	Specifies the RTP timeout interval used to clear hanging connections.

dspfarm profile

To enter DSP farm profile configuration mode and define a profile for digital signal processor (DSP) farm services, use the **dspfarm profile**command in global configuration mode. To delete a disabled profile, use the **no** form of this command.

Cisco Unified Border Element
dspfarm profile *profile-identifier* {**conference** | **mtp** | **transcode**} [**security**]
no dspfarm profile *profile-identifier*

Cisco Unified Border Element (Enterprise) Cisco ASR 1000 Series Router
dspfarm profile *profile-identifier* **transcode**
no dspfarm profile *profile-identifier*

Cisco Integrated Services Routers Generation 2 (Cisco ISR G2)
dspfarm profile *profile-identifier* {**conference** [**video** [**homogeneous** | **heterogeneous** | **guaranteed-audio**]] | **mtp** | **transcode** [**video** | **universal**]} [**security**]
no dspfarm profile *profile-identifier*

Syntax Description

profile identifier	Number that uniquely identifies a profile. Range is 1 to 65535. There is no default.
conference	Enables a profile for conferencing.
mtp	Enables a profile for Media Termination Point (MTP).
transcode	Enables a profile for transcoding.
security	Enables a profile for secure DSP farm services.
video	(Optional) Enables a profile for video conferencing or transcoding.
homogeneous	(Optional) Specifies that all video participants use the one video format that is configured in this profile. DSP resources are reserved to support the conference at configuration time. **Note** The homogeneous profiles only support one video codec.
heterogeneous	(Optional) Specifies that video participants can use the different video formats that are configured in the profile. You can configure up to 10 video codecs in the heterogeneous profile. DSP resources are reserved to support the different configurations at configuration time.
guaranteed-audio	(Optional) Specifies that video participants in a heterogeneous conference will at least have an audio connection. You can configure up to 10 video codecs in the guaranteed-audio profile. The DSP resources for audio streams are reserved at configuration time, but DSP resources to support video conferences are not reserved. If the video endpoint supports the video format specified in the profile and DSP resources are available when the participant joins the conference, the participant joins as a video conferee in the video conference.

Command Default

If this command is not entered, no profiles are defined for the DSP farm services.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(11)XW	The **security** keyword was added.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(22)T	Support for IPv6 was added.
15.0(1)M2 15.1(1)T	Support was modified for the Cisco IAD 2430, IAD 2431, IAD 2432, and IAD 2435, and the Cisco VG 202, VG 204, and VG 224 platforms.
Cisco IOS XE Release 3.2S	This command was modified. Support was added to the Cisco ASR 1000 Series Router. The **conference**, **mtp**& **security**keywords are not supported on the Cisco ASR 1000 Series Router in this release.
15.1(4)M	This command was modified. The **video** keyword was added.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.3S.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use this command to create a new profile or delete a disabled profile. After you create a new profile in dspfarm profile configuration mode, use the **no shutdown**command to enable the profile configuration, allocate resources and associate the profile with the application(s). If the profile cannot be enabled due to lack of resources, the system prompts you with a message "Can not enable the profile due to insufficient resources, resources available to support X sessions; please modify the configuration and retry."

If the DSP farm profile is successfully created, you enter the DSP farm profile configuration mode. You can configure multiple profiles for the same service.

Use the **no dspfarm profile** command to delete a profile from the system. If the profile is active, you cannot delete it; you must first disable it using the **shutdown** command. To modify a DSP farm profile, use the **shutdown** command in dspfarm profile configuration mode before you begin configuration.

The *profile identifier*uniquely identifies a profile. If the service type and *profile identifier*are not unique, the user is prompted with a message to choose a different profile identifier.

You must use the **security** keyword in order to enable secure DSP farm services such as secure transcoding.

Effective with Cisco IOS Releases 15.0(1)M2 and 15.1(1)T, platform support for the Cisco IAD 2430, IAD 2431, IAD 2432, and IAD 2435, and the Cisco VG 202, VG 204, and VG 225 is modified. These platforms are designed as TDM-IP devices and are not expandable to install extra DSP resources. So even though the **conference** keyword appears in the command syntax, this DSP service is not configurable on these platforms. If you try to configure conferencing on these platforms, the command-line interface displays the following message: " %This platform does not support Conferencing feature. "

The **transcode** keyword also appears in the command syntax, but this DSP service is not available on the Cisco VG 202, VG 204, and VG 224 platforms. If you try to configure transcoding on these platforms, the CLI displays the following message: " %This platform does not support Transcoding feature. "

Cisco ASR 1000 Series Router

The support for dspfarm profile command was added on Cisco ASR 1000 Series Router from Cisco IOS XE Release 3.2 and later releases. The command is used to create a dspfarm profile for different services.

Note The secure DSP farm services is always enabled for SPA-DSP on Cisco ASR 1000 Series Router. Only **transcode** keyword is supported on Cisco ASR 1000 Series Router for Cisco IOS XE Release 3.2s. The **conference**, **media**, and **security** keywords are not supported on Cisco ASR 1000 Series Router for Cisco IOS XE Release 3.2s.

In order to configure a video dspfarm profile, you must set **voice-service dsp-reservation** command to be less than 100 percent.

To enable dspfarm profiles for voice services, you must use the dsp services dspfarmcommand **under the voice-card submode.**

Examples

The following example enables DSP farm services profile 20 for conferencing:

```
Router(config)# dspfarm profile 20 conference
```

Note the response if the profile is already being used:

```
Router(config)# dspfarm profile 6 conference
Profile id 6 is being used for service TRANSCODING
 please select a different profile id
```

The following example enables DSP farm services profile 1 for transcoding:

```
Router(config)# dspfarm profile 1 transcode
```

Video Conferences

The following example enables DSP farm services profile 99 for homogeneous video. The conference supports four participants under one format (Video codec H.263, qcif resolution, and a frame-rate of 15 f/s).

```
Router(config)# dspfarm profile 99 conference video homogeneous
Router(config-dspfarm-profile)# codec h263 qcif frame-rate 15

Router(config-dspfarm-profile)# maximum conference-participant 4
```

Related Commands

Command	Description
dsp service dspfarm	Configures the DSP farm services for a specified voice card.
shutdown (DSP farm profile)	Disables the DSP farm profile.

Command	Description
voice-card	Enters voice card configuration mode
voice-service dsp-reservation	Configures the percentage of DSP resources are reserved for voice services and enables video services to use the remaining DSP resources.

dspfarm rtp timeout

To specify the Real-Time Transport Protocol (RTP) timeout interval used to clear hanging connections, use the **dspfarm rtp timeout** command in global configuration mode. To reset to the default, use the **no** form of this command.

dspfarm rtp timeout *seconds*
no dspfarm rtp timeout

Syntax Description

seconds	RTP timeout interval, in seconds. Range is from 10 to 7200. Default is 1200.

Command Default

1200 seconds (20 minutes)

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.

Usage Guidelines

The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide digital signal processor (DSP) resources.

Use this command to set the RTP timeout interval for when the error condition "RTP port unreachable" occurs.

Examples

The following example sets the RTP timeout value to 600 seconds (10 minutes):

```
Router# dspfarm rtp timeout 600
```

Related Commands

Command	Description
dspfarm (DSP farm)	Enables DSP-farm service.
dspfarm connection interval	Specifies the time interval during which to monitor RTP inactivity before deleting an RTP stream.
show dspfarm	Displays summary information about DSP resources.

dspfarm transcoder maximum sessions

To specify the maximum number of transcoding sessions to be supported by the digital signal processor (DSP) farm, use the **dspfarm transcoder maximum sessions** command in global configuration mode. To reset to the default, use the **no** form of this command.

dspfarm transcoder maximum sessions *number*
no dspfarm transcoder maximum sessions

Syntax Description

number	Number of transcoding sessions.

Command Default

0 sessions

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.

Usage Guidelines

The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide DSP resources.

Before using this command, you must disable DSP-farm service using the **no dspfarm** command.

Use this command in conjunction with the **dspfarm confbridge maximum sessions**commands.

The maximum number of transcoding sessions depends upon DSP availability in the DSP farm. A single DSP supports four transcoding sessions transmitted to and from G.711 and G.729 codecs.

Examples

The following example configures an NM-HDV or NM-HDV-FARM, specifies the maximum number of transcoding sessions, and enables DSP-farm services:

```
Router# configure terminal
Router(config)# no dspfarm
Router(config)# voice-card 2
Router(config-voicecard)# dsp services dspfarm
Router(config-voicecard)# exit
Router(config)# dspfarm transcoder maximum sessions 15
Router(config)# dspfarm
```

Related Commands

Command	Description
dspfarm (DSP farm)	Enables DSP-farm service.

Command	Description
dspfarm confbridge maximum sessions	Specifies the maximum number of conferencing sessions to be supported by a DSP farm.
dsp services dspfarm	Specifies the NM-HDV or NM-HDV-FARM on which DSP-farm services are to be enabled.
show dspfarm	Displays summary information about DSP resources.

dspint dspfarm

To enable the digital signal processor (DSP) interface, use the **dspint dspfarm** command in global configuration mode. This command does not have a no form.

dspint dspfarm *slot/port*

Syntax Description

slot	Slot number of the interface.
port	Port number of the interface.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced on the Cisco 7200 series routers.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(13)T	This command was implemented on the Cisco 7200 series.

Usage Guidelines

DSP mapping occurs when DSP resources on one advanced interface module (AIM) or network module are available for processing of voice time-division multiplexing (TDM) streams on a different network module or on a voice/WAN interface card (VWIC). This command is used on Cisco 3660 routers with multiservice interchange (MIX) modules installed or on Cisco 2600 series routers with AIMs installed.

To enter voice-card configuration mode for a particular voice card, from global configuration mode enter the **voice-card**command and the slot number for the AIM or network module that you want to add to the pool. See the **voice-card**command page for details on slot numbering.

The assignment of DSP pool resources to particular TDM streams is based on the order in which the streams are configured using the **ds0-group** command for T1/E1 channel-associated signaling (CAS) or using the **pri-group** command for ISDN PRI.

The assignment of DSP pool resources does not occur dynamically during call signaling.

To disable the interface use the **no shutdown** command.

Examples

The following example creates a DSP farm interface with a slot number of 1 and a port number of 0:

```
dspint dspfarm 1/0
```

To change codec complexity on the Cisco 7200 series, you must enter the following commands:

```
Router# configure terminal
Router(config)# dspint dspfarm 2/0
Router(config-dspfarm)# codec medium | high ecan-extended
```

Related Commands

Command	Description
ds0-group	Specifies the DS0 time slots that make up a logical voice port on a T1 or E1 controller.
no shutdown	Disables the interface.
pri-group	Specifies an ISDN PRI on a channelized T1 or E1 controller
show interfaces dspfarm dsp	Displays information about the DSP interface.
voice-card	Enters voice-card configuration mode.

dtmf-interworking

To enable a delay between the dtmf-digit begin and dtmf-digit end events in the RFC 2833 packets sent from Cisco Unified Border Element (Cisco UBE) or Cisco Unified Communications Manager Express (Cisco Unified CME) or to generate RFC 4733 compliance RTP Named Telephony Event (NTE) packets from CUBE, use the **dtmf-interworking** command in voice service or dial peer voice configuration mode. To remove the delay interval, use the **no** form of this command.

dtmf-interworking {**rtp-nte** | **standard** | **system**}
no dtmf-interworking

Syntax Description

rtp-nte	Enables a delay between the dtmf-digit begin and dtmf-digit end events of RTP NTE packets.
standard	Generates RTP NTE packets that are RFC 4733 compliant.
system	Specifies the default global dual tone multifrequency (DTMF) interworking configuration. This keyword is available only in dial peer voice configuration mode.

Command Default

RFC 2833 packet is sent in a single burst of three dtmf-digit begin events, one duration equaling 50 ms, and three dtmf-digit end events with a duration of 100 ms.

Command Modes

Voice service configuration (config-voi-serv)

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.
15.1(2)T5	This command was modified. The **standard** and **system** keywords were added.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

- **dtmf-interworking rtp-nte**—If your system is configured for RFC 2833 DTMF interworking and if the remote system cannot handle RFC 2833 packets sent in a single burst, use this command to introduce a delay between the dtmf-digit begin and end events in the RFC 2833 packet.
- **dtmf-interworking standard**—When the remote system needs RFC 4733 packets, then use this command to generate RFC 4733 compliance. In this configuration, one dtmf-digit begin event is initiated when CUBE receives start event.
- **dtmf-interworking system**—When this command is configured in dial peer voice configuration mode then the global level dtmf-interworking configuration is applicable. This is the default configuration under the dial peer.

Examples

The following example shows configuration of a delay between the dtmf-digit and events:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(config-voi-serv)# dtmf-interworking rtp-nte
Device(config-voi-serv)# end
```

The following example shows the generation of RTP NTE packets that are RFC 4733 compliant:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(config-voi-serv)# dtmf-interworking standard
Device(config-voi-serv)# end
```

Related Commands

Command	Description
keypad-normalize	Ensures that the delay configured for a dtmf-end event is always honored.
nte-end-digit-delay	Specifies the length of delay for each digit in a dtmf-digit end event.

dtmf timer inter-digit

To configure the dual tone multifrequency (DTMF) interdigit timer for a DS0 group, use the **dtmf timer inter-digit** command in T1 controller configuration mode. To restore the timer to its default value, use the **no** form of this command.

dtmf timer inter-digit *milliseconds*
no dtmf timer inter-digit

Syntax Description

milliseconds	DTMF interdigit timer duration, in milliseconds. Range is from 250 to 3000. The default is 3000.

Command Default

3000 milliseconds

Command Modes

T1 controller configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300.

Usage Guidelines

Use the **dtmf timer inter-digit** command to specify the duration in milliseconds the router waits to detect the end of DTMF digits. After this period, the router expects no more digits to arrive and establishes the call.

Examples

The following example, beginning in global configuration mode, sets the DTMF interdigit timer value to 250 milliseconds:

```
controller T1 2
 ds0-group 2 timeslots 4-10 type e&m-fgb dtmf dnis
 cas-custom 2
 dtmf timer inter-digit 250
```

Related Commands

Command	Description
cas-custom	Customizes E1 R2 signaling parameters for a particular E1 channel group on a channelized E1 line.
ds0-group	Configures channelized T1 time slots, which enables a Cisco AS5300 modem to answer and send an analog call.

dtmf-relay (Voice over Frame Relay)

To enable the generation of FRF.11 Annex A frames for a dial peer, use the **dtmf-relay** command in dial-peer configuration mode. To disable the generation of FRF.11 Annex A frames and return to the default handling of dial digits, use the **no** form of this command.

dtmf-relay
no dtmf-relay

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
12.0(3)XG	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T, and implemented on the Cisco 7200 series router.

Usage Guidelines

Cisco recommends that this command be used with low bit-rate codecs.

When **dtmf-relay** (VoFR) is enabled, the digital signal processor (DSP) generates Annex A frames instead of passing a dual tone multifrequency (DTMF) tone through the network as a voice sample. For information about the payload format of FRF.11 Annex A frames, see the Cisco IOS Wide-Area Networking Configuration Guide.

Examples

The following example shows how to enable FRF.11 Annex A frames for VoFR dial peer 200, starting from global configuration mode:

```
dial-peer voice 200 vofr
 dtmf-relay
```

Related Commands

Command	Description
called-number (dial peer)	Enables an incoming VoFR call leg to get bridged to the correct POTS call leg when using a static FRF.11 trunk connection.
codec (dial peer)	Specifies the voice coder rate of speech for a VoFR dial peer.
connection	Specifies a connection mode for a voice port.
cptone	Specifies a regional analog voice interface-related tone, ring, and cadence setting.

Command	Description
destination-pattern	Specifies the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
preference	Indicates the preferred order of a dial peer within a rotary hunt group.
session protocol	Establishes a session protocol for calls between the local and remote routers via the packet network.
session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
signal-type	Sets the signaling type to be used when connecting to a dial peer.

dtmf-relay (Voice over IP)

To specify how an H.323 or Session Initiation Protocol (SIP) gateway relays dual tone multifrequency (DTMF) tones between telephony interfaces and an IP network, use the **dtmf-relay**command in dial peer voice configuration mode. To remove all signaling options and send the DTMF tones as part of the audio stream, use the **no** form of this command.

dtmf-relay [**cisco-rtp**] [**h245-alphanumeric**] [**h245-signal**] [**rtp-nte** [**digit-drop**]] [**sip-notify**] [**sip-info**] [**sip-kpml**]
no dtmf-relay

Syntax Description

cisco -rtp	Forwards DTMF tones by using Real-Time Transport Protocol (RTP) with a Cisco proprietary payload type.
h245 -alphanumeric	Forwards DTMF tones by using the H.245 "alphanumeric" User Input Indication method. Supports tones from 0 to 9, *, #, and from A to D.
h245 -signal	Forwards DTMF tones by using the H.245 "signal" User Input Indication method. Supports tones from 0 to 9, *, #, and from A to D.
rtp -nte	Forwards DTMF tones by using RTP with the Named Telephone Event (NTE) payload type.
digit-drop	Passes digits out-of-band and drops in-band digits. **Note** The **digit-drop**keyword is only available when the **rtp-nte** keyword is configured.
sip-info	Forwards DTMF tones using SIP INFO messages. This keyword is available only if the VoIP dial peer is configured for SIP.
sip-kpml	Forwards DTMF tones using SIP KPML over SIP SUBSCRIBE/NOTIFY messages. This keyword is available only if the VoIP dial peer is configured for SIP.
sip-notify	Forwards DTMF tones using SIP NOTIFY messages. This keyword is available only if the VoIP dial peer is configured for SIP.

Command Default

DTMF tones are disabled and sent in-band. That is, they are left in the audio stream.

Command Modes

Dial peer voice configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco AS5300.
12.0(2)XH	The **cisco-rtp**, **h245-alphanumeric**, and **h245-signal**keywords were added.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.0(7)XK	This command was first supported for VoIP on the MC3810.

Release	Modification
12.1(2)T	Changes made in Cisco IOS Release 12.0(7)XK were integrated into Cisco IOS Release 12.1(2)T.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series and Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.1(5)XM2	This 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 was not included in this release.
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.
12.2(15)ZJ	The **sip-notify** keyword was added.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(11)T	The **digit-drop** keyword was added.
15.3(3)M	This command was modified. The **sip-info** and **sip-kpml** keywords were added.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

DTMF is the tone generated when you press a button on a touch-tone phone. This tone is compressed at one end of a call; when the tone is decompressed at the other end, it can become distorted, depending on the codec used. The DTMF relay feature transports DTMF tones generated after call establishment out-of-band using either a standard H.323 out-of-band method or a proprietary RTP-based mechanism. For SIP calls, the most appropriate method to transport DTMF tones is RTP-NTE or SIP-NOTIFY.

This command specifies how an H.323 or SIP gateway relays DTMF tones between telephony interfaces and an IP network.

You must include one or more keywords when using this command.

To avoid sending both in-band and out-of band tones to the outgoing leg when sending IP-to-IP gateway calls in-band (rtp-nte) to out-of band (h245-alphanumeric), configure the **dtmf-relay**command using the **rtp-nte**and **digit-drop** keywords on the incoming SIP dial peer. On the H.323 side, and for H.323 to SIP calls, configure this command using either the **h245-alphanumeric** or **h245-signal** keyword.

The SIP-NOTIFY method sends NOTIFY messages bidirectionally between the originating and terminating gateways for a DTMF event during a call. If multiple DTMF relay mechanisms are enabled on a SIP dial peer and are negotiated successfully, the SIP-NOTIFY method takes precedence.

SIP NOTIFY messages are advertised in an invite message to the remote end only if the **dtmf-relay** command is set.

You can configure **dtmf-relay sip-info** only if the **allow-connections sip to sip** command is enabled at the global level.

For SIP, the gateway chooses the format according to the following priority:

1. sip-notify (highest priority)
2. rtp-nte
3. None--DTMF sent in-band

The gateway sends DTMF tones only in the format that you specify if the remote device supports it. If the H.323 remote device supports multiple formats, the gateway chooses the format according to the following priority:

1. cisco-rtp (highest priority)
2. h245-signal
3. h245-alphanumeric
4. rtp-nte
5. None--DTMF sent in-band

The principal advantage of the **dtmf-relay** command is that it sends DTMF tones with greater fidelity than is possible in-band for most low-bandwidth codecs, such as G.729 and G.723. Without the use of DTMF relay, calls established with low-bandwidth codecs may have trouble accessing automated DTMF-based systems, such as voice mail, menu-based Automatic Call Distributor (ACD) systems, and automated banking systems.



Note The **cisco-rtp** keyword supports a proprietary Cisco implementation and operates only between two Cisco 2600 series or Cisco 3600 series routers running Cisco IOS Release 12.0(2)XH or later. Otherwise, the DTMF relay feature does not function, and the gateway sends DTMF tones in-band.

- The **cisco-rtp** keyword is supported on Cisco 7200 series routers.
- The **sip-notify** keyword is available only if the VoIP dial peer is configured for SIP.
- The **digit-drop** keyword is available only when the **rtp-nte** keywordis configured.

Examples

The following example configures DTMF relay with the **cisco-rtp** keyword when DTMF tones are sent to dial peer 103:

```
dial-peer voice 103 voip
 dtmf-relay cisco-rtp
```

The following example configures DTMF relay with the **cisco-rtp** and **h245-signal** keywords when DTMF tones are sent to dial peer 103:

```
dial-peer voice 103 voip
 dtmf-relay cisco-rtp h245-signal
```

The following example configures the gateway to send DTMF in-band (the default) when DTMF tones to are sent dial peer 103:

```
dial-peer voice 103 voip
 no dtmf-relay
```

The following example configures DTMF relay with the **digit-drop** keyword to avoid both in-band and out-of band tones being sent to the outgoing leg on H.323 to H.323 or H.323 to SIP calls:

```
dial-peer voice 1 voip
 session protocol sipv2
 dtmf-relay h245-alphanumeric rtp-nte digit-drop
```

The following example configures DTMF relay with the **rtp-nte** keyword when DTMF tones are sent to dial peer 103:

```
dial-peer voice 103 voip
 dtmf-relay rtp-nte
```

The following example configures the gateway to send DTMF tones using SIP NOTIFY messages to dial peer 103:

```
dial-peer voice 103 voip
 session protocol sipv2
 dtmf-relay sip-notify
```

The following example configures the gateway to send DTMF tones using SIP INFO messages to dial peer 10:

```
dial-peer voice 10 voip
  dtmf-relay sip-info
```

Related Commands

Command	Description
notify telephone-event	Configures the maximum interval between two consecutive NOTIFY messages for a particular telephone event.

dualtone

To enter cp-dualtone configuration mode for specifying a custom call-progress tone, use the **dualtone** command in custom-cpto ne voice-class configuration mode. To configure the custom-cptone voice class not to detect a call-progress tone, use the **no** form of this command.

dualtone {**busy** | **conference** | **disconnect** | **number-unobtainable** | **out-of-service** | **reorder** | **ringback**}
no dualtone {**busy** | **conference** | **disconnect** | **number-unobtainable** | **out-of-service** | **reorder** | **ringback**}

Syntax Description

busy	Configure busy tone.
conference	Configure conference join and leave tones.
disconnect	Configure disconnect tone.
number -unobtainable	Configure number-unavailable tone.
out -of-service	Configure out-of-service tone.
reorder	Configure reorder tone.
ringback	Configure ringback tone.

Command Default

No call-progress tones are defined within the custom-cptone voice class.

Command Modes

Custom-cptone voice-class configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 and Cisco 3600 series and on the Cisco MC3810.
12.2(2)T	This command was implemented on the Cisco 1750 router and integrated into Cisco IOS Release 12.2(2)T.
12.4(11)XJ2	The **conference** keyword was added.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

The **dualtone** command enters cp-dualtone configuration mode and specifies a call-progress tone to be detected. You can specify additional call-progress tones without exiting cp-dualtone configuration mode.

Any call-progress tones that are not specified are not detected.

To delete a call-progress tone from this custom-cptone voice class, use the **no** form of this command and the keyword for the tone that should not be detected; for example, **no dualtone busy**.

You must associate the class of custom call-progress tones with a voice port for this command to affect tone detection.

Use the **dualtone conference** command to define custom join and leave tones for hardware conferences.

Examples

The following example enters cp-dualtone configuration mode and specifies busy tone and ringback tone in the custom-cptone voice class country-x:

```
Router(config)# voice class custom-cptone country-x
Router(cfg-cptone)# dualtone busy
Router(cfg-cp-dualtone)# frequency 440 480
Router(cfg-cp-dualtone)# cadence 500 500
Router(cfg-cp-dualtone)# exit
Router(cfg-cptone)# dualtone ringback
Router(cfg-cp-dualtone)# frequency 400 440
Router(cfg-cp-dualtone)# cadence 2000 4000
```

The following example deletes ringback tone from the custom-cptone voice class country-x:

```
Router(config)# voice class custom-cptone country-x
Router(cfg-cptone)# no dualtone ringback
```

The following example configures a conference leave tone. The configured leave tone must be associated with a digital signal processor (DSP) farm profile:

```
Router(config)# voice class custom-cptone leavetone
Router(cfg-cptone)# dualtone conference
Router(cfg-cp-dualtone)# frequency 500 500
Router(cfg-cp-dualtone)# cadence 100 100 100 100 100
```

Related Commands

Command	Description
cadence	Defines the tone on and off durations for a call-progress tone.
conference-join custom-cptone	Defines a custom call-progress tone to indicate joining a conference.
conference-leave custom-cptone	Defines a custom call-progress tone to indicate leaving a conference.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
frequency	Defines the frequency components for a call-progress tone.
supervisory custom-cptone	Associates a class of custom call-progress tones with a voice port.
voice class custom-cptone	Creates a voice class for defining custom call-progress tones.



E

- e164, on page 143
- e911, on page 144
- early-offer, on page 145
- early-media update block, on page 147
- echo-cancel comfort-noise, on page 148
- echo-cancel compensation, on page 149
- echo-cancel coverage, on page 150
- echo-cancel enable, on page 152
- echo-cancel enable (controller), on page 154
- echo-cancel erl worst-case, on page 155
- echo-cancel loopback, on page 156
- echo-cancel mode, on page 157
- echo-cancel suppressor, on page 158
- element, on page 159
- emergency, on page 160
- emptycapability, on page 161
- emulate cisco h323 bandwidth, on page 162
- encap clear-channel standard, on page 164
- encapsulation atm-ces, on page 166
- encoding h450 call-identity, on page 167
- encoding h450 call-identity itu, on page 169
- encryption, on page 170
- endpoint alt-ep collect, on page 172
- endpoint alt-ep h323id, on page 174
- endpoint circuit-id h323id, on page 176
- endpoint max-calls h323id, on page 177
- endpoint naming, on page 178
- endpoint resource-threshold, on page 179
- endpoint ttl, on page 180
- erase vfc, on page 181
- error-category, on page 182
- error-code-override, on page 184
- error-correction, on page 187

- error-passthru, on page 189
- event-log, on page 190
- event-log (Privileged EXEC), on page 192
- event-log dump ftp, on page 194
- event-log error-only, on page 197
- event-log max-buffer-size, on page 198
- expect-factor, on page 200
- extsig mgcp, on page 202

e164

To configure the content of an E.164 pattern map, use the **e164** command in the voice class e164 pattern map mode. To remove the configuration from the content of an E.164 pattern map, use the **no** form of this command.

e164 *pattern*
no e164 *pattern*

Syntax Description

pattern	A full E.164 telephone number prefix.

Command Default

The content of an E.164 pattern map is not configured.

Command Modes

Voice class e164 pattern map configuration (config-voice class e164-pattern-map)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

You can create an E.164 pattern map in dial peer configuration mode before configuring the content of an E.164 pattern map in voice class E.164 pattern map mode. You must use the correct format of the E.164 pattern number when you add an E.164 pattern entry to a destination E.164 pattern map. You can also add multiple destination E.164 patterns to a pattern map.

Note When both incoming and outgoing dial peers are configured with **calling e164-pattern-map**, it's essential to apply a provision policy to the incoming dial peer to avoid call failures.

Examples

The following example shows how an E.164 pattern entry is configured on a destination E.164 pattern map:

```
Device(config)# voice class e164-pattern-map
Device(config-voice class e164-pattern-map)# e164 605
```

Related Commands

Command	Description
destination e164-pattern-map	Links an E.164 pattern map to a dial peer.
show voice class e164-pattern-map	Displays the information of the configuration of an E.164 pattern map.
url	Specifies the URL of a text file that has E.164 patterns configured on a destination E.164 pattern map.

e911

To enable E911 system services for SIP on the VoIP dial peer, use the **e911**command in voice service voip-sip configuration mode. To disable SIP E911 functionality, use the **no** form of this command.

e911
no e911

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Voice service voip-sip configuration (conf-serv-sip)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

The **no** form of the command disables E911 functionality from a global perspective. Output from the **show running-config** command shows whether E911 is configured. See also the **voice-class sip e911** and **debug csm neat** commands.

Examples

The following example enables E911 services in voice service VoIP SIP configuration mode:

```
Router# configure terminal
Router(config-term)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# e911
```

The following example disables E911 functionality:

```
Router(conf-serv-sip)# no e911
```

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 current configuration information.
voice-class sip e911	Configures e911 services on the voice dial peer.

early-offer

To force a Cisco Unified Border Element (Cisco UBE) to send a SIP invite with Early-Offer (EO) on the Out-Leg (OL), use the **early-offer** command in SIP, voice class tenant configuration mode, or dial peer configuration mode. To disable Early-Offer, use the **no** form of this command.

early-offer forced [**renegotiate** | [**always**]] **[system]**
no early-offer forced[**renegotiate** | [**always**]] **[system]**

Syntax Description

forced	Forcefully sends Early-Offer on the SIP Out-Leg.
renegotiate	Triggers a Delayed-Offer Re-invite to exchange complete media capability if the negotiated codecs are one of the following: • aaclld - Audio codec AACLD 90000 bps • h263 - Video codec H263 • h263+ - Video codec H263+ • h264 - Video codec H264 • mp4a - Wideband audio codec
always	Always triggers a Delayed-Offer Re-invite to exchange complete media capabilities.
system	Specifies that Early-Offer 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. The Cisco UBE does not distinguish SIP Delayed-Offer to Early-Offer call flows.

Command Modes

Voice service VoIP configuration (conf-serv-sip).

Dial-peer configuration (config-dial-peer).

Voice class tenant configuration (config-class).

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.
15.4(2)T, Cisco IOS XE Release 3.12S	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use this command to forcefully configure a Cisco UBE to send a SIP invite with EO on the Out-Leg (OL), Delayed-Offer to Early-Offer for all VoIP calls, SIP audio calls, or individual dial peers.

Examples

The following example shows SIP Early-Offer invites being configured globally:

```
Router(conf-serv-sip)# early-offer forced
```

The following example shows SIP Early-Offer invites being configured per dial peer:

```
Router(config-dial-peer)# voice-class sip early-offer forced
```

The following example shows SIP Early-Offer invites being in the voice class tenant configuration mode:

```
Router(config-class)# early-offer forced system
```

early-media update block

To block the UPDATE requests with SDP in an early dialog, use **early-media update block** command in global VoIP SIP configuration mode or voice class tenant configuration mode. To disable, use **no** form of this command.

early-media update block [**re-negotiate** | **system**]
no 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.
system	Specifies that the Early Dialog UPDATE requests 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

CUBE allows pass-through of early dialog UPDATE requests from one user agent to the other.

Command Modes

SIP configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

Command History

Release	Modification
Cisco IOS 15.5(3)M, Cisco IOS-XE 3.16S	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 Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

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 global voip sip configuration mode:

```
Router(conf-serv-sip)# early-media update block
```

The following example shows early dialog update block being configured in voice class tenant configuration mode:

```
Router(conf-class)# early-media update block system
```

echo-cancel comfort-noise

To specify that background noise be generated, use the **echo-cancel comfort-noise** command in controller configuration mode. To disable this feature, use the **no** form of this command.

echo-cancel comfort-noise
no echo-cancel comfort-noise

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

Use the **echo-cancel comfort-noise** command to generate background noise to fill silent gaps during calls if voice activated dialing (VAD) is activated. If comfort noise is not enabled and VAD is enabled at the remote end of the connection, the user hears nothing or silence when the remote party is not speaking.

The configuration of comfort noise affects only the silence generated at the local interface; it does not affect the use of VAD on either end of the connection or the silence generated at the remote end of the connection.

For the OC-3/STM-1 ATM Circuit Emulation Service network module, echo cancellation must be enabled.

Examples

The following example enables comfort noise on a T1 controller:

```
controller T1 0/0
 echo-cancel enable
 echo-cancel comfort-noise
```

Related Commands

Command	Description
echo-cancel enable (controller)	Enables echo cancellation on a voice port.
voice port	Specifies which port is used for voice traffic.

echo-cancel compensation

To set attenuation for loud signals, use the **echo-cancel compensation** command in controller configuration mode. To disable this feature, use the **no** form of this command.

echo-cancel compensation
no echo-cancel compensation

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

Use the **echo-cancel compensation** command to add attenuation control to the T1 or E1 controller. When this command is enabled, 6 decibels of attenuation are inserted if the signal level from the receive direction is loud. When loud signals are not received, the attenuation is removed.

For the OC-3/STM-1 ATM Circuit Emulation Service network module, echo cancellation must be enabled.

Examples

The following example enables attenuation control on a T1 controller:

```
controller T1 0/0
 echo-cancel enable
 echo-cancel compensation
```

Related Commands

Command	Description
echo-cancel enable (controller)	Enables echo cancellation on a voice port.
voice port	Specifies which port is used for voice traffic.

echo-cancel coverage

To adjust the size of the echo canceller (EC) and to select the extended EC when the Cisco default EC is present, use the **echo-cancel coverage** command in voice-port configuration mode. To reset this command to the default value (128 milliseconds [ms]), use the **no** form of this command.

echo-cancel coverage {**24** | **32** | **48** | **64** | **80** | **96** | **112** | **128**}
no echo-cancel coverage

Syntax Description

24	EC size of 24 ms.
32	EC size of 32 ms.
48	EC size of 48 ms.
64	EC size of 64 ms.
80	EC size of 80 ms.
96	EC size of 96 ms.
112	EC size of 112 ms.
128	EC size of 128 ms. This is the default.

Command Default

This command is enabled by default, and echo cancellation is set to 128 ms.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA	This command was implemented on the Cisco MC3810.
12.0(5)XK	The command was modified to add the 8-ms option.
12.0(5)XE	The command was implemented on the Cisco 7200 series.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(13)T	This command was modified to provide a new set of size options when the extended EC is configured. This command is supported on all T1 Digital Signal Processor (DSP) platforms.
12.3(11)T	This command was modified for use on NextPort platforms for use with the dual-filter G.168 echo canceller.
12.4(20)T	This command was modified to expand the values for echo cancellation to include 80, 96, 112, and 128 ms. The default was changed from 64 to 128 ms.

Usage Guidelines

Use the **echo-cancel coverage** command to adjust the coverage size of the EC. This command enables cancellation of voice that is sent out the interface and received on the same interface within the configured amount of time. If the local loop (the distance from the interface to the connected equipment that is producing the echo) is greater than this amount of time, the configured value of this command should be increased.

If you configure a greater value for this command, the EC takes longer to converge. In this case, you might hear a slight echo when the connection is initially set up. If the configured value for this command is too short, you might hear some echo for the duration of the call because the EC is not canceling the longer delay echoes.

There is no echo or echo cancellation on the network side (for example, the non-POTS side) of the connection.



Note This command is valid only if the echo cancellation feature has been enabled. For more information, see the **echo-cancel enable** command.

Beginning with Cisco IOS Release 12.4(20)T, the NextPort dual-filter G.168 echo canceller supports echo tails from 24-ms to 128-ms in 16-ms increments. The **echo-cancel coverage** command limits the echo canceller coverage to 128-ms on NextPort platforms. For backward compatibility, a voicecap used in "raw mode" will still configure older SPEware to settings greater than 64-ms when used with newer releases of Cisco IOS software. For situations when new SPEware is loaded onto an older Cisco IOS release, the NextPort dual-filter G.168 echo canceller automatically sets coverage time to 64 ms.

Examples

The following example enables the extended echo cancellation feature and adjusts the size of the echo canceller to 80 milliseconds:

```
Router (config-voiceport)# echo-cancel enable
Router (config-voiceport)# echo-cancel coverage 80
```

Related Commands

Command	Description
echo-cancel enable (controller)	Enables echo cancellation on a controller.
echo-cancel enable	Enables echo cancellation on a voice port.

echo-cancel enable

To enable the cancellation of voice that is sent out the interface and received back on the same interface, use the **echo-cancel enable**command in voice-port configuration mode or global configuration mode. To disable echo cancellation, use the **no** form of this command.

echo-cancel enable type [**hardware** | **software**]
no echo-cancel enable

Syntax Description

hardware	(Optional) Specifies that echo cancellation is enabled via the hardware on the network module.
software	(Optional) Specifies that echo cancellation is enabled via command-line interface entries.
Note The **hardware** and **software** keywords are available only when the optional hardware echo cancellation module is installed on the multiflex VWIC.	

Command Default

The Cisco-proprietary G.168 echo canceller (EC) is enabled with the echo suppressor turned off.

Command Modes

Voice-port configuration (config-voiceport)
Global configuration (config)

Command History

Release	Modification
11.3(1)T	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. This command was implemented on all TI digital signal processor (DSP) platforms.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T and the optional **hardware** and **software** keywords were added.

Usage Guidelines

The **echo-cancel enable**command enables cancellation of voice that is sent out the interface and received back on the same interface; sound that is received back in this manner is perceived by the listener as an echo. Disabling echo cancellation might cause the remote side of a connection to hear an echo. Because echo cancellation is an invasive process that can minimally degrade voice quality, this command should be disabled if it is not needed.

Typically a hybrid circuit can provide greater than 6 decibels (dB) echo return loss (ERL), so the extended EC is configured to handle 6 dB in the worst case by default. However, if a measurement shows that a circuit can provide only 6 dB ERL or less, the extended EC can be configured to use this lower rate.

The Cisco G.168 EC is enabled by default with the echo suppressor turned off. The echo suppressor can be turned on only when the default Cisco G.168 EC is used. The **echo-cancel suppressor** command used with the Cisco default EC is still visible when the extended EC is selected, but it does not do anything.

The **echo-cancel enable**command does not affect the echo heard by the user on the analog side of the connection.

There is no echo path for a 4-wire receive and transmit interface (also called ear and mouth and abbreviated as E&M). The echo canceller should be disabled for that interface type.



Note This command is valid only when the **echo-cancel coverage**command has been configured.

Examples

The following example enables the extended echo cancellation feature in voice-port configuration mode:

```
Router (config-voiceport)# echo-cancel enable
```

The following example enables the extended echo cancellation feature on the Cisco 1700 series or Cisco ICS7750 in global configuration mode:

```
Router (config)# echo-cancel enable
```

Related Commands

Command	Description
echo-cancel coverage	Specifies the amount of coverage for echo cancellation.
echo-cancel enable (controller)	Enables echo cancellation on a controller.
echo-cancel suppressor	Enables echo suppression to reduce initial echo before the echo canceller converges.
non-linear	Enables nonlinear processing in the echo canceler.

echo-cancel enable (controller)

To enable the echo cancel feature, use the **echo-cancel enable** command in controller configuration mode. To disable this feature, use the **no** form of this command.

echo-cancel enable
no echo-cancel enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled for all interface types

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

The **echo-cancel enable** command enables cancellation of voice that is sent out of the interface and received back on the same interface. Disabling echo cancellation might cause the remote side of a connection to hear an echo. Because echo cancellation is an invasive process that can minimally degrade voice quality, this command should be disabled if it is not needed.

The **echo-cancel enable**command does not affect the echo heard by the user on the analog side of the connection.

Note This command is valid only if the **echo-cancel coverage** command has been configured.

Examples

The following example enables the echo cancel feature on a T1 controller:

```
controller T1 0/0
 echo-cancel enable
 echo-cancel coverage 32
```

Related Commands

Command	Description
echo-cancel coverage	Specifies the amount of coverage for echo cancellation.
echo-cancel enable	Enables echo cancellation on a voice port.
non-linear	Enables nonlinear processing in the echo canceler.
voice port	Configures the voice port.

echo-cancel erl worst-case

To determine worst-case Echo Return Loss (ERL) in decibels (dB), use the **echo-cancel erl worst-case** command in voice-port configuration mode. To disable the command, use the **no** form.

echo-cancel erl worst-case {**6** | **3** | **0**}
no echo-cancel erl worst-case {**6** | **3** | **0**}

Syntax Description

6 | **3** | **0**	Values of 6, 3, or 0 dB ERL in the extended echo canceller (EC). The default is 6.

Command Default

Enabled at 6 dB when the extended G.168 EC is used

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This command is used only when the extended EC is present and is not supported with the Cisco proprietary-G.165 EC. This command predicts the worst-case ERL that the EC might encounter.

Examples

The following example shows a worst-case ERL of 3:

```
Router(config-voiceport)# echo-cancel erl worst-case 3
```

To check the configuration, enter the **show voice port**command in privileged EXEC mode:

```
Router# show voice port
.
.
Echo Cancel worst case ERL is set to 6 dB
Playout-delay Mode is set to adaptive
.
.
```

Related Commands

Command	Description
echo-cancel enable	Enables the cancellation of voice that is sent out and received on the same interface.

echo-cancel loopback

To place the echo cancellation processor in loopback mode, use the **echo-cancel loopback** command in controller configuration mode. To disable loopback of the echo cancellation processor, use the **no** form of this command.

echo-cancel loopback
no echo-cancel loopback

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

Use an **echo-cancel loopback**test on lines to detect and distinguish equipment malfunctions caused by either the line or the interface. If correct echo cancellation is not possible when an interface is in loopback mode, the interface is the source of the problem.

Examples

The following example sets up echo cancellation loopback diagnostics:

```
controller T1 0/0
 echo-cancel enable
 echo-cancel coverage 32
 echo-cancel loopback
```

Related Commands

Command	Description
echo-cancel enable (controller)	Enables echo cancellation on a controller.

echo-cancel mode

To enable echo cancel mode on the extended G.168 echo canceller, use the **echo-cancel mode** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

echo-cancel mode {**1** | **2**}
no echo-cancel mode

Syntax Description

1	Enables fast convergence for multiple echo reflectors and applies 0 dB Sin gain and 0 dB Sout gain.
2	Enables fast convergence for multiple echo reflectors and improves double-talk detection by applying 6 dB Sin gain and -6 dB Sout gain.

Command Default

No default behavior or values.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.3(7)	This command was introduced.

Usage Guidelines

This command enables an operation mode to improve echo canceller (EC) performance in systems that have multiple echo reflectors and double-talk caused by low volume. When this command is enabled, the extended EC cancels the echo better in multiple echo reflector scenarios, which occur most often in analog interfaces.

This command is available only if the extended G.168 echo canceller is enabled for the voice port.

If you select mode **2**, set the **echo-cancel erl worst-case** command to 0.

Examples

The following example sets the extended G.168 EC mode to 1 on a Cisco 1700 series router:

```
Router(config)# voice-port 1/0/1
Router(config-voiceport)# echo-cancel mode 1
```

Related Commands

Command	Description
echo-cancel coverage	Adjusts the size of the echo canceller.
echo-cancel enable	Enables echo cancellation for voice that is sent and received on the same interface.
echo-cancel erl worst-case	Determines worst-case ERL.

echo-cancel suppressor

To enable echo suppression to reduce initial echo before the echo canceller converges, use the **echo-cancel suppressor** command in voice-port configuration mode. To disable echo suppression, use the **no** form of this command.

echo-cancel suppressor *seconds*
no echo-cancel suppressor

Syntax Description

seconds	Suppressor coverage, in seconds. Range is from 1 to 10. Default is 7.

Command Default

No default behavior or values.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This command is used only when the echo canceller is enabled. In case of double-talk in the first number of seconds, the code automatically disables the suppressor.

Examples

The following example shows echo suppression configured for a suppression coverage of 9 seconds:

```
Router(config-voiceport)# echo-cancel suppressor 9
```

Related Commands

Command	Description
echo-cancel enable	Enables the cancellation of voice that is sent out and received on the same interface.

element

To define component elements of local or remote clusters, use the **element** command in gatekeeper configuration mode. To disable component elements of local or remote clusters, use the **no** form of this command.

element *gatekeeper-name ip-address* [*port*]
no element *gatekeeper-name ip-address* [*port*]

Syntax Description

gatekeeper -name	Name of the gatekeeper component to be added to the local or remote cluster.
ip -address	IP address of the gatekeeper to be added to the local or remote cluster.
port	(Optional) Registration, Admission, and Status (RAS) signaling port number for the remote zone. Range is from 1 to 65535. Default is the well-known RAS port number 1719.

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 the Cisco AS5850.

Examples

The following example places the SampleGK gatekeeper into the specified local or remote cluster:

```
element SampleGK 172.16.204.158 1719
```

Related Commands

Command	Description
zone cluster local	Defines a local grouping of gatekeepers, including the gatekeeper that you are configuring.
zone cluster remote	Defines a remote grouping of gatekeepers, including the gatekeeper that you are configuring.

emergency

Configure List of Emergency Numbers. Use the **no** form of this command to disable this feature.

emergency *LINE*
no emergency *LINE*

Syntax Description

LINE	List of numbers separated by '' SPACE.

Command Default

Not enabled by default.

Command Modes

voice service voip.

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 to get the emergency numbers configured.

Examples

```
Router(conf-voi-serv)#emergency 123 456 919465 915566
Router(conf-voi-serv)#
```

Related Commands

Command	Description

emptycapability

To eliminate the need for identical codec capabilities for all dial peers in the rotary group, use the **emptycapability** command in h.323 voice-service configuration mode. To return to the default configuration, use the **no** form of this command.

emptycapability
no emptycapability

Syntax Description

There are no keywords or arguments for this command.

Command Default

Identical codec capabilities are required on all dial peers.

Command Modes

Voice service H.323 configuration (conf-serv-h323)

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

The default dial-peer configuration requires that all members of a hunt group must have the same codec configured to complete calls. Configuring **emptycapability** on the IP-to-IP gateway (IPIPGW) eliminates the need for identical codec capabilities for all dial peers in the rotary group, and allows the IPIPGW to restart the codec negotiation end-to-end.

Note If extended caps (DTMF or T.38) are configured on the outgoing gateway or the trunking gateway, extended caps must be configured in both places.

Examples

The following example shows emptycapability being configured to allow the IPIPGW to restart codec negotiation from end-to-end regardless of codec configured on each endpoint:

```
Router(conf-serv-h323)# emptycapability
```

Related Commands

Command	Description
h323	Enters H.323 voice service configuration mode.

emulate cisco h323 bandwidth

To instruct the H.323 gateway to use H.323 version 2 behavior for bandwidth management, use the **emulate cisco h323 bandwidth** command in gateway configuration mode. To instruct the gateway to use H.323 version 3 behavior for bandwidth management, use the **no** form of the command.

emulate cisco h323 bandwidth
no emulate cisco h323 bandwidth

Syntax Description

This command has no keywords or arguments.

Command Default

No default behaviors or values

Command Modes

Gateway configuration (config-gateway)

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(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

Prior to Cisco IOS Release 12.2(2)XA, gateway calls were always reported to require a bandwidth of 64 kbps, the unidirectional bandwidth for a Cisco G.711 codec. If the endpoints in the call chose to use a more efficient codec, this was not reported to the Cisco gatekeeper.

In the version of the Cisco H.323 gateway in Cisco IOS Release 12.2(2)XA or later releases (which conform with H.323 version 3), the reported bandwidth is bidirectional. Initially, 128 kbps is reserved. If the endpoints in the call select a more efficient codec, the Cisco gatekeeper is notified of the bandwidth change.

For backward compatibility, the **emulate cisco h323 bandwidth** command allows devices running Cisco IOS Release 12.2(2)XA and later to conform to the H.323 version 2 bandwidth reporting implementation.

Examples

The following example shows that the router emulates the behavior of a Cisco H.323 version 2 gateway.

```
Router(config-gateway)# emulate cisco h323 bandwidth
```

Related Commands

Command	Description
bandwidth	Specifies the maximum aggregate bandwidth for H.323 traffic from a zone to another zone, within a zone, or for a session in a zone.
bandwidth remote	Specifies the total bandwidth for H.323 traffic between this gatekeeper and any other gatekeeper.

Command	Description
gateway	Enables gateway configuration commands.

encap clear-channel standard

To globally enable RFC 4040-based clear-channel codec negotiation for Session Initiation Protocol (SIP) calls on a Cisco IOS voice gateway or Cisco Unified Border Element (Cisco UBE), use the **encap clear-channel standard** command in voice service SIP configuration mode or voice class tenant configuration mode. To disable RFC 4040-based clear-channel codec negotiation for SIP calls globally on a Cisco IOS voice gateway or Cisco UBE, use the **no** form of this command.

encap clear-channel standard system
no encap clear-channel standard system

Syntax Description

standard	Specifies standard RFC 4040 encapsulation.
system	Specifies that the RFC 4040-based clear-channel codec negotiation for SIP calls 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--legacy encapsulation [X-CCD/8000] is used for clear-channel codec negotiation.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

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.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**.

Usage Guidelines

Use the **encap clear-channel standard** command in voice service SIP configuration mode to globally enable RFC 4040-based clear-channel codec negotiation [CLEARMODE/8000] for SIP calls on a Cisco IOS voice gateway or Cisco UBE. RFC 4040-based clear-channel codec negotiation allows 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 **encap clear-channel standard** command is enabled on a Cisco IOS voice gateway or Cisco UBE, calls using the Cisco IOS clear channel codec are translated into calls that use CLEARMODE/8000 so that the calls do not get rejected when they reach third-party SIP gateways.

To enable RFC 4040-based clear-channel codec negotiation for SIP calls on an individual dial peer, overriding the global configuration for the Cisco IOS voice gateway or Cisco UBE, use the **voice-class sip encap clear-channel standard** command in dial peer voice configuration mode. To globally disable RFC 4040-based clear-channel codec negotiation on a Cisco IOS voice gateway or Cisco UBE, use the **no encap clear-channel standard** command in voice service SIP configuration mode.

Examples

The following example shows how to enable RFC 4040-based clear-channel code negotiation globally for all dial peers on a Cisco IOS voice gateway or Cisco UBE:

```
Router> enable
Router# configure
 terminal
Router(config)# voice
 service
 voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# encap clear-channel standard
```

The following example shows how to enable RFC 4040-based clear-channel code negotiation globally in the voice class tenant configuration mode:

```
Router(config-class)# encap clear-channel system
```

Related Commands

Command	Description
voice-class sip encap clear-channel	Enables RFC 4040-based clear-channel codec negotiation for SIP calls on an individual dial peer on a Cisco IOS voice gateway or Cisco UBE.

encapsulation atm-ces

To enable circuit emulation service (CES) ATM encapsulation, use the **encapsulation atm-ces** command in interface configuration mode. To disable CES ATM encapsulation, use the **no** form of this command.

encapsulation atm-ces
no encapsulation atm-ces

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0	This command was integrated into Cisco IOS Release 12.0.

Usage Guidelines

This command is supported only on serial ports 0 and 1.

Examples

The following example enables CES ATM encapsulation on serial port 0:

```
interface serial 0
 encapsulation atm-ces
```

Related Commands

Command	Description
ces cell-loss-integration-period	Sets the CES cell-loss integration period.
ces clockmode synchronous	Configures the ATM CES synchronous clock mode.
ces connect	Maps the CES service to an ATM PVC.
ces initial-delay	Configures the size of the receive buffer of a CES circuit.
ces max-buf-size	Configures the send buffer of a CES circuit.
ces partial-fill	Configures the number of user octets per cell for the ATM CES.
ces service	Configures the ATM CES type.

encoding h450 call-identity

To set the Abstract Syntax Notation (ASN) Packed Encoding Rules (PER) format used for encoding and decoding the H.450 protocol data units (PDUs), use the **encoding h450 call-identity** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

encoding h450 call-identity {**cisco** | **itu**}
no encoding h450 call-identity

Syntax Description

cisco	Gateway uses a PER encoding format that is not compliant with ITU-T X.691 for encoding or decoding the H.450.2 callIdentity field.
itu	Gateway uses a PER encoding format that is compliant with ITU-T X.691 for encoding or decoding the H.450.2 callIdentity field.

Command Default

Cisco encoding is enabled at the global (voice-service configuration) level.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.3(7)T3	This command was integrated into Cisco IOS Release 12.3(7)T3.

Usage Guidelines

Use this command to set the encoding format in the voice-class assigned to individual dial peers. By default, Cisco encoding is enabled globally. However, Cisco encoding for the H.450.2 callIdentity field is not compliant with ITU-T X.691 and can cause interoperability problems with third-party devices during H.450.2 call transfer with consultation. Use the **itu**keyword to configure ITU-T X.691 encoding in the dial peer.

Use the **itu** keyword to set ITU-T X.691 encoding globally on the Cisco voice gateway. By default, Cisco encoding is enabled. However, Cisco encoding for the H.450.2 callIdentity field is not compliant with ITU-T X.691 and could cause interoperability problems with third-party devices during H.450.2 call transfer with consultation.



Note The **encoding h450 call-identity**command in voice-class configuration mode takes precedence over the **ncoding h450 call-identity itu**command.

Examples

The following example shows X.691-compliant encoding being enabled for the H.450-2 PDUs for calls on dial-peer 4:

```
voice class h323 1
 encoding h450 call-identity itu
dial-peer voice 4 voip
 voice-class h323 1
```

The following example enables Cisco encoding, which is not compliant with ITU-T X.691, on dial-peer 5:

```
voice class h323 1
 encoding h450 call-identity cisco
dial-peer voice 5 voip
 voice-class h323 1
```

By entering the **no encoding h450 call-identity** command in voice-class configuration mode, the following example shows the encoding for calls only on dial-peer 7 being reset to the global configuration. However, the **no encoding h450 call-identity** configuration is not displayed in the running configuration:

```
voice class h323 1
 no encoding h450 call-identity
dial-peer voice 7 voip
 voice-class h323 1
```

The following example illustrates a typical use case when the ITU-T encoding is configured for all the dial peers except dial-peer 4; dial-peer 4 uses Cisco encoding:

```
voice service voip
 h323
  encoding h450 call-identity itu
voice class h323 1
   encoding h450 call-identity cisco
dial-peer voice 1 voip
 destination-pattern 1..
dial-peer voice 2 voip
 destination-pattern 2..
dial-peer voice 3 voip
 destination-pattern 3..
dial-peer voice 4 voip
 destination-pattern 4..
 voice-class h323 1
```

The following example shows all dial-peers with the ITU-T X.691 being globally configured:

```
voice service voip
 h323
 encoding h450 call-identity itu
```

Related Commands

Command	Description
encoding h450 call-identity itu	Sets the ASN PER format used for encoding and decoding the H.450 PDUs.
voice class h323	Enters voice-class configuration mode and creates a voice class for H.323 attributes.

encoding h450 call-identity itu

To set the Abstract Syntax Notation (ASN) Packed Encoding Rules (PER) format used for encoding and decoding the H.450 protocol data units (PDUs), use the **encoding h450 call-identity itu**command in voice-service configuration mode. To reset to the default, use the **no** form of this command.

encoding h450 call-identity itu
no encoding h450 call-identity

Syntax Description

This command has no argument or keywords.

Command Default

Cisco encoding enabled globally

Command Modes

Voice-service configuration (config-voi-serv)

Command History

Release	Modification
12.3(11)T	This command was introduced on Cisco voice gateways.
12.3(7)T3	This command was integrated into Cisco IOS release 12.3(7)T3.

Usage Guidelines

Use this command to set ITU X.691 encoding globally on the Cisco voice gateway. By default, Cisco encoding is enabled. However, Cisco encoding for the H.450.2 callIdentity field is not compliant with ITU X.691 and could cause interoperability problems with third-party devices during H.450.2 call transfer with consultation.



Note The **encoding h450 call-identity**command in voice-class configuration mode takes precedence over this command.

Examples

The following example globally configures all dial-peers with the ITU X.691:

```
voice service voip
 h323
 encoding h450 call-identity itu
```

Related Commands

Command	Description
encoding h45 call-identity	Sets the Abstract Syntax Notation (ASN) Packed Encoding Rules (PER) format used for encoding and decoding the H.450 protocol data units (PDUs).
voice service voip	Enters voice-service configuration mode.

encryption

To set the algorithm to be negotiated with the provider, use the **encryption** command in settlement configuration mode. To reset to the default encryption method, use the **no** form of this command.

encryption {**des-cbc-sha** | **des40-cbc-sha** | **dh-des-cbc-sha** | **dh-des40-cbc-sha** | **null-md5** | **null-sha** | **all**}
no encryption {**des-cbc-sha** | **des40-cbc-sha** | **dh-des-cbc-sha** | **dh-des40-cbc-sha** | **null-md5** | **null-sha** | **all**}

Syntax Description

des -cbc-sha	Encryption type ssl_rsa_with_des_cbc_sha cipher suite.
des40 -cbc-sha	Encryption type ssl_rsa_export_with_des40_cbc_sha cipher suite.
dh -des-cbc-sha	Encryption type ssl_dh_rsa_with_des_cbc_sha cipher suite.
dh -des40-cbc-sha	Encryption type ssl_dh_rsa_export_with_des40_cbc_sha cipher suite.
null -md5	Encryption type ssl_rsa_with_null_md5 cipher suite.
null -sha	Encryption type ssl_rsa_with_null_sha cipher suite.
all	All encryption methods are used in the Secure Socket Layer (SSL).

Command Default

The default encryption method is **all**. If none of the encryption methods is configured, the system uses all of the encryption methods in the SSL session negotiation.

Command Modes

Settlement configuration (config-settlement)

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

For Cisco IOS Release 12.0(4)XH1, only one encryption method is allowed for each provider.

Examples

The following example shows the algorithm being set to be negotiated with the provider, using the **encryption** command:

```
settlement 0
 encryption des-cbc-sha
```

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
customer-id	Sets the customer identification.

Command	Description
device-id	Sets the device identification.
max-connection	Sets the maximum number of 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	Disables the settlement provider.
type	Specifies the provider type.
url	Specifies the ISP address.

endpoint alt-ep collect

To configure the collection of alternate routes to endpoints, use the **endpoint alt-ep collect**command in gatekeeper configuration mode. To disable alternate route collection, use the **no** form of this command.

endpoint alt-ep collect *number-or-alternate-routes* [**distribute**]
no endpoint alt-ep collect

Syntax Description

number-or-alternate-routes	Number of alternate routes to endpoints for the gatekeeper to collect before ending the collection process and sending the Location Confirmation (LCF) message to the requesting endpoint. Range for the *number-or-alternate-routes*argument is from 1 to 20. The default is 0, which indicates that alternate route collection is not enabled.
distribute	(Optional) Causes the gatekeeper to include alternate routes from as many LCF messages as possible in the consolidated list. Use of this keyword allows the gatekeeper to give fairness to the information of alternate routes present in various LCF messages. **Note** Identical alternate endpoints are removed from the list. That is, if an alternate endpoint received in an LCF message has an identical IP address or trunk group label or carrier ID as any alternate endpoints received in previous LCF messages, the previous duplicate alternate endpoints are removed from the consolidated list.

Command Default

The default value for the *number-or-alternate-routes*argument is 0, which indicates that alternate route collection is not enabled.

Command Modes

Gatekeeper configuration (config-gk)

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(8)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	Duplicate alternate endpoints received in an LCF message were removed from the consolidated list of endpoints. This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

Use this command to force the gatekeeper to collect a specified number of alternate routes to endpoints and to create a consolidated list of those alternate routes to report back to the requesting endpoint.

Examples

The following example shows that 15 alternate routes to endpoints should be collected:

```
Router(config-gk)# endpoint alt-ep collect 15
```

Related Commands

Command	Description
endpoint alt-ep h323id	Configures an alternate endpoint on a gatekeeper, including endpoint ID, IP address, port, and trunk group label or carrier-ID information.
show gatekeeper endpoints alternates	Displays information about alternate endpoints.

endpoint alt-ep h323id

To configure alternate endpoints, use the **endpoint alt-ep h323id**command in gatekeeper configuration mode. To disable alternate endpoints, use the **no** form of this command.

endpoint alt-ep h323id *h323-id ip-address* [*port-number*] [**carrier-id** *carrier-name*]
no endpoint alt-ep h323id

Syntax Description

h323 -id	H.323 name (ID) of the endpoint for which an alternate address is being supplied. This ID is used by a gateway when the gateway communicates with the gatekeeper. Usually, this H.323 ID is the name given to the gateway, with the gatekeeper domain name appended to the end.
ip -address	IP address of an alternate for this endpoint.
port -number	(Optional) Port number associated with the address of the alternate. Default is 1720.
carrier -id *carrier-name*	(Optional) Trunk group label or carrier ID of the alternate endpoint. It may be added in addition to the IP address of the alternate endpoint. The *carrier-name* argument is the name of the trunk group label or circuit ID.

Command Default

The default port number is 1720.

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 the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and the **carrier-id** keyword and *carrier-name* argument were added.

Usage Guidelines

This command defines the IP address for an alternate endpoint for the primary endpoint identified by its H.323 ID. The IP address is returned in the alternate endpoint field whenever the primary endpoint is returned in an Admission Confirmation (ACF) or Location Confirmation (LCF) message. The alternate endpoint provides an alternate address to which a call can be placed if a call to the primary endpoint fails.

This command provides a failover mechanism if a gateway becomes disabled for a period of time before the gatekeeper becomes aware of the problem. After receiving an ACF message from the gatekeeper with an alternate endpoint list, the Cisco gateway may attempt to use an alternate address if a SETUP message results in no reply from the destination. This command causes the alternate endpoints specified in the *h323-id* argument to be sent in all subsequent ACF and LCF messages. Gatekeepers that support the **endpoint alt-ep h323id** command can also send alternate endpoint information in Registration, Admissions, and Status (RAS) messages. The gatekeeper accepts IP, port call signal address, and trunk group ID and carrier ID information in endpoint

Registration Request (RRQ) messages. The gatekeeper list of alternates for a given endpoint includes the configured alternates and the alternates received in RRQ messages from that endpoint and any alternate endpoints received in incoming RAS LCF messages.

Examples

The following example shows that the endpoint at 172.16.53.15 1719 has been configured as an alternate for "GW10." There are no carrier IDs:

```
endpoint alt-ep h323id GW10 172.16.53.15 1719
```

The following example shows that an alternate endpoint list with different carrier IDs (CARRIER_ABC, CARRIER_DEF, and CARRIER_GHI) has been configured for "gwid":

```
endpoint alt-ep h323id gwid 1.1.1.1 carrier-id CARRIER_ABC
endpoint alt-ep h323id gwid 2.2.2.2 carrier-id CARRIER_DEF
endpoint alt-ep h323id gwid 1.1.1.1 carrier-id CARRIER_GHI
```

Related Commands

Command	Description
show gatekeeper endpoints	Displays information about alternate endpoints.

endpoint circuit-id h323id

To associate a circuit with a non-Cisco endpoint or on using a Cisco IOS release earlier than that on the gatekeeper, use the **endpoint circuit-id h323id**command in gatekeeper configuration mode. To delete the association, use the **no** form of this command.

endpoint circuit-id h323id *endpoint-h323id circuit-id* [**max-calls** *number*]
no endpoint circuit-id h323id *endpoint-h323id circuit-id* [**max-calls** *number*]

Syntax Description

endpoint -h323id	ID of the H.323 endpoint.
circuit -id	Circuit assigned to the H.323 endpoint.
max -calls *number*	(Optional) Maximum number of calls that this endpoint can handle. Range is from 1 to 10000. There is no default.

Command Default

No default behavior or values

Command Modes

Gatekeeper configuration (config-gk)

Command History

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

Usage Guidelines

The **endpoint circuit-id h323id** commandallows the gatekeeper and GKTMP server application to work with Cisco gateways that are running non-Cisco gateways or Cisco IOS releases that cannot identify incoming circuits. This command permits only one circuit to be associated with the endpoint.

Examples

The following example associates a non-Cisco endpoint first with a circuit **sample**, and assigns a maximum of 2750 calls to the endpoint:

```
Router(config)# gatekeeper
Router(config-gk)# endpoint circuit-id h323-id first sample max-calls 2750
```

Related Commands

Command	Description
show gatekeeper endpoint circuits	Displays information about all registered endpoints for a gatekeeper.

endpoint max-calls h323id

To set the maximum number of calls that are allowed for an endpoint, use the **endpoint max-calls h323id** command in gatekeeper configuration mode. To disable the set number, use the **no** form of this command.

endpoint max-calls h323id *endpoint-h323id max-number*
no endpoint max-calls h323id

Syntax Description

endpoint -h323id	H.323 ID of the endpoint.
max -number	Maximum number of calls that the endpoint can handle. The range is from 1 to 100000.

Command Default

This command is not configured by default.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modifications
12.3(1)	This command was introduced.
12.3(10)	This command was modified to reject the limit set by the endpoints.
12.3(14)T	This command was modified to reject the limit set by the endpoints.

Usage Guidelines

You must use the **endpoint resource-threshold** command and the **arq reject-resource-low** command to start resource monitoring on a gatekeeper before you can use this command. The **endpoint resource-threshold** command sets the call-capacity threshold of a gateway in the gatekeeper. The **arq reject-resource-low** command allows the endpoint to reject the limit of automatic repeat request message-packet (ARQs) when the endpoint reaches its configured maximum number of calls.

Examples

The following example shows how to set the maximum number of calls that GW-1 can handle to 1000:

```
gatekeeper
 endpoint max-calls h323id GW-1 1000
```

Related Commands

Command	Description
arq reject-resource-low	Enables the gatekeeper to send an ARQ to the requesting gateway if destination resources are low.
endpoint resource-threshold	Sets the call capacity threshold of a gateway in the gatekeeper.

endpoint naming

To customize the T3 endpoint naming convention on a per-MGCP-profile basis, use the **endpoint naming**command in MGCP profile configuration mode. To disable endpoint naming, use the **no** form of this command.

endpoint naming {**t1** | **t3**}
no endpoint naming

Syntax Description

t1	Flat-T3-endpoint naming convention.
t3	Hierarchical-T3-endpoint naming convention.

Command Default

t1

Command Modes

MGCP profile configuration (config-mgcp-profile)

Command History

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

Usage Guidelines

The option to select between a flat-endpoint naming convention and a hierarchical-T3-endpoint naming convention gives call agents flexibility without enforcing one naming convention. Signaling, backhauling, and trunks using SS7 are supported. T3 naming conventions on XCC signaling types, SS7, and ISDN are not supported.

Examples

The following example shows the T3 endpoint naming convention on an MGCP profile:

```
Router# configure terminal
Router(config)# mgcp profile default
Router(config-mgcp-profile)# endpoint naming t3
Router(config-mgcp-profile)# end
```

Related Commands

Command	Description
show mgcp	Displays MGCP configuration information.

endpoint resource-threshold

To set a gateway's call capacity thresholds in the gatekeeper, use the **endpoint resource-threshold**command in gatekeeper configuration mode. To delete the thresholds, use the **no** form of this command.

endpoint resource-threshold [**onset** *high-water-mark* | **abatement** *low-water-mark*]
no endpoint resource-threshold [**onset** *high-water-mark* | **abatement** *low-water-mark*]

Syntax Description

onset *high -water-mark*	(Optional) Maximum call volume usage for the gateway, as a percent. Range is from 1 to 99. The default is 90.
abatement *low -water-mark*	(Optional) Minimum call volume usage for the gateway, as a percent. Range is from 1 to 99. The default is 70.

Command Default

High-water-mark: 90 percent Low-water-mark: 70 percent

Command Modes

Gatekeeper configuration (config-gk)

Command History

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

Usage Guidelines

The gatekeeper monitors the call volume in each of its gateways. If the call capacity usage in a particular gateway exceeds the high-water-mark threshold, the gatekeeper stops sending calls to that gateway. When the gateway's active call volume falls below the low-water-mark threshold, the gatekeeper resumes sending new calls to the gateway. These thresholds are global values and affect all gateways registered with a given gatekeeper.

If neither threshold is set, the gatekeeper uses the default values.

Examples

The following example sets the high and low call-volume thresholds for all of its gateways:

```
Router(config)# gatekeeper
Router(config-gk)# endpoint resource-threshold onset 85 abatement 65
```

Related Commands

Command	Description
show gatekeeper endpoint circuits	Displays the information of all registered endpoints for a gatekeeper.

endpoint ttl

To enable the gatekeeper to assign a time-to-live (TTL) value to the endpoint when it registers with the gatekeeper, use the **endpoint ttl**command in gatekeeper configuration mode. To disable the TTL value, use the **no** form of this command.

endpoint ttl *seconds*
no endpoint ttl *seconds*

Syntax Description

seconds	TTL value, in seconds. Range is from 60 to 3600. The default is 1800.

Command Default

1800 seconds

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 the Cisco AS5850.

Usage Guidelines

This command specifies endpoint registration. Use this command to set the interval that the gatekeeper requires of an endpoint that does not supply its own value. Use a lower value to make the gatekeeper clear the registration of an unresponsive endpoint more quickly.

When an endpoint registers with the gatekeeper and does not provide a TTL value, the gatekeeper assigns this value as the time to live. When the TTL expires, the endpoint becomes subject to removal. However, the endpoint is queried a few times in an attempt to communicate with the device. If the device appears active, the registration does not expire. If the device is unresponsive after a few communication attempts, the endpoint is removed.

Examples

The following example enables a time to live value of 60 seconds:

```
endpoint ttl 60
```

Related Commands

Command	Description
timer cluster-element announce	Specifies the announcement period.
timer lrq seq delay	Specifies the timer for sequential LRQs.
timer lrq window	Specifies the window timer for LRQs.

erase vfc

To erase the flash memory of a specified voice feature card (VFC), use the **erase vfc**command in privileged EXEC mode.

erase vfc *slot*

Syntax Description

slot	Slot on the Cisco AS5300 in which the specified VFC resides. Range is from 0 to 2. There is no default.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco AS5300.

Usage Guidelines

Use the **erase vfc**command to erase the contents of flash memory for a specified VFC (thereby freeing space in VFC flash memory) including the default file list and the capability file list.

Examples

The following example erases the flash memory on the VFC located in slot 0:

```
Router# erase vfc 0
```

Related Commands

Command	Description
delete vfc	Deletes a file from VFC flash memory.

error-category

To specify Q.850 cause code mapping, use the **error-category** command in voice cause-code configuration mode. To disable Q.850 cause code mapping, use the **no** form of this command.

error-category *cause-code* **q850-cause** *number*
no error-category *cause-code* **q850-cause** *number*

Syntax Description

cause-code	Specifies error category value to be mapped to a configured Q850 cause code value. Values range from 128 to 278.
number	Specifies the default Q.850 cause code value. Values range from 1 to 127.

Command Default

The IEC mechanism defaults to the assigned Q.850 cause codes.

Command Modes

Voice cause-code configuration (conf-voice-cause)

Command History

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

Usage Guidelines

Only the Session Initiation Protocol (SIP) and H.323 subsystems use the category and Q.850 mapping tables to determine the disconnect cause code when releasing a call due to an internal error.

To disable all mappings, use the **no voice cause-code** command. To disable a single mapping, use the **voice cause-code**command, followed by the **no error-category**command.

Examples

The following example sets error category 128 to map to Q.850 cause code 27:

```
Router(config)# voice cause code
Router(conf-voice-cause)# error-category 128 q850-cause 27
```

The following example defines two mappings for categories 128 and 129:

```
Router(config)# voice cause-code
Router(conf-voice-cause)# error-category 128 q850-cause 27
Router(conf-voice-cause)# error-category 129 q850-cause 38
Router(conf-voice-cause)# exit
```

The following example removes the mapping for category 128 only, leaving 129 defined:

```
Router(config)# voice cause-code
Router(conf-voice-cause)# no error-category 128
Router(conf-voice-cause)# exit
```

The following example removes all configured mappings:

```
Router(config)# no voice cause-code
```

Related Commands

Command	Description
show voice cause-code	Displays internal error category to q.850 cause code mapping.
voice cause-code	Enables voice cause-code configuration mode.

error-code-override

To configure the Session Initiation Protocol (SIP) error code to be used at the dial peer, use the **error-code-override** command in voice service SIP, voice class tenant configuration mode, or dial peer voice configuration mode. To disable the SIP error code configuration, use the **no** form of this command.

error-code-override {**options-keepalive failure** | **call spike failure** | **cac-bandwidth failure**} *sip-status-code-number* **[system]**
no error-code-override {**options-keepalive failure** | **call spike failure** | **cac-bandwidth failure**}**[system]**

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 response error codec that is sent for the options-keepalive, cac-bandwidth, or call spike failure that happened at the dial peer. The range is 400–699. The default value is 500. The following table in the "Usage Guidelines" section describes these error codes.
system	Specifies that the SIP error code 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

By default the SIP error code is not configured.

Command Modes

Voice service SIP configuration (conf-ser-sip)

Dial peer voice configuration (conf-dial-peer)

Voice class tenant configuration (config-class)

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.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models under voice class tenant configuration.

Usage Guidelines

The **error-code-override** command in voice service SIP or dial peer voice configuration mode configures the error code response for options-keepalive, call spike, or cac-bandwidth failures. The **voice-class sip error-code-override** command in voice service SIP or dial peer voice configuration mode configures the error code responses for call spike failures.

The table below describes the SIP error codes.

Table 8: 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 using the **error-code-override** command for options-keepalive failures in voice service SIP configuration mode:

```
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(config-ser-sip)# error-code-override options-keepalive failure 503
```

The following example shows how to configure the SIP error code using the **error-code-override** command for call spike failures in dial peer voice configuration mode:

```
Router(config)# dial-peer voice 400
Router(conf-dial-peer)# error-code-override call spike failure 503
```

The following example shows how to configure the SIP error code for Call Admission Control bandwidth failures:

```
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(config-ser-sip)# error-code-override cac-bandwidth failure 503
```

The following example shows how to configure the SIP error code in the voice class tenant configuration mode:

```
Router(config-class)# error-code-override total-calls failure system
```

Related Commands

Command	Description
voice-class sip error-code-override	Configures the error code responses for call spike failures.

error-correction

To set error correction for the Signaling System 7 (SS7) signaling link when the SS7 Message Transfer Part Layer 2 (MTP2) variant is Telcordia (formerly Bellcore) or ITU-white, use the **error-correction** command in ITU configuration mode. To disable error correction, use the **no** form of this command.

error-correction [**basic** | **pcr** [**forced-retransmission** *parameters*]]
no error-correction

Syntax Description

basic	(Optional) Sets SS7 signaling link error correction to basic mode for configurations in which one-way propagation delay is less than 40 ms.
pcr	(Optional) Sets intercontinental SS7 signaling link error correction to Preventive Cyclic Retransmission (PCR) mode for configurations that are transmitted over satellite connections and for configurations in which one-way propagation delay is greater than 40 ms.
forced-retransmission	(Optional) Enables forced retransmission when the **pcr** keyword is selected. To disable forced retransmission, use the **no** form of the command.
parameters	(Optional) Sets the error-correction method for an SS7 signaling link. The following types of error correction are configurable: • **pcr-enabled** --Tracks the error-correction method on the SS7 signaling channel. The error-correction method can be either PCR or basic. PCR is disabled by default. • **forced-retransmission-enabled** --Tracks forced retransmission on the SS7 signaling channel. **Note** Forced retransmission is enabled only if PCR is enabled. • **n2** *octets* --The maximum number of N2 octets that can be queued in the RTB for an SS7 signaling channel before forced retransmission procedures are initiated. The number of octets can range from 200 to 4000. The default is 450. **Note** This parameter is ignored if forced retransmission is not enabled.

Command Default

Error correction is set to basic.

Command Modes

ITU configuration (config-ITU)

Command History

Release	Modification
12.3(2)T	This command was introduced on the Cisco 2600 series, Cisco AS5350, and Cisco AS5400 Cisco signaling link terminals (SLTs).

Usage Guidelines

The maximum supported signaling link loop (round trip) delay is 670 ms (the time between the sending of a message signal unit [MSU] and the reception of the acknowledgment for this MSU in undisturbed operation).

Examples

The following example sets the error-correction method to PCR and enables forced retransmission with the N2 parameter set and 1000 octets selected:

```
Router(config-ITU)# error-correction pcr forced-retransmission n2 1000
```

Related Commands

Command	Description
ss7 mtp2-variant	Configures an SS7 signaling link.

error-passthru

To enable the passage of error messages from the incoming SIP leg to the outgoing SIP leg, use the **error-passthru** command in Voice service SIP configuration mode. To disable error pass-through, use the **no** form of this command.

error-passthru system
no error-passthru

Syntax Description

system	Specifies that the error-passthrough command 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

Voice service SIP configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.3(4)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**.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

- Like-to-like error messages are not passed from the incoming SIP leg to the outgoing SIP leg. Error messages are passed through the CUBE when the **error-passthru** command is configured in Cisco IOS Release 12.4(15)T and later.

Examples

The following example shows the error message configured to pass from the incoming SIP leg to the outgoing SIP leg:

```
Router(conf-serv-sip)# error-passthru
```

The following example shows how to passthrough an error message in the voice class tenant configuration mode:

```
Router(config-class)# error-passthru system
```

event-log

To enable event logging for applications, use the **event-log** command in application configuration monitor configuration mode. To disable event logging, use the **no** form of this command.

event-log [**size** [*number of events*]] [**one-shot**] [**pause**]
no event-log

Syntax Description

size [*number of events*]	(Optional) Maximum number of OSPF events in the event log.
one-shot	(Optional) Mode that enables the logging of new events at one specific point in time. The event logging mode is cyclical by default, meaning that all new events are logged as they occur.
pause	(Optional) Enables the user to pause the logging of any new events at any time, while keeping the current events in the log.

Command Default

By default, event logging is not enabled. When event logging is enabled, it is cyclical by default.

Command Modes

Application configuration monitor configuration mode
OSPF for IPv6 router configuration mode

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application event-log** command.
12.2(33)SRC	Support for IPv6 was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

This command enables event logging globally for all voice applications. To enable or disable event logging for a specific application, use one of the following commands:

param event-log (application parameter configuration mode)

paramspace appcommon event-log (service configuration mode)

Note To prevent event logging from adversely impacting system resources for production traffic, the gateway uses a throttling mechanism. When free processor memory drops below 20-percent, the gateway automatically disables all event logging. It resumes event logging when free memory rises above 30 percent. While throttling is occurring, the gateway does not capture any new event logs even if event logging is enabled. You should monitor free memory and enable event logging only when necessary for isolating faults.

Examples

The following example shows event logging enabled:

```
application
 monitor
  event-log
```

The following example shows OSPF for IPv6 event logging enabled. The router instance is 1, the event-log size is 10,000, and the mode is one-shot.

```
ipv6 router ospf 1
 event-log size 10000 one-shot
```

Related Commands

Command	Description
call application event-log	Enables event logging for all voice application instances.
event-log dump ftp	Enables the gateway to write the contents of the application event log buffer to an external file.
event-log error-only	Restricts event logging to error events only for application instances.
event-log max-buffer-size	Sets the maximum size of the event log buffer for each application instance.
param event-log	Enables or disables event logging for a package.
paramspace appcommon event-log	Enables or disables event logging for a service (application).

event-log (Privileged EXEC)

To configure different event logging functions, use the **event-log** command in privileged EXEC mode.

event-log {**calibrate** | {**circular** | **platform-ticks**} {**off** | **on**} | {**disable** | **enable**} [*event-group*] | **init** | **mark** | **save** {*hostnameIP-address*} *prefix* | **timelog**}

Syntax Description

calibrate	Caliberates the platform clock.
circular	Enables or disables the circular event log.
off	Disables the circular event log.
on	Enables the circular event log.
disable	Disables event logging.
event-group	(Optional) Event group to be enabled or disabled. The range is from 1 to FFFFFFF.
enable	Enables event logging.
init	Initializes the event logging data structures.
mark	Marks an event log.
platform-ticks	Enables or disables platform ticks for a clock.
save	Saves the event log to the TFTP host as elog.out.
hostname	Hostname of the TFTP server to receive elog.out.
IP-address	IP address of the TFTP server to receive elog.out.
prefix	Prefix for the saved files.
timelog	Specifies time logging of 1000 events.

Command Default

Event logging functions are not configured.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.

Examples

The following example shows how to enable the circular event log:

```
Router# event-log circular on
```

Related Commands

Command	Description
event-log dump ftp	Enables the gateway to write the contents of the application event log buffer to an external file.
event-log error-only	Restricts event logging to error events only for application instances.
event-log max-buffer-size	Sets the maximum size of the event log buffer for each application instance.
param event-log	Enables or disables event logging for a package.
paramspace appcommon event-log	Enables or disables event logging for a service (application).

event-log dump ftp

To enable the gateway to write the contents of the application event log buffer to an external file, use the **event-log dump ftp** command in application configuration monitor configuration mode. To reset to the default, use the **no** form of this command.

event-log dump ftp *server* [*:port*] */path* **username** *username* **password** { **0** | **6** | **7** } *password*
no event-log dump ftp

Syntax Description

server	Name or IP address of the FTP server where the file is located.
: *port*	(Optional) Specific port number on the server.
/ *file*	Name and path of the file.
username	Username required to access the file.
encryption-type	(Optional) The Cisco proprietary algorithm used to encrypt the password. Values are 0 or 7. To disable encryption enter 0; to enable encryption enter 7. If you specify 7, you must enter an encrypted password (a password already encrypted by a Cisco router).
password {*0* | *6* | *7*}	Following are the password encryption types– • **0**– Specifies that the subsequent password is in plain text. Type **0** disables encryption. • **6**– Specifies that the subsequent password is encrypted using the AES algorithm. Ensure to provide a string in AES-encrypted format. • **7**– Specifies that the subsequent password is hidden. You must enter a Cisco-proprietary encrypted password string. • **LINE**– The cleartext password.
password	Password required to access the file.

Command Default

By default, this feature is not enabled on the gateway.

Command Modes

Application configuration monitor configuration (config-app-monitor)

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application event-log dump ftp** command.
Cisco IOS XE 26.2.1	This command was modified for the following: • To support Type 6 encryption. • To display warning message for insecure protocol usage.

Usage Guidelines

This command enables the gateway to automatically write the event log buffer to the named file either after an active application instance terminates or when the event log buffer becomes full. The default buffer size is 4 KB. To modify the size of the buffer, use the **event-log max-buffer-size** command in application configuration monitor configuration mode.

Starting from Cisco IOS XE 26.2.1 release, it is recommended to use Type 6 (AES) for all credential provisioning to comply with security standards. Usage of Type 0, or 7 triggers a syslog warning. Ensure **password encryption aes** and **key config-key password-encrypt** are enabled to support auto-conversion of Type 0, or 7 to Type 6 reversible encryption. If the encryption commands are not enabled, 0 and 7 password types are not converted to type 6; they remain saved as type 0 and 7

Enabling the gateway to write event logs to FTP could adversely impact gateway memory resources in some scenarios, for example, when:

- The gateway is consuming high processor resources and FTP does not have enough processor resources to flush the logged buffers to the FTP server.
- The designated FTP server is not powerful enough to perform FTP transfers quickly
- Bandwidth on the link between the gateway and the FTP server is not large enough
- The gateway is receiving a high volume of short-duration calls or calls that are failing

You should enable FTP dumping only when necessary and not enable it in situations where it might adversely impact system performance.

Warning Starting with Cisco IOS XE 26.2.1, a warning message is displayed when insecure protocols such as HTTP, FTP, or TFTP are used, as they do not provide encryption or authentication. Use secure alternatives such as HTTPS, SFTP, or SCP instead.

Examples

The following example shows type 6 encryption configuration, supported starting from Cisco IOS XE 26.2.1 release:

```
application
monitor
 event-log dump ftp 10.10.10.101/elogs/app-elogs.log username myname password 6
B]hHYYZ_aJZUeYSfW]]ZTT_O]JXMN`
```

The following example enables type 0 to type 6 auto-conversion, starting from Cisco IOS XE 26.2.1 release:

```
Router(config)#password encryption aes
Router(config)#key config-key password-encrypt
Router(config)#application
Router(config-app)#monitor
Router(config-app-monitor)# event-log dump ftp 10.10.10.101/elogs/app-elogs.log username
myname password 0 mypass
SECURITY WARNING - Module: APPLICATION_MONITOR, Command: event-log dump ftp
10.10.10.101/elogs/app-elogs.log username myname password 0 * ,
Reason: No encryption is configured, Description: Application monitor event log dump
configured with insecure FTP protocol -
vulnerable to credential exposure, Remediation: Transition to secure file transfer methods
 using SCP, SFTP, HTTPS protocols
```

```
Router(config-app-monitor)# end

Router# show run | sec event-log
  event-log
  event-log dump ftp 10.10.10.101/elogs/app-elogs.log username myname password 6
CGiJD[EZAHKD^\aPDNe`baCN^Pf_X]AAB
```

The following example shows the warning being displayed for the usage of insecure FTP protocol:

```
Device(config)#application
Device(config-app)#monitor
Device(config-app-monitor)#event-log dump ftp 10.10.10.101/elogs/app-elogs.log username
myname password 0 password
 SECURITY WARNING - Module: APPLICATION_MONITOR, Command: event-log dump ftp
ftp-server/elogs/app-elogs.log username myname password 0 *,
Reason: No encryption is configured, Description: Application monitor event log dump
configured with insecure FTP protocol - vulnerable to credential exposure,
Remediation: Transition to secure file transfer methods using SCP, SFTP, HTTPS protocols
Device(config-app-monitor)#
```

Examples

The following example enables the gateway to write application event logs to an external file named app_elogs.log on a server named ftp-server:

```
application
monitor
 event-log dump ftp ftp-server/elogs/app-elogs.log username myname password 0 mypass
```

Examples

The following example specifies that application event logs are written to an external file named app_elogs.log on a server with the IP address of 10.10.10.101:

```
application
monitor
 event-log dump ftp 10.10.10.101/elogs/app-elogs.log username myname password 0 mypass
```

Related Commands

Command	Description
call application event-log dump ftp	Enables the gateway to write the contents of the application event log buffer to an external file.
event-log	Enables event logging for applications.
event-log error-only	Restricts event logging to error events only for application instances.
event-log max-buffer-size	Sets the maximum size of the event log buffer for each application instance.

event-log error-only

To restrict event logging to error events only for application instances, use the **event-log error-only** command in application configuration monitor configuration mode. To reset to the default, use the **no** form of this command.

event-log error-only
no event-log error-only

Syntax Description

This command has no arguments or keywords.

Command Default

If logging is enabled, all application events are logged.

Command Modes

Application configuration monitor configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application event-log error-only** command.

Usage Guidelines

This command limits new event logging to error events only; it does not enable logging.

You must use either this command with the **event-log**command, which enables event logging for all voice applications, or enable event logging for a specific application using the **param event-log**command(package appcommon configuration mode) or the **paramspace appcommon event-log** command (service configuration mode).

Any events logged before this command is issued are not affected.

Examples

The following example enables event logging for error events only:

```
application
monitor
 event-log
  event-log error-only
```

Related Commands

Command	Description
call application event-log error-only	Restricts event logging to error events only for application instances.
event-log	Enables event logging for applications.
event-log dump ftp	Enables the gateway to write the contents of the application event log buffer to an external file.
event-log max-buffer-size	Sets the maximum size of the event log buffer for each application instance.

event-log max-buffer-size

To set the maximum size of the event log buffer for each application instance, use the **event-log max-buffer-size**command in application configuration monitor configuration mode. To reset to the default, use the **no** form of this command.

event-log max-buffer-size *kbytes*
no event-log max-buffer-size

Syntax Description

kbytes	Maximum buffer size, in kilobytes. Range is 1 to 50. Default is 4 KB.

Command Default

By default, the maximum size is set to 4 KB.

Command Modes

Application configuration monitor configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application event-log max-buffer-size** command.

Usage Guidelines

If the event log buffer reaches the limit set by this command, the gateway allocates a second buffer of equal size. The contents of both buffers are displayed when you use the **show call application session-level** command. When the first event log buffer becomes full, the gateway automatically appends its contents to an external FTP location if the **event-log dump ftp** command is used.

A maximum of two buffers are allocated for an event log. If both buffers are filled, the first buffer is deleted and another buffer is allocated for new events (the buffer wraps around). If the **event-log dump ftp** command is configured and the second buffer becomes full before the first buffer is dumped, event messages are dropped and are not recorded in the buffer.

Do not set the maximum buffer size to more than you need for a typical application session. After an active session terminates, the amount of memory used by the buffer is allocated to the history table and is maintained for the length of time set by the **history session retain-timer** command. Also consider that most fatal errors are captured at the end of an event log.

To conserve memory resources, write the event log buffer to FTP by using the **event-log dump ftp** command.

Examples

The following example sets the application event log buffer to 8 KB:

```
application
 monitor
  event-log max-buffer-size 8
```

Related Commands

Command	Description
event-log	Enables event logging for applications.

Command	Description
event-log dump ftp	Enables the gateway to write the contents of the application event log buffer to an external file.
call application event-log max-buffer-size	Maximum size of the event log buffer for each application instance.

expect-factor

To set the expect-factor value for voice quality, which affects the threshold calculated planning impairment factor (ICPIF) loss/delay busyout value, use the **expect-factor** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

expect-factor *voice-quality-specifications*
no expect-factor *voice-quality-specifications*

Syntax Description

voice-quality-specifications	Integers that represent quality of voice as described in ITU G.107. Range: 0 to 20, with 0 representing toll quality. Default: 10.

Command Default

10

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.2(8)T	The *voice-quality-specifications* default changed from 10 to 0.
12.3(3)T	The *voice-quality-specifications* default changed from 0 to 10.

Usage Guidelines

The expect factor impacts the calculated value of ICPIF. This value is used in conjunction with Simple Network Management Protocol (SNMP) to generate a trap when voice quality falls below a configured value. It also impacts the value of ICPIF reported in call-account records as well as in call-history values on the gateway.

Use this and related commands together on a dial peer as follows:

- Use this command to set the expect-factor value.
- Use the **icpif** command to set a threshold ICPIF value (the ICPIF calculation uses the expect-factor value as well as values for loss and delay).
- Use the **snmp enable peer-trap poor-qov** command to generate notifications in the form of SNMP traps to the network manager for calls whose ICPIF value exceeds the threshold.

Note For more information on ICPIF, see *IP SLAs--Analyzing VoIP Service Levels Using the VoIP Jitter Operation* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsla_c/hsvoipj.htm

Examples

The following example sets the expect factor for a dial peer:

```
dial-peer voice 10 voip
 expect-factor 0
```

Related Commands

Command	Description
icpif	Specifies the ICPIF threshold for calls sent by a dial peer.
snmp enable peer-trap poor-qov	Generates poor-quality-of-voice notifications for applicable calls associated with a VoIP dial peer.

extsig mgcp

To configure external signaling control by Media Gateway Control Protocol (MGCP) for a T1 or E1 trunk controller card, use the **extsig mgcp** command in controller configuration mode. To discontinue MGCP control for this controller, use the **no** form of this command.

extsig mgcp
no extsig mgcp

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Controller configuration (config-controller)

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 and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. 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, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

For T3 lines, each logical T1 trunk controller card must be configured using the **extsig mgcp** command.

Examples

The following example shows MGCP signaling control being configured for T1 controller 7/0:

```
controller T1 7/0
 framing esf
 extsig mgcp
 guard-timer 10 on-expiry reject
 linecode b8zs
 ds0-group 1 timeslots 1-24 type none service mgcp
```

Related Commands

Command	Description
dialer extsig	Configures an interface to initiate and terminate calls using an external signaling protocol.



F

- fax interface-type, on page 205
- fax protocol (dial peer), on page 207
- fax protocol (voice-service), on page 209
- fax protocol t38 (dial peer), on page 212
- fax protocol t38 (voice-service), on page 215
- fax rate (dial peer), on page 218
- fax rate (pots), on page 221
- fax rate (voice-service), on page 222
- fax receive called-subscriber, on page 224
- fax-relay (dial peer), on page 225
- fax-relay (voice-service), on page 228
- fax send center-header, on page 231
- fax send coverpage comment, on page 233
- fax send coverpage e-mail-controllable, on page 234
- fax send coverpage enable, on page 236
- fax send coverpage show-detail, on page 237
- fax send left-header, on page 239
- fax send max-speed, on page 241
- fax send right-header, on page 242
- fax send transmitting-subscriber, on page 244
- file-acct flush, on page 245
- file-acct reset, on page 246
- filter voice, on page 247
- flush, on page 248
- fmtp, on page 249
- forward-alarms, on page 251
- forward-digits, on page 252
- forward-to-voicemail, on page 254
- frame-relay voice bandwidth, on page 256
- freq-max-delay, on page 258
- freq-max-deviation, on page 260
- freq-max-power, on page 262
- freq-min-power, on page 264

- freq-pair, on page 266
- freq-power-twist, on page 268
- frequency (cp-dualtone), on page 270

fax interface-type

To specify the interface to be used for a fax call, use the **fax interface-type** command in global configuration mode. To reset to the default fax protocol, use the **no** form of this command.

fax interface-type {**fax-mail** | **modem** | **vfc**}
no fax interface-type {**fax-mail** | **modem** | **vfc**}

Syntax Description

fax -mail	Specifies that voice digital signal processors (DSPs) process fax store-and-forward data. This keyword replaces the **vfc** keyword for DSPs.
modem	(Cisco AS5300 only) Specifies that modem cards process fax store-and-forward data. **Note** This keyword is not supported except for instances documented in the "Usage Guidelines" section.
vfc	(Cisco AS5300 only) Specifies that voice feature cards (VFCs) process fax store-and-forward data. This keyword has been superseded by the **fax-mail** keyword and is retained for backward compatibility only.

Command Default

Cisco AS5300: See the "Usage Guidelines" section All other platforms: **fax-mail**

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(5)XM	The command was implemented on the Cisco AS5800.
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 and implemented on Cisco 1750 and the **fax-mail** keyword was added.
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 following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

When using this command to change the interface type for store-and-forward fax, you must reload (reboot or reset) the router.

On the Cisco AS5300 access server, the keyword **vfc** maps internally to the **fax-mail** keyword. If you use the **vfc** keyword with the **fax interface-type** command, the output from the **show running-config** command displays **fax-mail** as the option that was set.

The Cisco AS5300 defaults for the **fax interface-type** command are as follows:

- If the Cisco AS5300 has voice cards only, the default is the **fax-mail** keyword. The **modem** keyword is unavailable.
- If the Cisco AS5300 has modem cards only, the default is the **modem** keyword.
- If the Cisco AS5300 has both modem and voice cards, the default is the **modem** keyword.

Examples

The following example specifies the use of voice DSPs to process fax store-and-forward data:

```
Router(config)# fax interface-type fax-mail
```

The following example specifies the use of modems to process fax store-and-forward data on a Cisco AS5300:

```
Router(config)# fax interface-type modem
```

fax protocol (dial peer)

To specify the fax protocol to be used for a specific VoIP dial peer, use the **fax protocol**command in dial peer configuration mode. To return to the global default fax protocol, use the **system** keyword or the **no** form of this command.

Cisco AS5350, Cisco AS5400, Cisco AS5850
fax protocol {**none** | **system** | **pass-through** {**g711ulaw** | **g711alaw**}}
no fax protocol

All Other Platforms
fax protocol {**cisco** | **none** | **system** | **pass-through** {**g711ulaw** | **g711alaw**}}
no fax protocol

Syntax Description

cisco	Cisco-proprietary fax protocol.
none	No fax pass-through is attempted. All special fax handling is disabled, except for modem pass-through if configured with the **modem pass-through** command.
system	Uses the global configuration that was set using the **fax protocol** command in voice-service configuration mode.
pass -through	The fax stream uses one of the following high-bandwidth codecs: • **g711ulaw** --Uses the G.711 u-law codec. • **g711alaw** --Uses the G.711 a-law codec.

Command Default

system

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
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. The **none** keyword was introduced.
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(4)T	This command was integrated into Cisco IOS Release 12.2(4)T and implemented on the Cisco 1750.

Release	Modification
12.2(11)T	This command was implemented on the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. The **t.38**keyword and its options were moved to two new commands: **fax protocol t38** (dial peer) and **fax protocol t38** (voice-service).

Usage Guidelines

Use the **fax protocol** command in dial-peer configuration mode to configure the type of fax relay capability for a specific dial peer. Note the following command behavior:

- **fax protocol none** --Disables all fax handling.
- **no fax protocol** --Sets the fax protocol for the dial peer to the default, which is **system**.

If the **fax protocol**(voice-service) command is used to set fax relay options for all dial peers and the **fax protocol** (dial peer) command is used on a specific dial peer, the dial-peer configuration takes precedence over the global configuration for that dial peer.

Examples

The following example specifies that the fax stream use fax pass-through for VoIP dial peer 99:

```
dial-peer voice 99 voip
 fax protocol pass-through g711ulaw
```

Related Commands

Command	Description
fax protocol (voice-service)	Specifies the global default fax protocol to be used for all VoIP dial peers.
fax protocol t38 (dial peer)	Specifies the ITU-T T.38 standard fax protocol to be used for a specific VoIP dial peer.
fax protocol t38 (voice-service)	Specifies the global default ITU-T T.38 standard fax protocol to be used for all VoIP dial peers.

fax protocol (voice-service)

To specify the global default fax protocol to be used for all VoIP dial peers, use the **fax protocol**command in voice-service configuration mode. To return to the default fax protocol, use the **no** form of this command.

Cisco AS5350, Cisco AS5400, Cisco AS5850
fax protocol {**none** | **pass-through** {**g711ulaw** | **g711alaw**}}
no fax protocol

All Other Platforms
fax protocol {**cisco** | **none** | **pass-through** {**g711ulaw** | **g711alaw**}}
no fax protocol

Syntax Description

none	No fax pass-through is attempted. All special fax handling is disabled, except for modem pass-through (if configured with the **modem pass-through** command).
pass-through	The fax stream uses one of the following high-bandwidth codecs: • **g711alaw** --Uses the G.711 A-law codec. • **g711ulaw** --Uses the G.711 mu-law codec.
cisco	Cisco-proprietary fax protocol. The **cisco** keyword is the default for all platforms except the Cisco AS5350, Cisco AS5400, and Cisco AS5850. • This is the only valid option when you are using Cisco Unified CME 4.0(3) or a later version on Skinny Call Control Protocol (SCCP)-controlled FXS ports.

Command Default

If no fax protocol is specified, the **cisco** protocol is the default for all platforms except the Cisco AS5350, Cisco AS5400, and Cisco AS5850. For these three platforms, **none** is the default, so no fax pass-through is attempted.

Command Modes

Voice-service configuration (config-voi-serv)

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
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(4)T	This command was integrated into Cisco IOS Release 12.2(4)T and implemented on the Cisco 1750.

Release	Modification
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. The **t.38**keyword and its options were removed and added to two new commands: **fax protocol t38 (dial peer)** and **fax protocol t38 (voice-service)**.
12.4(11)T	Support for SCCP-controlled FXS ports was added.

Usage Guidelines

Use the **fax protocol**command with the **voice service voip** command to configure the fax relay capability for all VoIP dial peers.

Note the following command behavior:

- **fax protocol none** -- Disables all fax handling.
- **no fax protocol** --Sets the fax protocol to the default.

If the **fax protocol** (voice-service) command is used to set fax relay options for all dial peers and the **fax protocol** (dial peer) command is used on a specific dial peer, the dial-peer configuration takes precedence over the global configuration for that dial peer. When the **system**keyword is used in the dial-peer configuration of the **fax protocol**command, it specifies that the global default fax protocol set with this command is used by that dial peer.

In Cisco Unified CME 4.0(3) and later, the **fax protocol cisco** (voice-service) command is the only supported fax protocol option for SCCP-controlled FXS ports. G.711 fax pass-through is not supported for Cisco VG 224 and FXS ports.



Note The **modem passthrough protocol** and **fax protocol** commands cannot be configured at the same time. If you enter either one of these commands when the other is already configured, the command-line interface returns an error message. The error message serves as a confirmation notice because the **modem passthrough protocol** command is internally treated the same as the **fax protocol passthrough** command by the Cisco IOS software. For example, no other mode of fax protocol (for example, fax protocol T.38) can operate if the **modem passthrough protocol** command is configured.



Note Even though the **modem passthrough protocol** and **fax protocol passthrough**commands are treated the same internally, be aware that if you change the configuration from the **modem passthrough protocol** command to the **modem passthrough ns e** command, the configured **fax protocol passthrough** command is not automatically reset to the default. If default settings are required for the **fax protocol** command, you have to specifically configure the **fax protocol** command.

Examples

The following example specifies that the fax stream for all VoIP dial peers use fax pass-through:

```
voice service voip
 fax protocol pass-through g711ulaw
```

Related Commands

Command	Description
fax protocol (dial peer)	Specifies the fax protocol for a specific VoIP dial peer.
fax protocol t38 (dial peer)	Specifies the ITU-T T.38 standard fax protocol to be used for a specific VoIP dial peer.
fax protocol t38 (voice-service)	Specifies the global default ITU-T T.38 standard fax protocol to be used for all VoIP dial peers.
modem passthrough	Enables fax or modem pass-through over VoIP globally for all dial peers.
voice service voip	Enters voice-service configuration mode.

fax protocol t38 (dial peer)

To specify the ITU-T T.38 standard fax protocol to be used for a specific VoIP dial peer, use the **fax protocol t38** command in dial-peer configuration mode. To return to the default fax protocol, use the **no** form of this command.

Cisco AS5350, Cisco AS5400, Cisco AS5850 Platforms
fax protocol t38 [**nse** [**force**]] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**none** | **pass-through** {**g711ulaw** | **g711alaw**}}]
no fax protocol t38

All Other Platforms
fax protocol t38 [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**cisco** | **none** | **pass-through** {**g711ulaw** | **g711alaw**}}]
no fax protocol t38

Syntax Description

nse	(Optional) Uses NSEs to switch to T.38 fax relay.
force	(Optional) Unconditionally, uses Cisco network services engines (NSE) to switch to T.38 fax relay. This option allows T.38 fax relay to be used between Cisco H.323 or Session Initiation Protocol (SIP) gateways and Media Gateway Control Protocol (MGCP) gateways.
version {**0** | **3**}	(Optional) Specifies a version for configuring fax speed: • **0** --Configures version 0, which uses T.38 version 0 (1998--G3 faxing) • **3** --Configures version 3, which uses T.38 version 3 (2004--V.34 or SG3 faxing)
ls -redundancy *value*	(Optional) (T.38 fax relay only) Specifies the number of redundant T.38 fax packets to be sent for the low-speed V.21-based T.30 fax machine protocol. Range varies by platform from 0 (no redundancy) to 5 or 7. For details, see to command-line interface (CLI) help. Default is 0.
hs -redundancy *value*	(Optional) (T.38 fax relay only) Specifies the number of redundant T.38 fax packets to be sent for high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. Range varies by platform from 0 (no redundancy) to 2 or 3. For details, see the command-line interface (CLI) help. Default is 0.
fallback	(Optional) A fallback mode is used to transfer a fax across a VoIP network if T.38 fax relay could not be successfully negotiated at the time of the fax transfer.
cisco	(Optional) Cisco-proprietary fax protocol.
none	(Optional) No fax pass-through or T.38 fax relay is attempted. All special fax handling is disabled, except for modem pass-through if configured with the **modem pass-through**command.

pass -through	(Optional) The fax stream uses one of the following high-bandwidth codecs: • **g711ulaw** --Uses the G.711 mu-law codec. • **g711alaw** --Uses the G.711 a-law codec.

Command Default

ls-redundancy 0 hs-redundancy 0 fallback none for the Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms**ls-redundancy 0 hs-redundancy 0 fallback cisco** for all other platforms

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
12.2(13)T	This command was introduced.
15.1(1)T	This command was modified. The **version** keyword was added with the **0** and **3** keywords to specify fax speed as G3 or SG3.

Usage Guidelines

Use this command in dial-peer configuration mode to configure the type of fax relay capability for a specific dial peer. If the **fax protocol t38 (voice-service)** command is used to set fax relay options for all dial peers and the **fax protocol t38 (dial peer)** command is used on a specific dial peer, the dial-peer configuration takes precedence over the global configuration for that dial peer.

If you specify **version 3** in the **fax protocol t38** command and negotiate T.38 version 3, the fax rate is automatically set to 33600.

The **ls-redundancy** and **hs-redundancy** keywords are used to send redundant T.38 fax packets. Setting the **hs-redundancy**keyword to a value greater than 0 causes a significant increase in the network bandwidth consumed by the fax call.

Use the **nse force** option when the H.323 or SIP gateway is interoperating with a Cisco MGCP gateway and the call agent does not support the interworking and negotiation of T.38 fax relay and NSE attributes at the time of call setup. When the corresponding option is configured on the MGCP gateway, the **nse force**option allows T.38 fax relay to be used between Cisco H.323 or SIP gateways and MGCP gateways.

Examples

The following example show how to configure T.38 fax relay for VoIP:

```
dial-peer voice 99 voip
 fax protocol t38
```

The following example shows how to use NSEs to enter T.38 fax relay mode:

```
dial-peer voice 99 voip
 fax protocol t38 nse
```

The following example shows how to specify the T.38 fax protocol for this dial peer, set low-speed redundancy to a value of 1, and set high-speed redundancy to a value of 0:

```
dial-peer voice 99 voip
 fax protocol t38 ls-redundancy 1 hs-redundancy 0
```

Related Commands

Command	Description
fax protocol (dial peer)	Specifies the fax protocol for a specific VoIP dial peer.
fax protocol (voice-service)	Specifies the global default fax protocol to be used for all VoIP dial peers.
fax protocol t38 (voice-service)	Specifies the global default ITU-T T.38 standard fax protocol to be used for all VoIP dial peers.

fax protocol t38 (voice-service)

To specify the global default ITU-T T.38 standard fax protocol to be used for all VoIP dial peers, use the **fax protocol t38**command in voice-service configuration mode. To return to the default fax protocol, use the **no** form of this command.

Cisco AS5350, Cisco AS5400, Cisco AS5850 Platforms
fax protocol t38 [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**none** | **pass-through** {**g711ulaw** | **g711alaw**}}]
no fax protocol t38

All Other Platforms
fax protocol t38 [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**cisco** | **none** | **pass-through** {**g711ulaw** | **g711alaw**}}]
no fax protocol t38

Syntax Description

nse	(Optional) Uses network services engines (NSE) to switch to T.38 fax relay.
force	(Optional) Unconditionally, uses Cisco NSEs to switch to T.38 fax relay. This option allows T.38 fax relay to be used between Cisco H.323 or Session Initiation Protocol (SIP) gateways and Media Gateway Control Protocol (MGCP) gateways.
version {**0** | **3**}	(Optional) Specifies a version for configuring fax speed: • **0** --Configures version 0, which uses T.38 version 0 (1998--G3 faxing) • **3** --Configures version 3, which uses T.38 version 3 (2004--V.34 or SG3 faxing)
ls -redundancy *value*	(Optional) (T.38 fax relay only) Specifies the number of redundant T.38 fax packets to be sent for the low-speed V.21-based T.30 fax machine protocol. Range varies by platform from 0 (no redundancy) to 5 or 7. For details, refer to command-line interface (CLI) help. Default is 0.
hs -redundancy *value*	(Optional) (T.38 fax relay only) Specifies the number of redundant T.38 fax packets to be sent for high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. Range varies by platform from 0 (no redundancy) to 2 or 3. For details, refer to the command-line interface (CLI) help. Default is 0.
fallback	(Optional) A fallback mode is used to transfer a fax across a VoIP network if T.38 fax relay could not be successfully negotiated at the time of the fax transfer.
cisco	(Optional) Cisco-proprietary fax protocol.
none	(Optional) No fax pass-through or T.38 fax relay is attempted. All special fax handling is disabled, except for modem pass-through if configured with the **modem pass-through** command.
pass -through	(Optional) The fax stream uses one of the following high-bandwidth codecs: • **g711ulaw** --Uses the G.711 mu-law codec. • **g711alaw** --Uses the G.711 a-law codec.

Command Default

ls-redundancy 0 hs-redundancy 0 fallback none for the Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms**ls-redundancy 0 hs-redundancy 0 fallback cisco** for all other platforms

Command Modes

Voice-service configuration (config-voi-srv)

Command History

Release	Modification
12.2(13)T	This command was introduced.
15.1(1)T	This command was Modified. The **version** keyword was added with the **0** and **3** keywords to specify fax speed.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

Use the **fax protocol t38**command and the **voice service voip** command to configure T.38 fax relay capability for all VoIP dial peers. If the **fax protocol t38** (voice-service) command is used to set fax relay options for all dial peers and the **fax protocol t38** (dial-peer) command is used on a specific dial peer, the dial-peer configuration takes precedence over the global configuration for that dial peer.

If you specify **version 3** in the **fax protocol t38** command and negotiate T.38 version 3, the fax rate is automatically set to 33600.

The **ls-redundancy** and **hs-redundancy** keywords are used to send redundant T.38 fax packets. Setting the **hs-redundancy**keyword to a value greater than 0 causes a significant increase in the network bandwidth consumed by the fax call.

Use the **nse force** option when the H.323 or SIP gateway is interoperating with a Cisco MGCP gateway and the call agent does not support the interworking and negotiation of T.38 fax relay and NSE attributes at the time of call setup. When the corresponding option is configured on the MGCP gateway, the **nse force**option allows T.38 fax relay to be used between Cisco H.323 or SIP gateways and MGCP gateways.



Note Do not use the **cisco** keyword for the fallback option if you specified **version 3** for SG3 fax transmission.

Examples

The following example shows how to configure the T.38 fax protocol for VoIP:

```
voice service voip
 fax protocol t38
```

The following example shows how to use NSEs to unconditionally enter T.38 fax relay mode:

```
voice service voip
 fax protocol t38 nse
```

The following example shows how to specify the T.38 fax protocol for all VoIP dial peers, set low-speed redundancy to a value of 1, and set high-speed redundancy to a value of 0:

```
voice service voip
 fax protocol t38 ls-redundancy 1 hs-redundancy 0
```

Related Commands

Command	Description
fax protocol (dial peer)	Specifies the fax protocol for a specific VoIP dial peer.
fax protocol (voice-service)	Specifies the global default fax protocol to be used for all VoIP dial peers.
fax protocol t38 (dial peer)	Specifies the ITU-T T.38 standard fax protocol to be used for a specific VoIP dial peer.
voice service voip	Enters voice-service configuration mode.

fax rate (dial peer)

To establish the rate at which a fax is sent to a specified dial peer, use the **fax rate** command in dial-peer configuration mode. To reset the dial peer for voice calls, use the **no** form of this command.

fax rate {**2400** | **4800** | **7200** | **9600** | **12000** | **14400**} {**disable** | **voice**} [**bytes** *milliseconds*]
no fax rate

Syntax Description

2400	2400 bits per second (bps) fax transmission speed.
4800	4800 bps fax transmission speed.
7200	7200 bps fax transmission speed.
9600	9600 bps fax transmission speed.
12000	12000 bps fax transmission speed.
14400	14400 bps fax transmission speed.
disable	Disables fax relay transmission capability.
voice	Highest possible transmission speed allowed by the voice rate.
bytes *milliseconds*	(Optional) Specifies fax packetization rate, in milliseconds. Range is 20 to 48. Default is 20. • For Cisco fax relay, this keyword-argument pair is valid only on Cisco 2600 series, Cisco 3600 series, Cisco AS5300, and Cisco 7200 series routers. • For T.38 fax relay, this keyword-argument pair is valid only on Cisco AS5350, Cisco AS5400, and Cisco AS5850 routers. For other routers, the packetization rate for T.38 fax relay is fixed at 40 ms and cannot be changed.

Command Default

Voice rate

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced as the **fax-rate** command on the Cisco 3600.
12.0(2)XH	The **12000** keyword was added.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T and implemented on the Cisco MC3810.
12.1(3)T	The command name changed from **fax-rate** to **fax rate**(nonhyphenated).
12.1(3)XI	This command was implemented on the Cisco AS5300.

Release	Modification
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	The 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 following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

Use this command to specify the fax transmission rate to the specified dial peer.

The values for this command apply only to the fax transmission speed and do not affect the quality of the fax itself. The higher transmission speed values (14,400 bps) provide a faster transmission speed but monopolize a significantly large portion of the available bandwidth. The lower transmission speed values (2400 bps) provide a slower transmission speed and use a relatively smaller portion of the available bandwidth.

Note The fax call is not compressed using the **ip rtp header-compression** command because User Datagram Protocol (UDP) is being used and not Real-Time Transport Protocol (RTP). For example, a 9600 bps fax call takes approximately 24 kbps.

If the fax rate transmission speed is set higher than the codec rate in the same dial peer, the data sent over the network for fax transmission is above the bandwidth reserved for Resource Reservation Protocol (RSVP).

Tip Because a large portion of the available network bandwidth is monopolized by the fax transmission, Cisco does not recommend setting the fax rate value higher than the value of the selected codec. If the fax rate value is set lower than the codec value, faxes take longer to send but use less bandwidth.

The **voice** keyword specifies the highest possible transmission speed allowed by the voice rate. For example, if the voice codec is G.711, the fax transmission may occur at a rate up to 14,400 bps because 14,400 bps is less than the 64k voice rate. If the voice codec is G.729 (8k), the fax transmission speed is 7200 bps.

Examples

The following example configures a fax rate transmission speed of 9600 bps for faxes sent using a dial peer:

```
dial-peer voice 100 voip
 fax rate 9600 voice
```

The following example sets a fax rate transmission speed at 12,000 bps and the packetization rate at 20 milliseconds:

fax rate 12000 bytes 20

Related Commands

Command	Description
codec (dial peer)	Specifies the voice coder rate of speech for a dial peer.
fax protocol (dial peer)	Specifies the fax protocol for a specific VoIP dial peer.

fax rate (pots)

To establish the rate at which a fax is sent to the specified plain old telephone service (POTS) dial peer, use the **fax rate** command in dial-peer configuration mode. To reset the dial peer to handle only voice calls, use the **no** form of this command.

fax rate {**disable** | **system** | **voice**}
no fax rate

Syntax Description

disable	Disables fax-relay transmission capability.
system	Uses rate choice specified in global fax rate CLI under the **voice service pots**command.
voice	Highest possible transmission speed allowed by the voice rate for this dial peer. For example, if the voice codec is G.711, fax transmission may occur at a rate of up to 14,400 bps.

Command Default

System

Command Modes

dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.2(8)T	This command was introduced on the following platforms: Cisco 1700 series, Cisco 3600 series, and Cisco ICS 7750.

Usage Guidelines

This implementation of the **fax rate** command is only applicable to POTS dial peers.

Examples

The following example shows a fax rate transmission set to **voice** on POTS dial peer 1:

```
dial-peer voice 1 pots
 fax rate voice
```

Related Commands

Command	Description
codec (dial peer)	Specifies the voice coder rate of speech for a dial peer.
fax rate (voip)	Establishes the rate at which a fax is sent to the specified VoIP dial peer.

fax rate (voice-service)

To establish the rate at which a fax is sent for POTS-to-POTS voice calls, use the f**ax rate** command in voice-service configuration mode. To reset for voice only calls, use the **no** form of this command.

fax rate {**disable** | **voice**}
no fax rate

Syntax Description

disable	Disables fax relay transmission capability.
voice	Highest possible transmission speed allowed by the voice rate. For example, if the voice codec is G.711, fax transmission may occur at a rate of up to 14400 bps.

Command Default

fax rate voice command behavior is enabled by default

Command Modes

Voice service configuration (config-voi-serv)

Command History

Release	Modification
12.2(8)T	This command was introduced on the following platforms: Cisco 1700 series, Cisco 3600 series, and Cisco ICS 7750.
12.3(4)T	This command was modified so that the "fax rate voice" setting is the default setting for the **fax rate** command in voice-service configuration mode and, hence, will no longer be displayed in the running configuration.

Usage Guidelines

This implementation of the **fax rate** command applies only when voice service is set to POTS. Although **fax rate voice** command behavior is the default setting, you must specify this functionality in voice-service configuration mode in order to establish the rate at which a fax is sent for POTS-to-POTS voice calls. If you do not configure **fax rate voice** functionality and you do not specify **fax rate disable** command behavior, fax calls are processed as a regular voice calls and their completion is subject to line quality just like any other form of voice communication.



Note Because the **fax rate voice** command has been reclassified as a default setting, it will no longer automatically generate an entry in your gateway router's running configuration in NVRAM. If your gateway configuration requires **fax rate voice** command functionality, you must reconfigure your gateway after loading a Cisco IOS image earlier than Cisco IOS Release 12.3(4)T.

Examples

The following example shows voice service fax rate transmission set to **disable**:

```
voice service pots
 fax rate disable
```

Related Commands

Command	Description
fax protocol (voice -service)	Specifies the global default fax protocol for all VoIP dial peers.
voice service	Specifies the voice encapsulation type.

fax receive called-subscriber

To define the called subscriber identification (CSI), use the **fax receive called-subscriber command in**global configuration mode. To disable the configured CSI, use the **no** form of this command.

fax receive called-subscriber {**d***telephone-number*}
no fax receive called-subscriber {**d***telephone-number*}

Syntax Description

d	Wildcard that indicates that the information displayed is captured from the configured destination pattern.
telephone-number	Destination telephone number. Valid entries are the plus sign (+), numerals from 0 through 9, and the space character. This string can specify an E.164 telephone number; if you choose to configure an E.164 telephone number, you must use the plus sign as the first character.

Command Default

Enabled with a null string

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Use this command to define the number displayed in the liquid crystal display (LCD) of the sending fax device when you are sending a fax to a recipient. Typically, with a standard Group 3 fax device, this is the telephone number associated with the receiving fax device. The command defines the CSI.

This command applies to on-ramp store-and-forward fax functions.

Examples

The following example configures the number 555-0134 as the called subscriber number:

```
fax receive called-subscriber 5550134
```

fax-relay (dial peer)

To enable the suppression of call menu (CM) tones or answer (ANS) tones from reaching the Super Group 3 (SG3) fax machines, thereby forcing the SG3 fax machines to train down and negotiate to G3 speeds, to enable ANS tone treatment, or to disable fax-relay Error Correction Mode (ECM) on a VoIP dial peer, use the **fax-relay** command in dial peer configuration mode. To disable these functions, use the **no** form of this command.

fax-relay {**ans-disable** | **ans-treatment** | **ecm-disable** | **sg3-to-g3** [*system*]}
no fax-relay {**ans-disable** | **ans-treatment** | **ecm-disable** | **sg3-to-g3** [*system*]}

Syntax Description

ans-disable	Suppresses ANS tones at originating SG3 fax machines so that the SG3 fax machines can operate at G3 speeds using fax relay.
ans-treatment	Enables modem and fax answer tone treatment.
ecm-disable	Disables fax-relay ECM on a VoIP dial peer.
sg3-to-g3	Enables SG3 machines to negotiate to G3 speeds using fax relay.
system	(Optional) The protocol set to be used in the voice-service configuration mode.

Command Default

Modem upspeed occurs when ANS tones are detected. Fax-relay ECM is enabled.

ANS tone treatment is not enabled.

SG3 machines negotiate to G3 speeds using fax relay.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.1(3)T	This command was introduced as the **fax-relay ecm-disable** command.
12.1(5)XM	This command was integrated into Cisco IOS Release 12.1(5)XM and implemented on the Cisco AS5800 Series Universal Gateways.
12.1(5)XM2	This command was integrated into Cisco IOS Release 12.1(5)XM2 and implemented on the Cisco AS5350 and Cisco AS5400 Series Universal Gateways.
12.2(2)XB1	This command was integrated into Cisco IOS Release 12.2(2)XB1 and implemented on the Cisco AS5850 Series Universal Gateways.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.4(4)T	This command was modified. The **sg3-to-g3** *system* keyword and argument pair was added.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T and implemented on Cisco 1700 and Cisco 2800 Series routers.

Release	Modification
12.4(20)T1	This command was modified. The **ans-disable** keyword was added to support the suppression of ANS tones from reaching the SG3 fax machines, thereby enabling the SG3 fax machines to negotiate to G3 speeds.
15.1(4)M	This command was modified. The **ans-treatment** keyword was added to support the modem and fax ANS tone treatment.

Usage Guidelines

The **ans-disable** keyword helps to ensure that modem upspeed does not occur when ANS tones are detected. When the **fax-relay ans-disable** command is enabled, modem-related sessions fail because the ANS tones are squelched at the digital signal processor (DSP) level by the TI C5510 DSP.

When the **fax-relay ans-treatment** command is enabled, the modem and fax ANS tone treatment is enabled. An ANS tone is a modem answer tone of 2100 Hz. Occasionally, the ANS tone is followed by a phase reversal. ANS tone treatment is a mechanism to handle ANS tones with or without phase reversal and to generate/transmit RFC 2833 modem tone events on detection of ANS tones. For ANS tone treatment to be triggered, the **dtmf-relay rtp-nte** command has to be enabled in dial peer configuration mode and the RFC 2833 Dual Tone Multifrequency (DTMF) relay has to be negotiated for the audio session.

When the **fax-relay ecm-disable** command is enabled, the DSP fax-relay firmware disables ECM by modifying the Digital Information Signal (DIS) T.30 message when the DSP channel starts the fax relay and cannot be changed during the fax relay. ECM disable is performed on DIS signals in both directions so that ECM is disabled in both directions even if only one gateway is configured with ECM disabled. This setting is provisioned when the DSP channel starts fax relay and cannot be changed during the fax relay session.

When the **fax-relay sg3-to-g3** command is enabled, the DSP fax-relay firmware suppresses the V.8 CM tone and the fax machines negotiate down to G3 speeds for the fax stream. Modem communication is impacted if the session does not negotiate either modem passthrough or relay. Use this command for H.323 and Session Initiation Protocol (SIP) signaling types.

The **fax-relay** command is also available in voice-service configuration mode, but the **ecm-disable** *system* keyword and argument pair is not available in voice-service configuration mode.

Examples

The following example shows how to disable ECM on the voice dial peer:

```
Device> enable
Device(config)# dial-peer voice 25 voip
Device(config-dial-peer)# fax-relay ecm-disable
```

The following example shows how to enable SG3 V.8 fax CM message suppression on the voice dial peer for H.323 and SIP signaling types:

```
Device> enable
Device(config)# dial-peer voice 25 voip
Device(config-dial-peer)# fax-relay sg3-to-g3
```

The following dial-peer configuration shows how to enable ANS tone squelching at the DSP level for all VoIP dial peers:

```
Device> enable
Device(config)# dial-peer voice 25 voip
Device(config-dial-peer)# fax-relay ans-disable
```

The following example shows how to enable ANS tone treatment:

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 25 voip
Device(config-dial-peer)# dtmf-relay rtp-nte
Device(config-dial-peer)# modem passthrough nse codec g711ulaw redundancy maximum-session
5
Device(config-dial-peer)# fax-relay ans-treatment
Device(config-dial-peer)# exit
```

Related Commands

Command	Description
dtmf-relay (Voice over IP)	Forwards dual tone multifrequency tones by using RTP with the NTE payload type.
fax-relay (voice-service)	Allows ANS tones to be disabled for SG3 machines to operate at G3 speeds using fax relay, enables ANS tone treatment, or enables the fax stream between two SG3 fax machines to negotiate to G3 speeds on a VoIP dial peer.
mgcp fax-relay	Allows ANS tones to be disabled for SG3 machines to operate at G3 speeds for MGCP fax relay or enables the fax stream between two SG3 fax machines to negotiate down to G3 speeds for MGCP fax relay.
modem passthrough (Dial-peer)	Enables fax or modem pass-through over VoIP for a specific dial peer.

fax-relay (voice-service)

To enable the suppression of call menu (CM) tones or answer (ANS) tones from reaching the Super Group 3 (SG3) fax machines, thereby forcing the SG3 fax machines to train down and negotiate to G3 speeds, or to enable answer (ANS) tone treatment, use the **fax-relay** command in voice-service configuration mode. To disable these functions, use the **no** form of this command.

fax-relay {**ans-disable** | **ans-treatment** | **sg3-to-g3**}
no fax-relay {**ans-disable** | **ans-treatment** | **sg3-to-g3**}

Syntax Description

ans-disable	Suppresses ANS tones at originating SG3 fax machines so that the SG3 fax machines can operate at G3 speeds using fax relay.
ans-treatment	Enables modem and fax answer tone treatment.
sg3-to-g3	Enables SG3 machines to negotiate to G3 speeds using fax relay.

Command Default

Modem upspeed occurs when ANS tones are detected.

ANS tone treatment is not enabled.

SG3 machines negotiate to G3 speeds using fax relay.

Command Modes

Voice-service configuration (conf-voi-serv)

Command History

Release	Modification
12.4(4)T	This command was introduced as the **fax-relay sg3-to-g3** command.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T and implemented on Cisco 1700 and Cisco 2800 Series routers.
12.4(20)T	This command was modified. The **ans-disable** keyword was added to support the suppression of ANS tones from reaching the SG3 fax machines, thereby enabling the SG3 fax machines to negotiate to G3 speeds.
15.1(4)M	This command was modified. The **ans-treatment** keyword was added to support the modem and fax ANS tone treatment.

Usage Guidelines

The **ans-disable** keyword helps to ensure that modem upspeed does not occur when ANS tones are detected. When the **fax-relay ans-disable** command is enabled, modem-related sessions fail because the ANS tones are squelched at the digital signal processor (DSP) level by the TI C5510 DSP.

When the **fax-relay ans-treatment** command is enabled, the modem and fax ANS tone treatment is enabled. An ANS tone is a modem answer tone of 2100 Hz. Occasionally, the ANS tone is followed by a phase reversal.

ANS tone treatment is a mechanism to handle ANS tones with or without phase reversal and to generate/transmit RFC 2833 modem tone events on detection of ANS tones. For ANS tone treatment to be triggered, the **dtmf-relay rtp-nte** command has to be enabled in voice-service configuration mode and the RFC 2833 Dual Tone Multifrequency (DTMF) relay has to be negotiated for the audio session.

When the **fax-relay sg3-to-g3** command is enabled, the DSP fax-relay firmware suppresses the V.8 CM tone and the fax machines negotiate down to G3 speeds for the fax stream. Modem communication is impacted if the session does not negotiate either modem passthrough or relay. Use this command for H.323 and Session Initiation Protocol (SIP) signaling types.

Examples

The following example shows how to enable SG3 V.8 fax CM message suppression for all VoIP dial peers:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# fax-relay sg3-to-g3
```

The following example shows how to enable ANS tone squelching at DSP level for all VoIP dial peers:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# fax-relay ans-disable
```

The following example shows how to enable ANS tone treatment:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# dtmf-relay rtp-nte
Device(conf-voi-serv)# modem passthrough nse codec g711ulaw redundancy maximum-session 5
Device(conf-voi-serv)# fax-relay ans-treatment
Device(conf-voi-serv)# exit
```

Related Commands

Command	Description
dtmf-relay (Voice over IP)	Forwards dual tone multifrequency tones by using RTP with the NTE payload type.
fax-relay (dial-peer)	Allows ANS tones to be disabled for SG3 machines to operate at G3 speeds using fax relay, enables ANS tone treatment, disables fax-relay ECM on a VoIP dial peer, or enables the fax stream between two SG3 fax machines to negotiate to G3 speeds on a VoIP dial peer.

Command	Description
mgcp fax-relay	Allows ANS tones to be disabled for SG3 machines to operate at G3 speeds for MGCP fax relay or enables the fax stream between two SG3 fax machines to negotiate to G3 speeds for MGCP fax relay.
modem passthrough (Voice-service)	Enables fax or modem pass-through over VoIP globally for all dial peers.

fax send center-header

To specify the data that appears in the center position of the fax header information, use the **fax send center-header command in**global configuration mode. To remove the selected options, use the **no** form of this command.

fax send center-header {**$a** | **$d$** | **$p$** | **$s$** | **$t$**} *string*
no fax send center-header {**$a** | **$d$** | **$p$** | **$s$** | **$t$**} *string*

Syntax Description

a	Wildcard that inserts the date in the selected position.
d	Wildcard that inserts the destination address in the selected position.
p	Wildcard that inserts the page count in the selected position.
s	Wildcard that inserts the sender's address in the selected position.
t	Wildcard that inserts the transmission time in the selected position.
string	Text string that provides personalized information. Valid characters are any text plus wildcards--for example, Time:t. There is no default.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Mail messages that contain only text or contain text attachments (text of the MIME media type) can be converted by the off-ramp gateway into a format understood by a fax machine's text-to-fax converter. When this conversion is performed, this command indicates what header information is added to the center top position of those pages.

Mail messages with TIFF attachments (MIME media image type and TIFF subtype) are expected to include their own per-page headers.



Note Faxed header information cannot be converted from TIFF files to standard fax transmissions.

This command lets you configure several options by combining one or more wildcards with text string information to customize your fax header information.



Note If the information you have selected for the **fax send center-header** command exceeds the space allocated for the center fax header, the information is truncated.

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example selects the fax transmission time as the centered fax header:

```
fax send center-header $t$
```

The following example configures the company name "widget" and its address as the centered fax header:

```
fax send center-header widget $s$
```

Related Commands

Command	Description
fax send left -header	Specifies the data that appears on the left in the fax header.
fax send right -header	Specifies the data that appears on the right in the fax header.

fax send coverpage comment

To define customized text for the title field of a fax cover sheet, use the **fax send coverpage comment command in**global configuration mode. To disable the defined comment, use the **no** form of this command.

fax send coverpage comment *string*
no fax send coverpage comment *string*

Syntax Description

string	Text string that adds customized text in the title field of the fax cover sheet. Valid characters are any ASCII characters.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

This command can be overridden by the **fax send coverpage e-mail-controllable** command.

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example configures an individualized title comment of "XYZ Fax Services" for generated fax cover sheets:

```
fax send coverpage enable
fax send coverpage comment XYZ Fax Services
```

Related Commands

Command	Description
fax send coverpage e -mail-controllable	Controls the cover page generation on a per-recipient basis, based on the information contained in the destination address of the e-mail message.
fax send coverpage enable	Generates fax cover sheets.
fax send coverpage show -detail	Prints all of the e-mail header information as part of the fax cover sheet.

fax send coverpage e-mail-controllable

To defer to the cover page setting in the e-mail header to generate a standard fax cover sheet, use the **fax send coverpage e-mail-controllable command in**global configuration mode. To disable standard fax sheet generation, use the **no** form of this command.

fax send coverpage e-mail-controllable
no fax send coverpage e-mail-controllable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300 universal access server.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750 access router.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

You can also use the destination address of an e-mail message to control the cover page generation on a per-recipient basis. Use thiscommand to configure the router to defer to the cover page setting in the e-mail header.

In essence, the off-ramp router defers to the setting configured in the e-mail address itself. For example, if the address has a parameter set to cover=no, this parameter overrides the setting for the **fax send coverpage enable** command, and the off-ramp gateway does not generate and send a fax cover page. If the address has a parameter set to cover=yes, the off-ramp gateway defers to this parameter setting to generate and send a fax cover page.

The table below shows examples of what the user would enter in the To: field of the e-mail message.

Table 9: Sample Entries for the To: Field

To: Field Entries	Description
FAX=+1-312-555-3260@fax.com	Fax sent to an E.164-compliant long distance telephone number in the United States. If the **fax coverpage enable**command is entered, store-and-forward fax generate a fax cover page.
FAX=+1-312-555-3260/cover=no@fax.com	Fax sent to an E.164-compliant long distance telephone number in the United States. In this example, the **fax send coverpage enable** command is superseded by the cover=no statement. No cover page is generated.

To: Field Entries	Description
FAX=+1-312-555-3260/cover=yes@fax.com	Fax sent to an E.164-compliant long distance telephone number in the United States. In this example, the **fax send coverpage enable** command is superseded by the cover=yes statement. Store-and-forward fax generates a fax cover page.



Note This command applies to off-ramp store-and-forward fax functions.

Examples

The following example enables standard generated fax cover sheets:

```
fax send coverpage enable
fax send coverpage e-mail-controllable
```

Related Commands

Command	Description
fax send coverpage comment	Defines customized text for the title field of a fax cover sheet.
fax send coverpage enable	Generates fax cover sheets.
fax send coverpage show -detail	Prints all the e-mail header information as part of the fax cover sheet.

fax send coverpage enable

To generate fax cover sheets for faxes that were converted into e-mail messages, use the **fax send coverpage enable** command in global configuration mode. To disable fax cover sheet generation, use the **no** form of this command.

fax send coverpage enable
no fax send coverpage enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

This command applies to off-ramp store-and-forward fax functions.

Note This command is applicable only to faxes that were converted to e-mail messages. The Cisco AS5300 universal access server does not alter fax TIFF attachments. Therefore you cannot use this command to enable the Cisco AS5300 to generate fax cover pages for faxes that are converted from TIFF files to standard fax transmissions.

Examples

The following example enables the generation of fax cover sheets:

```
fax send coverpage enable
```

Related Commands

Command	Description
fax send coverpage comment	Defines customized text for the title field of a fax cover sheet.
fax send coverpage e -mail-controllable	Defers to the cover page setting in the e-mail header to generate a standard fax cover sheet
fax send coverpage show -detail	Prints all the e-mail header information as part of the fax cover sheet.

fax send coverpage show-detail

To display all e-mail header information as part of the fax cover sheet, use the **fax send coverpage show-detail**command in global configuration mode. To prevent the e-mail header information from being displayed, use the **no** form of this command.

fax send coverpage show-detail
no fax send coverpage show-detail

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

This command applies to off-ramp store-and-forward fax functions.

Note This command is applicable only to faxes that are converted to e-mail messages. The Cisco AS5300 universal access server does not alter fax TIFF attachments. Therefore, you cannot use this command to enable the Cisco AS5300 to display additional fax cover page information for faxes that are converted from TIFF files to standard fax transmissions.

Examples

The following example configures an individualized generated fax cover sheet that contains the e-mail header text:

```
fax send coverpage enable
no fax send coverpage e-mail-controllable
fax send coverpage show-detail
```

Related Commands

Command	Description
fax send coverpage comment	Defines customized text for the title field of a fax cover sheet.

Command	Description
fax send coverpage e -mail-controllable	Defers to the cover page setting in the e-mail header to generate a standard fax cover sheet.
fax send coverpage enable	Generates fax cover sheets.

fax send left-header

To specify the data that appears on the left in the fax header, use the **fax send left-header** command in global configuration mode. To disable the selected options, use the **no** form of this command.

fax send left-header {**$a** | **$d$** | **$p$** | **$s$** | **$t$**} *string*
no fax send left-header {**$a** | **$d$** | **$p$** | **$s$** | **$t$**} *string*

Syntax Description

a	Wildcard that inserts the date in the selected position.
d	Wildcard that inserts the destination address in the selected position.
p	Wildcard that inserts the page count in the selected position.
s	Wildcard that inserts the sender's address in the selected position.
t	Wildcard that inserts the transmission time in the selected position.
string	Text string that provides customized information. Valid characters are any combination of ASCII characters and the wildcards listed above.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Mail messages that contain only text or text attachments (text of MIME media type) can be converted by the off-ramp device into a format understood by fax machines using a text-to-fax converter. When this conversion is performed, the **fax send left-header** command is used to indicate what header information should be added to the top left of those pages.

Mail messages with TIFF attachments (MIME media image type and TIFF subtype) are expected to include their own per-page headers, and the Cisco IOS software does not modify TIFF attachments.

This command lets you configure several options at once by combining one or more wildcards with text string information to customize your fax header information.

If the information you select for the **fax send left-header** command exceeds the space allocated for the left fax header, the information is truncated.

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example puts the fax transmission time on the left side of the fax header:

```
fax send left-header $t$
```

The following example puts the company name "widget" and its address on the left side of the fax header:

```
fax send left-header widget $s$
```

Related Commands

Command	Description
fax send center-header	Specifies the data that appears in the center of the fax header.
fax send right-header	Specifies the data that appears on the right in the fax header.

fax send max-speed

To specify the maximum speed at which an outbound fax is transmitted, use the **fax send max-speed command in**global configuration mode. To disable the selected speed, use the **no** form of this command.

fax send max-speed {**2400** | **4800** | **7200** | **9600** | **12000** | **14400**}
no fax send max-speed {**2400** | **4800** | **7200** | **9600** | **12000** | **14400**}

Syntax Description

2400	Transmission speed of 2400 bits per second (bps).
4800	Transmission speed of 4800 bps.
7200	Transmission speed of 7200 bps.
9600	Transmission speed of 9600 bps.
12000	Transmission speed of 12,000 bps.
14400	Transmission speed of 14,400 bps. This is the default.

Command Default

14,400 bps

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example sets the outbound fax transmission rate at 2400 bps:

```
fax send max-speed 2400
```

fax send right-header

To specify the data that appears on the right in the fax header information, use the **fax send right-header command in**global configuration mode. To disable the selected options, use the **no** form of this command.

fax send right-header {**$a** | **$d$** | **$p$** | **$s$** | **$t$**} *string*
no fax send right-header {**$a** | **$d$** | **$p$** | **$s$** | **$t$**} *string*

Syntax Description

a	Wildcard that inserts the date in the selected position.
d	Wildcard that inserts the destination address in the selected position.
p	Wildcard that inserts the page count in the selected position.
s	Wildcard that inserts the sender address in the selected position.
t	Wildcard that inserts the transmission time in the selected position.
string	Text string that provides customized information. Valid characters are any combination of ASCII characters and the wildcards listed above.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Mail messages that contain only text or text attachments (text of MIME media type) can be converted by the off-ramp device into a format understood by fax machines using the text-to-fax converter. When this conversion is performed, this command is used to indicate what header information should be added to top right of those pages.

Mail messages with TIFF attachments (MIME media image type and TIFF subtype) are expected to include their own per-page headers, and the Cisco IOS software does not modify TIFF attachments.

This command lets you configure several options at once by combining one or more wildcards with text string information to customize your fax header information.

Note If the information you select for the **fax send right-header**command exceeds the space allocated for the right fax header, the information is truncated.

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example puts the fax date in the right-hand side of the fax header:

```
fax send right-header $a$
```

The following example puts the company name "XYZ" and its address in the right-hand side of the fax header:

```
fax send right-header XYZ $s$
```

Related Commands

Command	Description
fax send center -header	Specifies the data that appears in the center in the fax header.
fax send left -header	Specifies the data that appears on the left in the fax header.

fax send transmitting-subscriber

To define the transmitting subscriber information (TSI), use the **fax send transmitting-subscriber**command in global configuration mode. To disable the configured value, use the **no** form of this command.

fax send transmitting-subscriber {**s***string*}
no fax send transmitting-subscriber {**s***string*}

Syntax Description

s	Wildcard that inserts the sender name from the RFC 822 header (captured by the on-ramp device from the sending fax machine) in the selected position.
string	Originating telephone number. Valid entries are the plus sign (+), numerals from 0 through 9, and the space character. This string can specify an E.164 telephone number; if you choose to configure an E.164 telephone number, you must use the plus sign as the first character.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

The transmitting subscriber number is the number of the originating fax and is displayed in the LCD of the receiving fax device. Typically, with a standard Group 3 fax device, this number is the telephone number associated with the transmitting or sending fax device. This command defines the TSI.

This command applies to off-ramp store-and-forward fax functions.

Examples

The following example configures the company number as captured by the on-ramp device from the sending fax machine:

```
fax send transmitting-subscriber +14085550134
```

file-acct flush

To manually flush call detail records (CDRs) from the buffer to the accounting file, use the **file-acct flush** command in privileged EXEC mode.

file-acct flush {**with-close** | **without-close**}

Syntax Description

with-close	Call records are appended to the accounting file and the file is closed.
without-close	Call records are appended to the accounting file and the file remains open.

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

Use this command if you need to manually flush the buffer, for example, if flash becomes full or you do not want to wait until the buffer is automatically flushed. This command immediately flushes the buffer and appends all CDRs in the buffer to the current accounting file. CDRs are automatically flushed from the buffer and written to the file whenever there is enough data based on the **maximum buffer-size** command or after the timer set with the **maximum cdrflush-timer** command expires.

Using the **with-close** keyword closes the current file and opens a new file after appending the records. Using the **without-close** keyword leaves the current file open after appending the records.

Examples

The following example appends the records to the accounting file and closes the file:

```
file-acct flush with-close
```

Related Commands

Command	Description
gw-accounting	Enables an accounting method for collecting CDRs.
maximum buffer-size	Sets the maximum size of the file accounting buffer.
maximum cdrflush-timer	Sets the maximum time to hold call records in the buffer before appending the records to the accounting file.
maximum fileclose-timer	Sets the maximum time for saving records to an accounting file before closing the file and creating a new one.
primary	Sets the primary location for storing the CDRs generated for file accounting.
secondary	Sets the backup location for storing CDRs if the primary location becomes unavailable.

file-acct reset

To manually switch back to the primary device for file accounting, use the **file-acct reset** command in privileged EXEC mode.

file-acct reset

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

This command allows you to switch back to the primary device when it becomes available if the backup device is currently being used because the primary device failed.

If the file transfer to the primary device fails, the file accounting process retries the primary device up to the number of times defined by the **maximum retry-count** command and then switches to the secondary device defined with the **secondary** command. This command flushes the buffer and writes the call detail records (CDRs) to the currently active file before resetting to the primary device and opening a new file.

If the secondary device also fails, the accounting process ends and the system logs an error. New CDRs are dropped until one device comes back online and you use this command. The system then immediately resets to the primary device, if available.

Examples

The following example shows how to switch back to the primary device:

```
Router# file-acct reset
```

Related Commands

Command	Description
gw-accounting	Enables an accounting method for collecting CDRs.
maximum retry-count	Sets the maximum number of times the router attempts to connect to the primary file device before switching to the secondary device
primary	Sets the primary location for storing the CDRs generated for file accounting.
secondary	Sets the backup location for storing CDRs if the primary location becomes unavailable.

filter voice

To specify that voice calls bypass authentication, authorization, and accounting (AAA) preauthentication, use the **filter voice** command in AAA preauthentication configuration mode. To disable AAA bypass, use the **no** form of this command.

filter voice
no filter voice

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

AAA preauthentication configuration (config-preauth)

Command History

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

Examples

The following example specifies that voice calls bypass AAA preauthentication:

```
Router(config)# aaa preauth
Router(config-preauth)# filter voice
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication configuration mode.

flush

To enable file mode accounting flush options, use the **flush**command in privileged EXEC mode.

flush {**with-close** | **without-close**}

Syntax Description

with-close	Enables file accounting flush pending accounting to the file, and closes the file when the process is complete.
without-close	Enables file accounting flush pending accounting to file.

Command Default

File mode accounting flush options are not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **flush** command flushes pending accounting records to the file.

Examples

In the following example, the **flush with-close**command enables file accounting flush pending accounting to the file, and closes the file when the process is complete:

```
Router# flush with-close
```

Related Commands

Command	Description
maximum cdrflush-timer	Sets the maximum time to hold call records in the buffer before appending the records to the accounting file.

fmtp

To set a format-specific string for a codec, use the **fmtp** command in codec-profile configuration mode. To disable the format string, use the **no** form of this command.

fmtp *string*
no fmtp

Syntax Description

string	fmtp:payload type name1= val1; name2 = val2...

For Cisco Unified Customer Voice Portal (Cisco Unified CVP), the dynamic payload number is in the range of 96 to 127 for H.263+. For H263, it is always 34. For H.263+, this number must be entered but it is not used. Cisco Unified CVP uses either the default value for H.263+ (118) or the value defined for the VoIP dial peer using the command **rtp payload-type cisco-codec-video-h263+ ,**a number in the range 96 to 127.

Other parameters can be the following:

- SQCIF = 1 - 32
- QCIF = 1 - 32
- CIF = 1 - 32
- 4CIF = 1 - 32
- 16CIF = 1 - 32
- MAXBR (max bitrate) = Value in 100 bits per second (500 = 50000 bits per second). This value is another that is not used. Always set H.324 to 50K.
- D--1 (Enable H.263 Annex D)
- F--1 (Enable H.263 Annex F)
- I--1 (Enable H.263 Annex I)
- J--1 (Enable H.263 Annex J)
- K--1 to 4 (Enable H.263 Annex K) (Annex K is Slice Structured Mode)
  - 1--Slices In Order, Nonrectangular
  - 2--Slices In Order, Rectangular
  - 3--Slices Not Ordered, Nonrectangular
  - 4--Slices Not Ordered, Rectangular
- N=[1,4] (Enable H.263 Annex N) (Annex N is Reference Picture Selection Mode)
  - 1--NEITHER: No back-channel data is returned from the decoder to the encoder.
  - 2--ACK: The decoder returns only acknowledgment messages.
  - 3--NACK: The decoder returns only nonacknowledgment messages.
  - 4--ACK+NACK: The decoder returns both acknowledgment and nonacknowledgment messages.
- P=[x,y] (Enable H.263 Annex P) (Annex P is Reference Picture Resampling). Annex P can have either one or two parameters, depending on the values selected. There are four options, and six valid combinations.

- 1--dynamicPictureResizingByFour
- 2--dynamicPictureResizingBySixteenthPel
- 3--dynamicWarpingHalfPel
- 4--dynamicWarpingSixteenthPel.

The valid combinations are:

-
  - 1
  - 1,3
  - 2
  - 2, 3
  - 2, 4
  - 3
- T=1 (Enable H.263 Annex T)
- CUSTOM = x, y, MPI -- Defines a custom picture format, where X is the X-axis size in pixels, Y is the Y-axis size in pixels, and MPI is the frame rate (30/(1.001*MPI)). X and Y must be divisible by 4, and MPI has a value of 1to 32.

Command Default

No string is configured.

Command Modes

Codec-profile configuration (config-codec-profile)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

The profile is selected by entering the command:

video codec h263/h263+ profile 1000

The video codec h263/h263+ profile can be used in a voip dial peer or as a voice class codec entry.

Examples

The following example shows an fmtp string for video codec profile 116:

```
codec profile 116 H263
 clockrate 90000
 fmtp "fmtp:120 SQCIF=1;QCIF=1;CIF=1;CIF4=2;MAXBR=3840;I=1"
```

Related Commands

Command	Description
clock-rate	Sets the clock rate for the codec.

forward-alarms

To turn on alarm forwarding so that alarms that arrive on one T1/E1 port are sent to the other port on dual-mode multiflex trunk interface cards, use the **forward-alarms** command in controller configuration mode on the one port. To reset to the default so that no alarms are forwarded, use the **no** form of this command.

forward-alarms
no forward-alarms

Syntax Description

This command has no arguments or keywords.

Command Default

Alarm forwarding is disabled

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

When you enter this command, physical-layer alarms on the configured port are forwarded to the other port on dual-port cards, simulating a one-way repeater operations. The system forwards RAIs (remote alarm indications, or Yellow Alarms), alarm indication signals (AIS, or Blue Alarms), losses of frame (LOF alarms, or Red Alarms), and losses of signaling (LOS alarms, or Red Alarms).

Examples

The following example turns on alarm forwarding on controller E1 0/0:

```
controller e1 0/0
 forward-alarms
```

forward-digits

To specify which digits to forward for voice calls, use the **forward-digits** command in dial peer configuration mode. To specify that any digits not matching the destination-pattern are not to be forwarded, use the no form of this command.

forward-digits {*num-digit* | **all** | **extra**}
no forward-digits

Syntax Description

num -digit	The number of digits to be forwarded. If the number of digits is greater than the length of a destination phone number, the length of the destination number is used. Range is 0 to 32. Setting the value to 0 is equivalent to entering the **no forward-digits** command.
all	Forwards all digits. If **all** is entered, the full length of the destination pattern is used.
extra	If the length of the dialed digit string is greater than the length of the dial-peer destination pattern, the extra right-justified digits are forwarded. However, if the dial-peer destination pattern is variable length ending with the character "T" (for example: T, 123T, 123...T), extra digits are not forwarded.

Command Default

Dialed digits not matching the destination pattern are forwarded

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(2)T	This command was integrated into Cisco IOS Release 12.0(2)T. The **implicit option** keyword was added.
12.0(4)T	This command was modified to support ISDNBF PRI QSIG signaling calls.
12.0(7)XK	This command was implemented on the Cisco 2600 series and Cisco 3600 series. The **implicit** keyword was removed and the **extra** keyword was added.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

This command applies only to POTS dial peers. Forwarded digits are always right justified so that extra leading digits are stripped. The destination pattern includes both explicit digits and wildcards if present.

For QSIG ISDN connections, entering the **forward-digits all** command implies that all the digits of the called party number are sent to the ISDN connection. When the **forward-digits** *num-digit* command and a number from 1 to 32 are entered, the number of digits of the called party number specified (right justified) are sent to the ISDN connection.

Examples

The following example shows that all digits in the destination pattern of a POTS dial peer are forwarded:

```
dial-peer voice 1 pots
 destination-pattern 8...
 forward-digits all
```

The following example shows that four of the digits in the destination pattern of a POTS dial peer are forwarded:

```
dial-peer voice 1 pots
 destination-pattern 555....
 forward-digits 4
```

The following example shows that the extra right-justified digits that exceed the length of the destination pattern of a POTS dial peer are forwarded:

```
dial-peer voice 1 pots
 destination-pattern 555....
 forward-digits extra
```

Related Commands

Command	Description
destination-pattern	Defines the prefix or the full E.164 telephone number to be used for a dial peer.
show dial-peer voice	Displays configuration information for dial peers.

forward-to-voicemail

To configure forwarding of calls to voicemail so that all incoming calls to a directory number are forwarded to voicemail, use the **forward-to-voicemail** command. The **stcapp feature access-code** command must be enabled on the Cisco voice gateway. To disable call forwarding, use the **no** form of this command.

forward-to-voicemail *forward-to-voicemail-code*
no forward-to-voicemail

Syntax Description

forward-to-voicemail-code	Default prefix and code is **7.
keypad-character	In Cisco IOS Release 15.0(1)M and later releases, the string can be either of the following: • Three digits (000-999) • Four digits (0000-9999)

Command Default

Call forwarding to voicemail is not set.

Command Modes

STC application feature access-code configuration (config-stcapp-fac).

Command History

Cisco IOS Release	Cisco Product	Modification
12.4(11)T	Cisco Unified CME 4.0(3)	This command was introduced.
15.0(1)M	--	This command was modified. The default user behavior of the feature access code was modified.

Usage Guidelines

In Cisco IOS Release 15.0(1)M and later releases, if the length of the keypad-character argument is three or four digits, phone users are not required to dial a prefix or any special characters to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **2. If the feature code is 788, the phone user dials only 788, without the FAC prefix, to access the corresponding feature.

The FAC for forward-to-voicemail follows the same rules as for other FAC, such as **call forward all** in terms of allowable string as its FAC code.

Examples

The following example show how to configure forward-to-voicemail using a four digit code:

```
VG224(config-stcapp-fac)# forward-to-voicemail 1234

do not use prefix. forward-to-voicemail is 1234
```

Related Commands

Command	Description
call-forward all	Configures call forwarding so that all incoming calls to a particular directory number are forwarded to another directory number.

Command	Description
call forward cancel	Defines a feature code for a FAC to cancel the call-forward-all condition.
show stcapp feature codes	Displays all FACs.
stcapp feature access-code	Enables FACs and enters STC application feature access-code configuration mode for changing values of the prefix and features codes from the default.

frame-relay voice bandwidth

To specify how much bandwidth should be reserved for voice traffic on a specific data-link connection identifier (DLCI), use the **frame-relay voice bandwidth** command in map-class configuration mode. To release the bandwidth previously reserved for voice traffic, use the **no** form of this command.

frame-relay voice bandwidth *bits-per-second*
no frame-relay voice bandwidth *bits-per-second*

Syntax Description

bits-per-second	Bandwidth, in bits per second (bps), reserved for voice traffic for the specified map class. Range is from 8000 to 45000000. Default is 0, which disables voice calls.

Command Default

Disabled (zero)

Command Modes

Map-class configuration (config-map-class)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.0(5)T	The **queue** *depth* keyword and argument were added.
12.2(1)	The **queue** *depth* keyword and argument were removed.

Usage Guidelines

To use this command, you must first associate a Frame Relay map class with a specific DLCI and then enter map-class configuration mode and set the amount of bandwidth to be reserved for voice traffic for that map class.

If a call is attempted and there is not enough remaining bandwidth reserved for voice to handle the additional call, the call is rejected. For example, if 64 kbps is reserved for voice traffic and a codec and payload size is being used that requires 10 kbps of bandwidth for each call, the first six calls attempted are accepted, but the seventh call is rejected.

Reserve queues are not required for Voice over Frame Relay (VoFR).

Note Cisco strongly recommends that you set voice bandwidth to a value less than the committed information rate (CIR) if Frame Relay traffic shaping is configured. Cisco also strongly recommends that you set the minimum CIR (using the **frame-relay mincir** command) to be at least equal to or greater than the voice bandwidth.

Calculating Required Bandwidth

The bandwidth required for a voice call depends on the bandwidth of the codec, the voice packetization overhead, and the voice frame payload size. The smaller the voice frame payload size, the higher the bandwidth required for the call. To make the calculation, use the following formula:

required_bandwidth = codec_bandwidth x (1 + overhead / payload_size)

As an example, the overhead for a VoFR voice packet is between 6 and 8 bytes: a 2-byte Frame Relay header, a 1- or 2-byte FRF.11 header (depending on the CID value), a 2-byte cyclic redundancy check (CRC), and a 1-byte trailing flag. If voice sequence numbers are enabled in the voice packets, there is an additional 1-byte sequence number. The table below shows the required voice bandwidth for the G.729 8000-bps speech coder for various payload sizes.

Table 10: Required Voice Bandwidth Calculations for G.729

Codec	Codec Bandwidth	Voice Frame Payload Size	Required Bandwidth per Call (6-Byte OH)	Required Bandwidth per Call (8-Byte OH)
G.729	8000 bps	120 bytes	8400 bps	8534 bps
G.729	8000 bps	80 bytes	8600 bps	8800 bps
G.729	8000 bps	40 bytes	9200 bps	9600 bps
G.729	8000 bps	30 bytes	9600 bps	10134 bps
G.729	8000 bps	20 bytes	10400 bps	11200 bps

To configure the payload size for the voice frames, use the **codec** command from dial-peer configuration mode.

Examples

The following example shows how to reserve 64 kbps for voice traffic for the "vofr" Frame Relay map class:

```
interface serial 1/1
 frame-relay interface-dlci 100
  class vofr
  exit
map-class frame-relay vofr
 frame-relay voice bandwidth 64000
```

Related Commands

Command	Description
codec (dial-peer)	Specifies the voice coder rate of speech for a VoFR dial peer.
frame-relay fair-queue	Enables weighted fair queueing for one or more Frame Relay PVCs.
frame-relay fragment	Enables fragmentation for a Frame Relay map class.
frame-relay interface-dlci	Assigns a DLCI to a specified Frame Relay subinterface on the router or access server.
frame-relay mincir	Assigns the minimum CIR for Frame Relay traffic shaping.
map-class frame-relay	Specifies a map class to define QoS values for an SVC.

freq-max-delay

To specify the maximum timing difference allowed between the two frequencies for detection of a tone, use the **freq-max-delay** commandin voice-class configuration mode. To reset to the default allowed timing difference, use the **no** form of this command.

freq-max-delay *time*
no freq-max-delay

Syntax Description

time	Maximum number of 10-millisecond time intervals by which the two frequencies in a tone may differ from each other and be detected. Range is from 10 to 100 (100 milliseconds to 1 second). Default is 10 (100 milliseconds).

Command Default

10 (100 milliseconds)

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.1(5)XM	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 1750.

Usage Guidelines

This command creates a detection limit for one parameter within a voice class that you can apply to any voice port.

You must specify a time value greater than the timing difference expected in the tone to be detected.

Examples

The following example configures a maximum timing difference of 200 milliseconds for voice class 100:

```
voice class dualtone 100
 freq-max-delay 20
```

The following example configures a maximum timing difference of 160 milliseconds for voice class 70:

```
voice class dualtone-detect-params 70
 freq-max-delay 160
```

Related Commands

Command	Description
dualtone	Defines the tone and cadence for a custom call-progress tone.
freq-pair	Specifies the frequency components of a tone to be detected.

Command	Description
supervisory answer dualtone	Enables answer supervision on a voice port.
voice class dualtone	Creates a voice class for FXO tone detection parameters.

freq-max-deviation

To specify the maximum frequency deviation allowed in a tone, use the **freq-max-deviation command in**voice-class configuration mode. To reset to the default maximum frequency deviation, use the **no** form of this command.

freq-max-deviation *hertz*
no freq-max-deviation

Syntax Description

hertz	Maximum cycles per second (Hz) by which tone frequencies may deviate from the configured frequencies and be detected. The value applies to both frequencies of a dual tone. Range is from 10 to 125. The default is 10.

Command Default

10 Hz

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.1(5)XM	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 1750.

Usage Guidelines

This command creates a detection limit for one parameter within a voice class that you can apply to any voice port.

Be sure that the frequency deviation is less than the smallest frequency difference between any two call-progress tones to prevent overlapping of detectable frequencies. If detectable frequencies overlap, one of the call-progress tones is not detected.

You must specify a time value greater than the expected frequency deviation in the tone to be detected.

Examples

The following example configures a maximum frequency deviation of 20 Hz for voice class 100:

```
voice class dualtone 100
 freq-max-deviation 20
```

The following example configures a maximum frequency deviation of 20 Hz for voice class 70:

```
voice class dualtone-detect-params 70
 freq-max-deviation 20
```

Related Commands

Command	Description
dualtone	Defines the tone and cadence for a custom call-progress tone.

Command	Description
freq-pair	Specifies the frequency components of a tone to be detected.
supervisory answer dualtone	Enables answer supervision on a voice port.
supervisory dualtone-detect-params	Assigns the boundary and detection tolerance parameters to a voice port.
voice class dualtone	Creates a voice class for FXO tone detection parameters.

freq-max-power

To specify the upper limit of tone power allowed in a tone, use the **freq-max-power** command in voice-class configuration mode. To reset to the default maximum tone power, use the **no** form of this command.

freq-max-power *dBm0*
no freq-max-power

Syntax Description

dBm0	Upper limit of the tone power that is detected, in dBm0 (where dBm0 is decibels referred to one milliwatt and corrected to a 0-dBm effective power level). Range is from 0 to -20. The default is -10.

Command Default

-10 dBm0

Command Modes

Voice-class configuration

Command History

Release	Modification
12.1(5)XM	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 1750.

Usage Guidelines

This command creates a detection limit for one parameter within a voice class that you can apply to any voice port.

You must specify a power value greater than the expected maximum power of a tone to be detected.

Examples

The following example configures a maximum tone power of -20 dBm0 for voice class 100:

```
voice class dualtone 100
 freq-max-power -20
```

The following example configures a maximum tone power of -6 dBm0 for voice class 70:

```
voice class dualtone-detect-params 70
 freq-max-power -6
```

Related Commands

Command	Description
dualtone	Defines the tone and cadence for a custom call-progress tone.
freq-pair	Specifies the frequency components of a tone to be detected.
supervisory answer dualtone	Enables answer supervision on a voice port.

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 dualtone	Creates a voice class for FXO tone detection parameters.

freq-min-power

To specify the lower limit of tone power allowed in a tone, use the **freq-min-power**command in voice-class configuration mode. To reset to the default minimum tone power, use the **no** form of this command.

freq-min-power *dBm0*
no freq-min-power

Syntax Description

dBm0	Lower limit of tone power that is detected, in dBm0 (where dBm0 is decibels referred to one milliwatt and corrected to a 0-dBm effective power level). Range is from -10 to -35. The default is -30.

Command Default

-30 dBm0

Command Modes

Voice-class configuration

Command History

Release	Modification
12.1(5)XM	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 1750.

Usage Guidelines

This command creates a detection limit for one parameter within a voice class that you can apply to any voice port.

You must specify a power value less than the expected minimum power of a tone to be detected.

Examples

The following example configures a tone-power lower limit of -15 dBm0 for voice class 100:

```
voice class dualtone 100
 freq-min-power -15
```

The following example configures a tone-power lower limit of -25 dBm0 for voice class 70:

```
voice class dualtone-detect-params 70
 freq-min-power -25
```

Related Commands

Command	Description
dualtone	Defines the tone and cadence for a custom call-progress tone.
freq-pair	Specifies the frequency components of a tone to be detected.
supervisory answer dualtone	Enables answer supervision on a voice port.
supervisory dualtone-detect-params	Assigns the boundary and detection tolerance parameters to a voice port.

Command	Description
voice class dualtone	Creates a voice class for FXO tone detection parameters.

freq-pair

To specify the frequency components of a tone to be detected, use the **freq-pair** command in voice-class configuration mode. To cancel detection of a tone, use the **no** form of this command.

freq-pair *tone-id frequency-1 frequency-2*
no freq-pair *tone-id*

Syntax Description

tone-id	Tag identifier for a tone to be detected. Range is from 1 to 16. There is no default.
frequency-1	One frequency component of the tone to be detected, in Hz. Range is from 300 to 3600. There is no default.
frequency-2	A second frequency component of the tone to be detected, in Hz. Range is frm 300 to 3600, or you can specify 0. There is no default.

Command Default

No tone is specified for detection

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.1(3)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.

Usage Guidelines

To detect a tone with two frequency components (a dualtone), configure frequencies for *frequency-1* and *frequency-2* .

To detect a tone with only one frequency component, configure a frequency for *frequency-1* and enter 0 for *frequency-2* .

You can configure a router to detect up to 16 tones.

Examples

The following example configures tone number 1 (tone-id 1) with frequency components of 480 Hz and 2400 Hz:

```
voice class dualtone 100
 freq-pair 1 480 2400
 exit
```

The following example configures tone number 1 (tone-id 1) with frequency components of 480 Hz and 2400 Hz and tone number 2 (tone-id 2) with frequency components of 560 Hz and 880 Hz:

```
voice class dualtone 50
 freq-pair 1 480 2400
 freq-pair 2 560 880
 exit
```

Related Commands

Command	Description
frag-pre-queuing	Specifies the maximum timing difference allowed between the two frequencies for detection of a tone.
freq-max-deviation	Specifies the maximum frequency deviation allowed in a tone.
freq-max-power	Specifies the upper limit of the tone power allowed in a tone.
freq-min-power	Specifies the lower limit of the tone power allowed in a tone.
freq-power-twist	Specifies the power difference allowed between the two frequencies of a tone.
voice class dualtone	Creates a voice class for FXO tone detection parameters.

freq-power-twist

To specify the power difference allowed between the two frequencies of a tone, use the **freq-power-twist**command in voice - class configuration mode. To reset to the default power difference allowed, use the **no** form of this command.

freq-power-twist *dBm0*
no freq-power-twist

Syntax Description

dBm0	Maximum power difference allowed between the two frequencies of a tone, in dBm0 (where dBm0 is decibels referred to one milliwatt and corrected to a 0-dBm effective power level). Range is from 0 to 15. The default is 6.

Command Default

6 dBm0

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.1(5)XM	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 1750.

Usage Guidelines

This command creates a detection limit for one parameter within a voice class that you can apply to any voice port.

You must specify a power value greater than the expected maximum power difference of the two frequencies in the tone to be detected.

Examples

The following example configures a maximum allowed power difference of 3 dBm0 between the two tone frequencies for voice class 100:

```
voice class dualtone 100
 freq-power-twist 3
```

The following example configures a maximum allowed power difference of 15 dBm0 between the two tone frequencies in voice class 70:

```
voice class dualtone-detect-params 70
 freq-power-twist 15
```

Related Commands

Command	Description
dualtone	Defines the tone and cadence for a custom call-progress tone.
freq-pair	Specifies the frequency components of a tone to be detected.

Command	Description
supervisory answer dualtone	Enables answer supervision on a voice port.
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 dualtone	Creates a voice class for FXO tone detection parameters.

frequency (cp-dualtone)

To define the frequency components for a call-progress tone, use the **frequency** command in cp- dualtone configuration mode. To reset to the default frequency components, use the **no** form of this command.

frequency *frequency-1* [*frequency-2*]
no frequency

Syntax Description

frequency -1	One frequency component of the tone to be detected, in Hz. Range is from 300 to 3600. The default is 300.
frequency -2	(Optional) A second frequency component of the tone to be detected, in Hz. Range is from 300 to 3600 or you can specify 0. The default is that no second frequency component is detected.

Command Default

300-Hz single tone

Command Modes

cp-dualtone configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 1750.

Usage Guidelines

This command specifies the frequency component for a class of custom call-progress tones.

You need to define the frequency that you want a voice port to detect. Reenter the command for each additional frequency to be detected.

You need to associate the class of custom call-progress tones with a voice port for this command to affect tone detection.

Examples

The following example defines the frequency components for the busy tone in custom-cptone voice class country-x.

```
voice class custom-cptone country-x
 dualtone busy frequency 480 620
```

Related Commands

Command	Description
supervisory custom-cptone	Associates a class of custom call-progress tones with a voice port.
voice class custom-cptone	Creates a voice class for defining custom call-progress tones.
voice class dualtone-detect-params	Modifies the boundaries and limits for custom call-progress tones defined by the **voice class custom-cptone** command.



G

- g729 annexb-all, on page 272
- g729-annexb override, on page 274
- g732 ber, on page 275
- gatekeeper, on page 276
- gateway, on page 277
- gcid, on page 278
- global (application configuration), on page 280
- groundstart auto-tip, on page 281
- group, on page 282
- group auto-reset, on page 284
- group cumulative-ack, on page 286
- group out-of-sequence, on page 288
- group receive, on page 290
- group retransmit, on page 292
- group set, on page 294
- group timer, on page 296
- group-params, on page 298
- gw-accounting, on page 299
- gw-type-prefix, on page 303

g729 annexb-all

To configure Cisco IOS Session Initiation Protocol (SIP) gateway to treat the G.729br8 codec as superset of G.729r8 and G.729br8 codecs to interoperate with the Cisco Unified Communications Manager, use the **g729 annexb-all** command in voice service SIP configuration mode or voice class tenant configuration mode. To return to the default global setting for the gateway, where G.729br8 codec represents only the G.729br8 codec, use the **no** form of this command.

g729 annexb-all system
no g729 annexb-all system

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	Specifies that the codec 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

G.729br8 codec is not viewed as superset of G.729r8 and G.729br8 codecs.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

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.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

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 Cisco IOS SIP gateway for interoperation with Cisco Unified Communications Manager (formerly known as the Cisco CallManager, or CCM), use the **g729-annexb-all** command in voice service SIP configuration mode to allow connection of calls between two DSPs with incompatible G.729 codecs. Use the **voice-class sip g729 annexb-all** command in dial peer voice configuration mode to configure G.729 codec interoperation settings for a dial peer that override global settings for the Cisco IOS SIP gateway.

Examples

The following example configures a Cisco IOS SIP gateway (globally) to be able to connect calls between otherwise incompatible G.729 codecs:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# g729 annexb-all
```

The following example configures a Cisco IOS SIP gateway (globally) to be able to connect calls between otherwise incompatible G.729 codecs in the voice class tenant configuration mode:

```
Router(config-class)# g729 annexb-all system
```

Related Commands

Command	Description
voice-class sip g729 annexb-all	Configures an individual dial peer on a Cisco IOS SIP gateway to view a G.729br8 codec as superset of G.729r8 and G.729br8 codecs.

g729-annexb override

To configure settings for G729 codec interoperability and override the default value if annexb attribute is not present. Use the **no** form of this command to disable this feature.

g729-annexb override
no g729-annexb override

Syntax Description

override	Overrides the default value, if **annexb** attribute is not present in g729 codec.

Command Default

Not enabled by default.

Command Modes

SIP UA configuration (config-sip-ua).

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

Usage Guidelines

The default value of g729-annexb is set to YES. When g729-annexb override is configured under sip-ua mode, the default value of g729-annexb will be set to NO. So, g729-annexb is not negotiated when G729 codec is selected for the call.

Examples

```
SATYA_2070(config-sip-ua)#g729-annexb override
SATYA_2070(config-sip-ua)#
```

g732 ber

To enable G.732 processing and reporting for the E1 controller, use the **g732 ber** command in controller configuration mode. To disable processing and reporting, use the **no** form of this command.

g732 ber
no g732 ber

Syntax Description

This command has no arguments or keywords.

Command Default

G.732 is disabled.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.2(2)T	This command was introduced on the Cisco 2611.
12.2(15)T	This command was implemented on the Cisco AS5350 and Cisco AS5400 network access server (NAS) platforms.

Usage Guidelines

By default, G.732 reporting is disabled to prevent a change in E1 behavior for sites that do not want G.732 reporting.

Once ITU-T G.732 is enabled, the E1 controller is placed in the DOWN state if the bit error rate (BER) on the line is greater than 10e-3. The controller is restored to the UP state if the BER drops below 10e-4 for longer than two seconds. When the G.732 alarm is declared, the transmitter sends a remote alarm indication (RAI) yellow alarm.

You can restore ITU-T G.732 functionality by performing a power cycle or a software reload.

Examples

The following example applies to a Cisco 2611 and shows enabled G.732 processing and reporting for E1 controller 0/0:

```
controller e1 0/0
 g732 ber
```

The following example applies to a Cisco AS5400 with an 8-PRI E1 dial feature card (DFC) in slot 4:

```
controller e1 4/0
 g732 ber
```

Related Commands

Command	Description
show controllers e1	Displays information about E1 links.

gatekeeper

To enter gatekeeper configuration mode, use the **gatekeeper** command in global configuration mode.

gatekeeper

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2500 series and Cisco 3600 series.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T and implemented on the Cisco MC3810.

Usage Guidelines

Press Ctrl-Z or use the **exit** command to exit gatekeeper configuration mode.

Examples

The following example brings the gatekeeper online:

```
gatekeeper
 no shutdown
```

gateway

To enable the H.323 VoIP gateway, use the **gateway**command in global configuration mode. To disable the gateway, use the **no** form of this command.

gateway
no gateway

Syntax Description

This command has no arguments or keywords.

Command Default

The gateway is unregistered

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the following platforms: Cisco 3600 series, Cisco AS5300, and Cisco AS5800.
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

Use this command to enable H.323 VoIP gateway functionality. After you enable the gateway, it attempts to discover a gatekeeper by using the H.323 RAS GRQ message. If you enter **no gateway voip**, the VoIP gateway unregisters with the gatekeeper via the H.323 RAS URQ message.

Examples

The following example enables the gateway:

```
gateway
```

gcid

To enable Global Call ID (Gcid) for every call on an outbound leg of a VoIP dial peer for a SIP endpoint, use the **gcid** command in voice-service configuration mode. To return to the default, use the **no** form of this command.

gcid
no gcid

Syntax Description

This command has no arguments or keywords.

Command Default

Gcid is disabled.

Command Modes

Voice service configuration (config-voi-serve)

Command History

Cisco IOS Release	Cisco Product	Modification
12.4(11)XW2	Cisco Unified CME 4.2	This command was introduced.
12.4(15)XY	Cisco Unified CME 4.2(1)	This command was introduced.
12.4(15)XZ	Cisco Unified CME 4.3	This command was introduced.
12.4(20)T	--	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Cupertino 17.7.1a	--	Introduced support for YANG models.

Usage Guidelines

This command in voice-service configuration mode enables Global Call ID (Gcid) in the SIP header for every call on an outbound leg of a VoIP dial peer for a SIP endpoint.

When a call moves around and between the SIP endpoint and the target on a VoIP network because of redirect, transfer, and conference, the SIP Call-ID continues to change. For call control purposes, a unique Gcid is issued for every outbound call leg. A single Gcid remains the same for the same call in the system, and is valid for redirect, transfer, and conference events, including 3-party conferencing when a call center phone acts as a conference host. A SIP header, Cisco_GCID, is added into SIP Invite and REFER requests and to certain other responses to pass the Gcid to the target.

Examples

The following partial output shows the configuration for the **gcid** command:

```
router# show running-configuration
!
!
!
voice service voip
 gcid
 callmonitor
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to h323
 allow-connections sip to sip
```

```
no supplementary-service sip moved-temporarily
sip
registrar server expires max 120 min 60
```

global (application configuration)

To enter application configuration global mode, use the **global** command in application configuration mode.

global

Syntax Description

No arguments or keywords

Command Default

No default behavior or values

Command Modes

Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use this command to enter application configuration global mode. You can then configure applications for a dial peer to use for incoming calls when it does not have an explicit application configured.

If an application is defined on the dial peer, that application always takes precedence over the global application configured in application configuration global mode. The applications configured in this mode execute only when a dial peer has no application configured.

Examples

The following example shows the clid_authen_collect application is configured as the default global application for all inbound dial peers that do not have a specific application configured:

```
application
global
service default clid_authen_collect
```

Related Commands

Command	Description
call application global	Configures an application to use for incoming calls whose incoming dial peer does not have an explicit application configured.

groundstart auto-tip

To configure a timing delay on an FXO groundstart voice port, use the **groundstart auto-tip**command in voice-port configuration mode. To disable the configured timeout, use the **no** form of this command.

groundstart auto-tip [**delay** *timer*]
no groundstart auto-tip [**delay** *timer*]

Syntax Description

delay	Indicates that a specific delay time will be configured.
timer	Specifies the wait time in milliseconds that the FXO groundstart voice port will wait for a tip ground acknowledgment.

Command Default

This command is disabled by default. If the command is used without the optional keyword, the default time of 200 ms is activated.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.3(11)T2	This command was introduced into Cisco IOS Release 12.3(11)T2. This command is not supported on the Cisco 1700 series platform.

Usage Guidelines

This command should only be used after you encounter call setup problems involving FXO groundstart analog voice ports. If these problems occur, first load the latest image for your Cisco IOS Release (for example, if you are running Release 12.3(11)T, you should replace this image with Release 12.3(11)T2. Upgrading the software image should eliminate the problem. If not, then use this command as a troubleshooting measure--it should be enabled in a configuration only if you encounter problems in connecting outgoing calls. After the **groundstart auto-tip** command is configured, the problem should not occur again.

Use the **groundstart auto-tip**command only for voice ports configured for FXO groundstart signaling.

The following example sets the delay wait time for tip ground acknowledgment to 250 ms:

```
Router# configure terminal
Router(config)# voice-port 2/0/0
Router(config-voiceport)# shutdown
Router(config-voiceport)# groundstart auto-tip delay 250
Router(config-voiceport)# no shutdown
Router(config-voiceport)# exit
```

Related Commands

Command	Description
voice-port	Specifies that a voice port will be used in the connection.

group

To configure the maximum number of segments that are received in a session group or to associate the group with a specified session set, use the **group**command in backhaul-session-manager configuration mode. To restore the default number, use the **no** form of this command.

group {**group-name cumulative ack count** | **out-of-sequence count** | **receive count** | **retransmit count** | **set set-name**}
no group {**group-name cumulative ack** | **out-of-sequence** | **receive** | **retransmit** | **set**}

Syntax Description

group -name	Session-group name.
cumulative ack *count*	Maximum number of segments received before acknowledgment. Range is from 0 to 255. Default is 3 segments.
out -of-sequence *count*	Maximum number of out-of-sequence segments that can be received in a session group before an ACK is sent. Range is from 0 to 255. Default is 3 segments.
receive *count*	Maximum number of segments in the receive window of the media gateway. This is the maximum number of segments the media gateway is allowed to receive before it sends an ACK. Range is from 1 to 64. Default is 32 segments.
retransmit *count*	Maximum number of retransmits allowed in a session group. Range is from 0 to 255. Default is 2 retransmits.
set *set -name*	Session-set name.

Command Default

For the **cumulative ack** and **out-of-sequence** keywords, the default is 3 segments. For the **receive** keyword, the default is 32 segments. For the **retransmit** keyword, the default is 2 retransmits. The **set** keyword has no default behavior or values.

Command Modes

Backhaul-session-manager configuration (config-bsm)

Caution Do not change this command or the keywords unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. This command was implemented on the Cisco IAD2420 series. This command does not support the access servers in this release.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Examples

The following example configures the session group named group5 to send an acknowledgment after four segments have been received:

```
group group5 cumulative-ack 4
```

The following example configures the session group named group5 to send an acknowledgment after four out-of-sequence segments have been received:

```
group group5 out-of-sequence 4
```

The following example configures the session group named group5 to receive a maximum of 10 segments:

```
group group5 receive 10
```

The following example configures the session group named group5 to allow as many as 3 retransmits:

```
group group5 retransmit 3
```

The following example associates the session group named group5 with the session set named set1:

```
group group5 set set1
```

Related Commands

Command	Description
group auto-reset	Specifies the maximum number of auto-resets for a session group.
group cumulative-ack	Specifies maximum cumulative acknowledgments.
group out-of-sequence	Specifies maximum out-of-sequence segments that are received before an EACK is sent.
group receive	Specifies maximum receive segments.
group retransmit	Specifies maximum retransmits.
group timer	Specifies timeouts.

group auto-reset

To specify the maximum number of auto-resets for a session group, use the **group auto-reset** command in backhaul session manager configuration mode. To restore the default number, use the **no** form of this command.

group group-name auto-reset count
no group group-name auto-reset

Syntax Description

group -name	Name of session group.
count	Maximum number of auto-resets before the connection is considered failed. Range is from 0 to 255. The default is 5.

Command Default

5 auto-resets

Command Modes

Backhaul session manager configuration (config-bsm)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 series.
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 was implemented on the Cisco IAD2420 series.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Caution Do not change the auto-reset number unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Examples

The following example specifies a maximum of six auto-resets for the session group named "group5":

```
Router(config-bsm)# group group5 auto-reset 6
```

Related Commands

Command	Description
group cumulative-ack	Configures the maximum number of segments that are received in a session group before an acknowledgment is sent.

Command	Description
group out-of-sequence	Configures the maximum out-of-sequence segments that are received before an EACK is sent.
group receive	Configures the maximum number of segments in the receive window of a session group.
group retransmit	Configures the maximum number of retransmits.

group cumulative-ack

To configure the maximum number of segments that are received before an acknowledgment is sent, use the **group cumulative-ack** command in backhaul session manager configuration mode. To set the value to the default, use the **no** form of this command.

group *group-name* **cumulative-ack** *count*
no group *group-name* **cumulative-ack** *count*

Syntax Description

group -name	Name of session group.
count	Maximum number of segments that are received before acknowledgment. Range is from 0 to 255. The default is 3.

Command Default

3 segments

Command Modes

Backhaul session manager configuration (config-bsm)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 series.
12.2(8)T	This command was implemented on the Cisco IAD2420 series.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Caution Do not change this parameter unless instructed to do so by Cisco technical support. Incorrectly set parameters can cause sessions to fail.

Examples

The following example sets the cumulative acknowledgment maximum to 4 for the group named "group1":

```
Router(config-bsm)# group group5 cumulative-ack 4
```

Related Commands

Command	Description
group auto-reset	Configures the maximum auto-reset value.

Command	Description
group out-of-sequence	Configures the maximum number of out-of-sequence segments that are received before an EACK is sent.
group receive	Configures the maximum number of receive segments.
group retransmit	Configures the maximum number of retransmits.

group out-of-sequence

To configure the maximum number of out-of-sequence segments that are received before an error acknowledgement (EACK) is sent, use the **group out-of-sequence** command in backhaul session manager configuration mode. To set the value to the default, use the **no** form of this command.

group *group-name* **out-of-sequence** *count*
no group *group-name* **out-of-sequence** *count*

Syntax Description

group-name	Name of the session group.
count	Maximum number of out-of-sequence segments. Range is from 0 to 255. The default is 3.

Command Default

3 segments

Command Modes

Backhaul session manager configuration (config-bsm)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 series.
12.2(8)T	This command was implemented on the Cisco IAD2420 series.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Caution Do not change this parameter unless instructed to do so by Cisco technical support. Incorrectly set parameters can cause sessions to fail.

Examples

The following example sets the out-of-sequence maximum to 4 for the group named "group5":

```
Router(config-bsm)# group group5 out-of-sequence 4
```

Related Commands

Command	Description
group auto-reset	Configures the maximum auto-reset value.
group cumulative-ack	Configures the maximum number of cumulative acknowledgments.
group receive	Configures the maximum number of receive segments.

Command	Description
group retransmit	Configures the maximum number of retransmits.

group receive

To configure the maximum number of receive segments, use the **group receive** command in backhaul session manager configuration mode. To set the value to the default, use the **no** form of this command.

group *group-name* **receive** *count*
no group *group-name* **receive** *count*

Syntax Description

group -name	Name of the session group.
count	Maximum number of segments in a receive window. The far end should send no more than this number of segments before receiving an acknowledgment for the oldest outstanding segment. Range is 1 to 64. The default is 32.

Command Default

32 segments

Command Modes

Backhaul session manager configuration



Caution Do not change this parameter unless instructed to do so by Cisco technical support. Incorrectly set parameters can cause sessions to fail.

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 series.
12.2(8)T	This command was implemented on the Cisco IAD2420 series.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Examples

The following example sets the receive maximum to 10 for the group named "group5":

```
Router(config-bsm)# group group5 receive 10
```

Related Commands

Command	Description
group auto-reset	Configures the maximum auto-reset value.
group cumulative-ack	Configures the maximum number of cumulative acknowledgments.

Command	Description
group out-of-sequence	Configures the maximum number of out-of-sequence segments that are received before an EACK is sent.
group retransmit	Configures the maximum number of retransmits.

group retransmit

To configure the maximum number of retransmits, use the **group retransmit** command in backhaul session manager configuration mode. To set the value to the default, use the **no** form of this command.

group *group-name* **retransmit** *count*
no group *group-name* **retransmit** *count*

Syntax Description

group -name	Name of the session group.
count	Maximum number of retransmits. Range is 0 to 255. The default is 2.

Command Modes

2 retransmits

Command Modes

Backhaul session manager configuration (config-bsm)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 series.
12.2(8)T	This command was implemented on the Cisco IAD2420 series.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.



Caution Do not change this parameter unless instructed to do so by Cisco technical support. Incorrectly set parameters can cause sessions to fail.

Examples

The following example sets the retransmit maximum to 3 for the group named "group5":

```
Router(config-bsm)# group
 group5
 retrans 3
```

Related Commands

Command	Description
group auto-reset	Configures the maximum auto-reset value.
group cumulative-ack	Configures the maximum number of cumulative acknowledgments.

Command	Description
group out-of-sequence	Configures the maximum number of out-of-sequence segments that are received before an EACK is sent.
group receive	Configures the maximum number of receive segments.

group set

To create a session group and associate it with a specified session set, use the **group**command in backhaul session manager configuration mode. To delete the group, use the **no** form of this command.

group *grp-name* **set** *set-name*
no group *grp-name*

Syntax Description

grp -name	Name of the session group.
set -name	Name of the session set.

Command Default

No default behavior or values

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 series.
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 was implemented on the Cisco IAD2420 series.

Examples

The following example shows session group **group5** being associated with session set **set1**:

```
Router(config-bsm)# group group5 set set1
```

Related Commands

Command	Description
group auto-reset	Specifies the maximum number of auto-resets for a session group.
group cumulative-ack	Configures the maximum number of segments that are received in a session group before an acknowledgment is sent.
group out-of-sequence	Configures the maximum out-of-sequence segments that are received before an EACK is sent.
group receive	Configures the maximum number of segments in the receive window of a session group.
group retransmit	Configures the maximum number of retransmits.
group timer cumulative-ack	Configures cumulative acknowledgment timeout.

Command	Description
group timer keepalive	Configures keepalive (or null segment) timeout.
group timer retransmit	Configures retransmission timeout.
group timer transfer	Configures state transfer timeout.

group timer

To configure the maximum number of milliseconds for which the Reliable User Datagram Protocol (RUDP) delays before sending an acknowledgment for a received segment, sending a keepalive segment, retransmitting a segment, or transferring a segment, use the **group timer**command in backhaul-session-manager configuration mode. To restore the default values, use the **no** form of this command.

group *group-name* **timer** {**cumulative ack** *time* | **keepalive** *time* | **retransmit** *t ime* | **transfer** *time*}
no group *group-name* **timer cumulative ack**

Syntax Description

group -name	Name of session group.
cumulative ack *time*	Number of milliseconds for which RUDP delays before sending an acknowledgment for a received segment. Range is 100 to 65535. The default is 100.
keepalive *time*	Number of milliseconds before RUDP sends a keepalive segment when no RUDP packets are received or sent. Range is 100 to 65535. The default is 1000.
retransmit *time*	Number of milliseconds for which RUDP waits before retransmitting the segment. Range is 100 to 65535. The default is 300.
transfer *time*	Number of milliseconds for which RUDP waits to receive a selection of a new session from the application during a transfer state. Range is 0 to 65535. The default is 2000.

Command Default

cumulative ack : 100 milliseconds**keepalive**: 1000 milliseconds**retransmit:**300 milliseconds**transfer**: 2000 milliseconds

Command Modes

Backhaul-session-manager configuration (config-bsm)

Caution Do not change the group timer parameters unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
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 was implemented on the Cisco IAD2420 series.

Release	Modification
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

The retransmit timer must be greater than the cumulative-ack timer.

Cumulative acknowledgment timeout is the maximum number of milliseconds for which RUDP delays before sending an acknowledgment for a received segment.

Examples

The following example specifies 325 milliseconds as the maximum acknowledgment delay for the session group named "group5":

```
group group5 timer cumulative-ack 325
```

The following example configures RUDP to send keepalive segments if no RUDP packets are received or sent for 2.5 seconds (2500 milliseconds) in the session group named "group5".

```
group group5 timer keepalive 2500
```

The following example sets a retransmit time of 650 milliseconds for the session group named "group5":

```
group group5 timer retransmit 650
```

Related Commands

Command	Description
group	Specifies the maximum number of segments that are received in a session group.

group-params

To define groups of parameters that can be used by applications, use the **group-params** command in application configuration mode. There is no **no** form of the command.

group-params *groupname*

Syntax Description

groupname	Name of the parameter group that you are creating.

Command Default

No default behavior or values

Command Modes

Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command allows you to define groups of parameters so that a group of parameters can be used by multiple services or packages (applications). Parameter groups are defined globally and once a group is defined, it is available for another service or package to use. Groups can contain parameters under multiple parameterspaces. In cases where a parameter is defined individually and in a parameter group, the individual parameter definition is given precedence.

Examples

The following example shows a parameter group named "fax," that contains two parameters:

```
application
group-params fax
  paramspace fax_detect2 pin-len 9
  paramspace fax_detect1 retry-count 9
```

gw-accounting

To enable an accounting method for collecting call detail records (CDRs), use the **gw-accounting** command in global configuration mode. To disable an accounting method, use the **no** form of this command.

gw-accounting {**aaa** | **file** | **syslog** [**stats**]}
no gw-accounting {**aaa** | **file** | **syslog** [**stats**]}

Syntax Description

aaa	Enables accounting through the AAA system and sends call detail records to the RADIUS server in the form of vendor-specific attributes (VSAs).
file	Enables the file accounting method to store call detail records in .csv format.
syslog	Enables the system logging facility to output accounting information in the form of a system log message.
stats	(Optional) Enables voice quality statistics to be sent to the system log.
voip	Enables generic gateway-specific accounting.

Command Default

No accounting method is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(6)NA2	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T. The **vsa** keyword was added.
12.1(1)T	The **voip** keyword was added.
12.2(11)T	The **h323**, **vsa**, and **voip** keywords were replaced by the **aaa** keyword.
12.4(11)XW	The **stats** keyword was added.
12.4(15)XY	The **file** keyword was added.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Cupertino 17.9.1a	Allows transfer of CUBE CDRs using SFTP.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

This command enables you to output accounting data in one of the following ways:

Using RADIUS Vendor-Specific Attributes

The IETF draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26).

Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not appropriate for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair." The value is a string of the format:

```
protocol: attribute sep value *
```

"Protocol" is a value of the Cisco "protocol" attribute for a particular type of authorization. "Attribute" and "value" are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and "sep" is "=" for mandatory attributes and "*" for optional attributes. This allows the full set of features available for TACACS+ authorization to also be used for RADIUS. For a list of VSA fields and their ASCII values, see the *>Cisco IOS Security Configuration Guide* for your Cisco IOS release.

Use the **gw-accounting aaa**command to enable the VSA method of accounting.

Using File Format

This method stores CDRs in comma separated values (CSV) format. These CDR records can be stored in a file on external or internal flash or on a file on a FTP or SFTP server.

Each CDR has a fixed number of fields whose names and position order are predefined. Ten generic fields capture feature-related information. The CDR has feature fields representing the basic feature and feature fields representing the supplementary services.

Use the **gw-accounting file** command to enable the .csv file method of accounting.

Using syslog Records

The syslog accounting option exports the information elements associated with each call leg through a system log message, which can be captured by a syslog daemon on the network. The syslog output consists of the following:

```
<server timestamp> <gateway id> <message number> : <message label> : <list of AV pairs>
```

Use the **gw-accounting syslog** command to enable the syslog method of gathering accounting data.

The table below describes the syslog message fields.

Table 11: syslog Message Output Fields

Field	Description
server timestamp	Time stamp created by the server when it receives the message to log.
gateway id	Name of the gateway that sends the message.
message number	Number assigned to the message by the gateway.
message label	String used to identify the message category.
list of AV pairs	String that consists of <attribute name> <attribute value> pairs separated by commas.

You can enable **aaa**, **file**, or **syslog** simultaneously; call detail records are generated using all methods that you enable.

Overloading the Acct-Session-ID field

Attributes that cannot be mapped to standard RADIUS are packed into the Acct-Session-ID field as ASCII strings separated by the character "/". The Acct-Session-ID attribute definition contains the RADIUS account session ID, which is a unique identifier that links accounting records associated with the same login session for a user. To support additional fields, the following string format is defined for this field:

```
<session id>/<call leg setup time>/<gateway id>/<connection id>/<call origin>/
<call type>/<connect time>/<disconnect time>/<disconnect cause>/<remote ip address>
```

The table below describes the field attributes that are used with the overloaded acct-session-ID method.

Table 12: Field Attributes in Overloaded Acct-Session-ID

Field Attribute	Description
Session-Id	Standard RADIUS account session ID.
Setup-Time	Q.931 setup time for this connection in Network Time Protocol (NTP) format: hour, minutes, seconds, milliseconds, time zone, day of week, month, day of month, and year.
Gateway-Id	Name of the underlying gateway in the form "gateway.domain_name."
Call-Origin	Origin of the call relative to the gateway. Possible values are **originate** and **answer**.
Call-Type	Call leg type. Possible values are **telephony** and **VoIP**.
Connection-Id	Unique global identifier used to correlate call legs that belong to the same end-to-end call. The field consists of 4 long words (128 bits). Each long word displays as a hexadecimal value separated by a space character.
Connect-Time	Q.931 connect time for this call leg, in NTP format.
Disconnect-Time	Q.931 disconnect time for this call leg, in NTP format.
Disconnect-Cause	Reason that a call was taken offline as defined in the Q.931 specification.
Remote-Ip-Address	Address of the remote gateway port where the call is connected.

Because of the limited size of the Acct-Session-ID string, it is impossible to include many information elements in it. Therefore, this feature supports only a limited set of accounting information elements.

Use the **attribute acct-session-id overloaded** command to configure the overloaded session ID method of applying H.323 gateway-specific accounting.

Examples

The following example shows accounting enabled using RADIUS VSA attributes:

```
gw-accounting aaa
```

The following example shows accounting enabled using the syslog method:

```
gw-accounting syslog
```

The following example shows accounting enabled using the file method.

From Cisco IOS XE Cupertino 17.9.1a onwards, CUBE allows CDR transfer using SFTP:

```
Router# show running-config | section gw-accounting
gw-accounting file
 primary sftp [2001:420:54ff:13::312:175]//cdrtest username bob password 6 P^AV^_3
 secondary ifs flash:cdrtest2
 maximum buffer-size 15
 maximum retry-count 3
 maximum fileclose-timer 300
 maximum cdrflush-timer 245
 cdr-format compact
```

Related Commands

Command	Description
acct-template	Selects a group of voice accounting attributes to collect.
attribute acct-session-id overloaded	Overloads the acct-session-id attribute with call detail records.
radius-server vsa send	Enables the voice gateway to recognize and use VSAs.

gw-type-prefix

To configure a technology prefix in the gatekeeper, use the **gw-type-prefix** command in gatekeeper configuration mode. To remove the technology prefix, use the no form of this command.

gw-type-prefix *type-prefix* [[**hopoff** *gkid1*] [**hopoff** *gkid2*] [**hopoff** *gkidn*] [**seq** | **blast**]] [**default-technology**] [**gw ipaddr** *ipaddr* [*port*]]
no gw-type-prefix *type-prefix* [[**hopoff** *gkid1*] [**hopoff** *gkid2*] [**hopoff** *gkidn*] [**seq** | **blast**]] [**default-technology**] [**gw ipaddr** *ipaddr* [*port*]]

Syntax Description

type -prefix	A technology prefix is recognized and is stripped before checking for the zone prefix. It is strongly recommended that you select technology prefixes that do not lead to ambiguity with zone prefixes. Do this by using the # character to terminate technology prefixes, for example, 3#.
hopoff *gkid*	(Optional) Use this option to specify the gatekeeper where the call is to hop off, regardless of the zone prefix in the destination address. The *gkid* argument refers to a gatekeeper previously configured using the zone local or zone remote comment. You can enter this keyword and argument multiple times to configure redundant gatekeepers for a given technology prefix.
seq | **blast**	(Optional) If you list multiple hopoffs, this indicates that the LRQs should be sent sequentially or simultaneously (blast) to the gatekeepers according to the order in which they were listed. The default is to send them sequentially.
default-technology	(Optional) Gateways registering with this prefix option are used as the default for routing any addresses that are otherwise unresolved.
gw ipaddr *ipaddr* [*port*]	(Optional) Use this option to indicate that the gateway is incapable of registering technology prefixes. When it registers, it adds the gateway to the group for this type prefix, just as if it had sent the technology prefix in its registration. This parameter can be repeated to associate more than one gateway with a technology prefix.

Command Default

By default, no technology prefix is defined, and LRQs are sent sequentially to all the gatekeepers listed.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the following platforms: Cisco 2500 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T. This command was modified to allow the user to specify multiple hopoffs.
12.1(2)T	This command was modified to allow the user to specify whether LRQs should be sent simultaneously or sequentially to the gatekeepers.

Release	Modification
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco MC3810, and Cisco 7200 series.

Usage Guidelines

More than one gateway can register with the same technology prefix. In such cases, a random selection is made of one of them.

You do not have to define a technology prefix to a gatekeeper if there are gateways configured to register with that prefix and if there are no special flags (**hopoff** *gkid* or **default-technology**) that you want to associate with that prefix.

You need to configure the gateway type prefix of all remote technology prefixes that are routed through this gatekeeper.

Examples

The following example defines two gatekeepers for technology zone 3:

```
gw-type-prefix 3#* hopoff c2600-1-gk hopoff c2514-1-gk
```

Related Commands

Command	Description
show gatekeeper gw-type-prefix	Displays the list of currently defined technology zones and the gatekeepers responsible for each.
zone prefix	Configures the gatekeeper with knowledge of its own prefix and the prefix of any remote zone.



H

- h225 alt-ep hunt, on page 307
- h225 connect-passthru, on page 312
- h225 display-ie, on page 314
- h225 h245-address, on page 316
- h225 h245-address on-connect (H.323 voice-class), on page 318
- h225 h245-address on-connect (H.323 voice-service), on page 320
- h225 h245-address setup, on page 322
- h225 id-passthru, on page 324
- h225 plus-digit passthru, on page 325
- h225 signal overlap, on page 327
- h225 start-h245, on page 328
- h225 timeout call-proceeding, on page 329
- h225 timeout keepalive, on page 331
- h225 timeout setup, on page 332
- h225 timeout t302, on page 333
- h225 timeout t304, on page 334
- h225 timeout tcp call-idle (H.323 voice service), on page 335
- h225 timeout tcp establish, on page 336
- h225 timeut ntf, on page 337
- h245 address-check, on page 339
- h245 passthru, on page 340
- h245 timeout, on page 341
- h323, on page 343
- h323 asr, on page 344
- h323 call start, on page 345
- h323 gatekeeper, on page 347
- h323 h323-id, on page 348
- h323 interface, on page 349
- h323 qos, on page 350
- h323 t120, on page 351
- h323-annexg, on page 352
- h323-gateway voip bind srcaddr, on page 354
- h323-gateway voip h323-id, on page 355

- h323-gateway voip id, on page 356
- h323-gateway voip interface, on page 358
- h323-gateway voip tech-prefix, on page 359
- h323zone-id (voice source group), on page 361
- h450 h450-3 timeout, on page 362
- handle-replaces, on page 363
- hangup-last-active-call, on page 365
- header-passing, on page 367
- history-info, on page 369
- history session event-log save-exception-only, on page 370
- history session max-records, on page 371
- history session retain-timer, on page 372
- hold-resume, on page 373
- hopcount, on page 374
- host (SIP URI), on page 375
- host-registrar, on page 377
- http client cache memory, on page 379
- http client cache query, on page 381
- http client cache refresh, on page 382
- http client connection idle timeout, on page 384
- http client connection persistent, on page 385
- http client connection timeout, on page 386
- http client cookie, on page 387
- http client post-multipart, on page 388
- http client response timeout, on page 389
- http client secure-ciphersuite, on page 390
- http client secure-trustpoint, on page 394
- hunt-scheme least-idle, on page 395
- hunt-scheme least-used, on page 397
- hunt-scheme longest-idle, on page 399
- hunt-scheme random, on page 401
- hunt-scheme round-robin, on page 402
- hunt-scheme sequential, on page 404
- huntstop, on page 406

h225 alt-ep hunt

To configure alternate endpoint hunts for failed calls in an IP-to-IP gateway (IPIPGW), use the **h225 alt-ep hunt**command in H.323 voice-service configuration mode. To control the alternate endpoint hunts based on call disconnect cause codes, use the **no**form of this command.

h225 alt-ep hunt
no h225 alt-ep hunt [**all***cause-code*]

Syntax Description

all	Perform alternate hunt for all disconnect cause codes.
cause-code	A code returned from the destination router to indicate why an attempted end-to-end call was unsuccessful. The table in the "Usage Guidelines" section describes the possible values.

Command Default

Alternate endpoint hunt is enabled for all cause codes

Command Modes

H.323 voice-service configuration (conf-serv-h323)

Command History

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

Usage Guidelines

The default behavior of the gateway is to retry all alternate endpoints received from the gatekeeper regardless of the ReasonComplete reason. Only the **no alt-ep hunt** command will be visible in the configuration. 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. You can enter the keyword, decimal value, or hexadecimal value.

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.

Table 13: 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

Keyword	Description	Decimal	Hex
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
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 primary rate ISDN (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

Keyword	Description	Decimal	Hex
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
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

Keyword	Description	Decimal	Hex
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
req-vpci-vci-unavail	Requested virtual path connection identifier (VPCI) virtual channel identifier (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 inquiry.	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 shows the alternate endpoint hunts with the user-busy disconnect cause code disabled:

```
Router(conf-serv-h323)# no h225 alt-ep hunt user-busy
```

Related Commands

Command	Description
gatekeeper	Enters gatekeeper configuration mode.

h225 connect-passthru

To immediately pass H.225 connect messages from the trunking gateway to the outgoing gateway via a Cisco Unified Border Element, use the **h225 connect-passthru** command in voice class or H.323 voice-service configuration mode. To return to the default behavior, use the **no** form of this command.

h225 connect-passthru
no h225 connect-passthru

Syntax Description

This command has no arguments or keywords.

Command Default

The H.225 messages are not sent to the outgoing gateway until TCS/MSD/OLC negotiation takes place.

Command Modes

H.323 voice-service configuration (conf-serv-h323)
Voice class configuration (config-class)

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

Calls placed through a Cisco Unified Border Element may fail to connect when the originating or terminating H.323 device is a non-Cisco IOS VoIP device such as Cisco Unified Communications Manager.

The default behavior of H.323-to-H.323 calls through a Cisco Unified Border Element is to delay sending a H.225 Connect message to the originating H323 device until the H245 TCS/MSD/OLC negotiation takes place. During this process, an H.225 Connect message with an H.245 address present from the terminating H.323 device is changed to an H.225 Progress message, followed by an H.225 Facility message with the embedded H.245 address. This can cause connection failures if the originating H.323 device is waiting for the H.225 Connect message to begin the H245 TCS/MSD/OLC negotiation.

The **h225 connect-passthru** command is used to immediately pass H.225 connect messages from the trunking gateway to the outgoing gateway via a Cisco Unified Border Element.

Configuring the **h225 connect-passthru** command in H.323 voice-service configuration is recommended for all calls passed through the Cisco Unified Border Element. This command option will be present only when the **allow-connections** command is configured.

This command is often configured with the **h245 passthru tcsnonstd-passthru** command and **emptycapability** command when interworking is configured between non-Cisco IOS H.323 devices.

Examples

The following example shows the **h225 connect-passthru**command being configured under H.323 voice-service configuration mode:

```
Router(conf-serv-h323)# h225 connect-passthru
```

The following example shows the **h225 connect-passthru**command being configured under voice class configuration mode:

```
Router(config-class)# h225 connect-passthru
```

Related Commands

Command	Description
allow-connections	Allows connections between specific types of endpoints in a VoIP network.
emptycapability	Eliminates the need for identical codec capabilities for all dial peers in the rotary group
h245 passthru tcsnonstd-passthru	Passes TCS parameter (CCM data only).

h225 display-ie

To allow the Cisco Unified Communication Manager to ignore the H.225 Facility message and process the H.225 Notify message used to display the calling name on the IP Phone, use the **h225 display-ie ccm-compatible** command in voice service or voice class configuration mode. To return to the default configuration, use the **no** version of the command.

h225 display-ie ccm-compatible system
no h225 display-ie ccm-compatible system

Syntax Description

ccm-compatible	Q931 Facility with calling name is received the gateway sends both H225 Notify and H225 Facility messages with the calling name in the Display IE.
system	Interprets the H.323 Notify Display IE so that the IP Phone can display the calling name on the IP Phone

Command Default

Disabled. The Cisco Unified Communication Manager ignores the IE and does not display the calling name on the Cisco IP Phone.

Command Modes

H.323 voice-service configuration (conf-serv-h323)
Voice class configuration (config-class)

Command History

Release	Modification
12.4(11)XW	This command was introduced.
12. 4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

When the gateway is interoperating with Cisco Unified Communication Manager, you must enable the **h225 display-ie ccm-compatible** command to display the IE received in Q931 Facility message is sent out in the H.225 Notify message.

When the **h225 display-ie ccm-compatible**command is configured, the gateway sends the H.225 Facility message and the H.225 Notify message to the Cisco Unified Communication Manager, which ignores the H.225 Facility message, and processes the H.225 Notify message.

Note While interoperating only with Cisco Unified Connections Manager you must configure the **h225 display-ie ccm-compatible** command.

Behavior and configuration will vary based on the configuration mode the command is configured:

- When the **h225 display-ie ccm-compatible** command is configured under voice class, the CLI under voice class takes precedence. Even if the **h225 display-ie ccm-compatible** command is not configured under global voice service voip, the command configured under voice class takes effect. This means that when a Q931 Facility with calling name is received the gateway sends both H225 Notify and H225 Facility messages with the calling name in the Display IE.

The configured command is visible in the **show running-configuration** output under voice class.

- When the **h225 display-ie ccm-compatible system** command is configured under voice class, the command configured under global voice service VoIP takes precedence. If the **h225 display-ie ccm-compatible system** command is configured under voice service voip, the gateway sends a H225 Notify message. If the **h225 display-ie ccm-compatible system** command is not configured under voice service voip, the gateway will not send the H225 Notify message.

When the **system** keyword is configured, the command is not visible in the **show running-configuration** output.

- Configuring **no h225 display-ie ccm-compatible system** in voice class configuration mode, the command that is configured under voice class takes precedence. Even when **no h225 display-ie ccm-compatible system** command is configured under voice service voip, the gateway will not send the H225 Notify message received, and the calling name does not display on the IP Phone.

Use the **no** version to disable sending H225 Notify message on a particular VoIP dial-peer. The **no** form of the command is shown under voice class in the **show running-configuration**.

Examples

The following example shows a gateway being configured to send H.225 Notify message that displays the calling name on an IP Phone.

```
voice class h323 1
h225 display-ie ccm-compatible system
```

Related Commands

Command	Description
show running-configuration	Displays the contents of the currently running configuration file.

h225 h245-address

To control sending an H.245 address to a remote site use the **h225 h245-address** command in H.323 voice-service configuration mode or to a H.323 voice class in global configuration mode. To disable the delay in sending H.245 address in H.225 messages, use the **no** form of this command.

h225 h245-address {**facility** | **listen-on-setup** | **on-alert** | **on-progress**}
no h225 h245-address

Syntax Description

facility	Provides IP-to-IP H.245 address reporting via the H.225 Facility msg.
listen-on-setup	IP-to-IP invokes H.245 listener if the H.245 address received in setup.
on-alert	Specifies the H.225 address on alerting control.
on-progress	Specifies the H.225 address progress control.

Command Default

The H.245 address is sent in H.225 Callproceeding message.

Command Modes

H.323 voice-service configuration (conf-serv-h323)
H.323 voice class (config-class)

Command History

Release	Modification
12.4(15)T7	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **h225 h245-address on-alert** command controls sending the local H.245 address to the remote side. Configuring the **h225 h245-address on-alert** command forces the Cisco IOS gateway to send the H.245 address in the H.225 alerting message instead of in the H.225 callproceeding message.

To configure the **h225 h245-address on-alert**command for a voice class. First create an H.323 voice class that is independent of a dial peer with the **voice class h323** command in global configuration mode and configure the **allow-connections** command.

Note 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 globally delays the sending the H.245 transport address until call alerting happens:

```
Router(config)
#
 voice service voip
```

```
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 h245-address on-alert
```

The following example shows listen-on-setup capability configured mode after creating a voice class in global configuration mode and configuring the required **allow-connections** command:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# voice service voip
Router(conf-voi-serv)# allow-connections H323 to h323

Router(conf-voi-serv)# exit

Router(config)# voice class h323 5
Router(config-class)# h225 h245-address listen-on-setup
```

Related Commands

Command	Description
allow-connections	Allows connections between specific types of endpoints in a VoIP network.
h225 h245-address on-connect (H.323 voice-class)	Enables for an individual dial peer a delay in the exchange of H.225 messages for the relay of H.245 transport addresses until call connections are made.
h323	Enters Voice service H.323 configuration mode.
voice class h323	Creates an H.323 voice class that is independent of a dial peer and can be used on multiple dial peers.
voice-class h323	Assigns an H.323 voice class to a VoIP dial peer.
voice service	Enters voice-service configuration mode.

h225 h245-address on-connect (H.323 voice-class)

To enable for an individual dial peer a delay in the exchange of H.225 messages for the relay of H.245 transport addresses until call connections are made, use the **h225 h245-address on-connect**command in voice-class configuration mode. To disable the delay of H.225 messages, use the **no** form of this command.

h225 h245-address on-connect
no h225 h245-address on-connect

Syntax Description

This command has no arguments or keywords.

Command Default

H.225 messages that contain H.245 addresses are delayed until calls are connected.

Command Modes

Voice-class configuration (config-voice-class)

Command History

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

Usage Guidelines

The functionality specified by this command allows Cisco CallManager Express 3.1 (Cisco CME 3.1) or later systems to interwork with Cisco CallManager in the same network. This command should always be enabled.

When simple A-to-B calls are made from a Cisco CallManager phone to a Cisco CME IP phone, the Cisco CallManager must play in-band ringback tone locally to the originating phone. The Cisco CallManager stops the tone generation if it receives the call's H.245 address before the call is answered. The **h225 h245-address on-connect** command ensures that the H.245 address is not sent before the call is answered (connected). This command is enabled by default unless the **no** form of this command has been used. In addition, the **telephony-service ccm-compatible** command must also be enabled to detect calls from Cisco CallManager, which is the default.

This command can also be used in an H.323 voice-service definition to globally enable or disable this behavior.

Examples

The following example creates a voice class with the tag of 4, which delays the exchange of H.225 messages for H.245 transport address relay until a call connection is made. Voice class 4 is then applied to dial peer 36.

```
Router(config)
#
 voice class h323 4
Router(config-voice-class)# h225 h245-address on-connect
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
h225 h245-address on-connect (H.323 voice-service)	Globally delays the exchange of H.225 messages for the relay of H.245 transport addresses until call connections are made.
telephony-service ccm-compatible (H.323 voice-class)	For an individual dial peer, enables the detection of a Cisco CallManager system in the network.
telephony-service ccm-compatible (H.323 voice-service)	Globally enables the detection of a Cisco CallManager system in the network.
voice class	Enters voice-class configuration mode.

h225 h245-address on-connect (H.323 voice-service)

To globally delay the exchange of H.225 messages for the relay of H.245 transport addresses until call connections are made, use the **h225 h245-address on-connect**command in H.323 voice-service configuration mode. To globally disable the delay, use the **no** form of this command.

h225 h245-address on-connect
no h225 h245-address on-connect

Syntax Description

This command has no arguments or keywords.

Command Default

H.225 messages that contain H.245 addresses are delayed until calls are connected.

Command Modes

H.323 voice-service configuration (conf-serv-h323)

Command History

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

Usage Guidelines

The functionality specified by this command allows Cisco CallManager Express 3.1 (Cisco CME 3.1) or later systems to interwork with Cisco CallManager in the same network. This command should always be enabled.

When simple A-to-B calls are made from a Cisco CallManager phone to a Cisco CME IP phone, the Cisco CallManager must play in-band ringback tone locally to the originating phone. The Cisco CallManager stops the tone generation if it receives the call's H.245 address before the call is answered. The **h225 h245-address on-connect** command ensures that the H.245 address is not sent before the call is answered (connected). This behavior is the default when a Cisco CME system detects an incoming call from a Cisco CallManager unless the **no** form of this command has been used. In addition, the **telephony-service ccm-compatible** command must also be enabled to detect calls from Cisco CallManager, which is the default.

This command can also be used in an H.323 voice-class definition to enable or disable this behavior for individual dial peers.

Examples

The following example globally delays the exchange of H.225 messages for H.245 transport address relay until a call connection is made.

```
Router(config)
#
 voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 h245-address on-connect
```

Related Commands

Command	Description
h225 h245-address on-connect (H.323 voice-class)	Enables for an individual dial peer a delay in the exchange of H.225 messages for the relay of H.245 transport addresses until call connections are made.
h323	Enters H.323 voice-service configuration mode.

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

h225 h245-address setup

To allow a gateway to connect to an H.245 address received simultaneously with the H.225 setup message use the **h225 h245-address setup** command in voice service configuration mode or a H.323 voice class in global configuration mode. To return to the default behavior, use the **no** form of this command.

h225 h245-address setup
no h225 h245-address setup

Syntax Description

setup	Connects the gateway to the H.245 address simultaneously with an incoming H.225 setup message.

Command Default

This command is disabled by default. The gateway does not connect to the H.245 address received along with the H.225 setup message.

Command Modes

H.323 voice-service configuration (conf-serv-h323)
H.323 voice class (config-class)

Command History

Release	Modification
12.4(15)T3	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Configuring the **h225 h245-address setup**command allows the gateways to receive both the H.225 setup message simultaneously with the H.245 address message.

To configure the **h225 h245-address setup**command for a voice class. First create an H.323 voice class that is independent of a dial peer with the **voice class h323** command in global configuration mode and configure the **allow-connections** command.

Note 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 shows the gateway globally configured to connect to the H.245 address received along with the H.225 setup message:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 h245-address setup
```

The following example shows the gateway configured in a voice-class to connect to the H.245 address received along with H.225 setup message:

```
Router(config)# voice class h323 12
Router(config-class)# h225 h245-address setup
```

Related Commands

Command	Description
allow-connections	Allows connections between specific types of endpoints in a VoIP network.
h225 h245-address on-connect (H.323 voice-class)	Enables for an individual dial peer a delay in the exchange of H.225 messages for the relay of H.245 transport addresses until call connections are made.
h323	Enters Voice service H.323 configuration mode.
voice class h323	Creates an H.323 voice class that is independent of a dial peer and can be used on multiple dial peers.
voice-class h323	Assigns an H.323 voice class to a VoIP dial peer.
voice service	Enters voice-service configuration mode.

h225 id-passthru

To enable video call connections to pass through between endpoints regardless of software version, use the **h225 id-passthru**command in H.323 voice-service configuration mode. To return to the default, use the **no**form of this command.

h225 id-passthru
no h225 id-passthru

Syntax Description

This command has no arguments or keywords.

Command Default

Video calls are completed on endpoints using the same software version.

Command Modes

H.323 voice-service configuration (config-serv-h323)

Command History

Release	Modification
12.3(14)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Video calls complete when the endpoints are operating the same version of software. Use this command to allow connections between video endpoints that are using different software versions.

Examples

The following example allows video calls to connect when the polycom endpoints are using different software versions:

```
Router(config-serv-h323)# h225 id-passthru
```

Related Commands

Command	Description
h323	Enables H.323 voice service configuration commands.

h225 plus-digit passthru

To prefix and pass the plus digit (+) into a phone number on an H.323 trunk, use the **h225 plus-digit passthru**command in H.323 voice service configuration mode. To stop passing of the plus digit into a phone number, use the **no** form of this command.

For releases prior to 15.1(3)T
h225 plus-digit-passthru-calling
no h225 plus-digit-passthru-calling
h225 plus-digit-passthru-called
no h225 plus-digit-passthru-called

For 15.1(3)T and later releases
h225 plus-digit passthru {**destination** | **source**}
no h225 plus-digit passthru {**destination** | **source**}

Syntax Description

destination	Prefixes and passes the plus digit (+) into a destination (called) number on an H.323 trunk.
source	Prefixes and passes the plus digit (+) into a source (calling) number on an H.323 trunk.

Command Default

The plus digit is not prefixed and passed into a called or a calling number on an H.323 trunk.

Command Modes

H.323 voice service configuration (conf-serv-h323)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.1(3)T	This command was modified. The **destination** and **source** keywords replaced **plus-digit-passthru-calling** and **plus-digit-passthru-called**for Cisco IOS Releaase 15.1(3)T and later releases.

Usage Guidelines

When a "+" is prefixed before the dialed digits, the carrier recognizes the call as an International call without the country specific international operator dial string. The leading "+" digit in a dial-peer match pattern is used to match a phone number with a leading "+" E.164 digit. It is not used as a regular expression symbol but is a valid E.164 digit that should be preserved across the VoIP network.

Examples

The following example shows how to add the plus digit for the calling number using the **h225 plus-digit passthru source** command:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 plus-digit passthru source
```

The following example shows how to add the plus digit for the called number using the **h225 plus-digit passthru destination** command:

```
Router(config)# voice service voip
```

```
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 plus-digit passthru destination
```

h225 signal overlap

To activate overlap signaling to the destination gateway, use the **h225 signal overlap**command in H.225 voice-service configuration mode. To stop sending overlap signaling messages, use the **no** form of this command.

h225 signal overlap
no h225 signal overlap

Syntax Description

This command has no arguments or keywords.

Command Default

H.225 signaling overlap is disabled.

Command Modes

H.323 voice-service configuration (conf-serv-h323)

Command History

Release	Modification
12.2(15)T11	This command was introduced.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines

The terminating gateway is responsible for collecting all the called number digits. This is implemented by the dial peers matching destination patterns. When H.225 signal overlap is configured on the originating gateway, it sends the SETUP to the terminating gateway once a dial-peer match is found. The originating gateway sends all further digits received from user to the terminating gateway using INFO messages until it receives a sending complete from the user. The terminating gateway receives the digits in SETUP and subsequent INFO messages and does a dial-peer match. If a match is found, it sends a SETUP with the collected digits to the PSTN. All subsequent digits are sent to the PSTN using INFO messages at which time the call is complete.

Examples

The following example enables overlap signalling on the H.225 gateway:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 signal overlap
```

Related Commands

Command	Description
h323	Enables H.323 voice service configuration commands.
voice service	Enters voice-service configuration mode and specifies the voice encapsulation type.

h225 start-h245

To hold the H.245 connection procedures until after the H.225 connections are made, use the **h225 start-h245** command in H.323 voice-class configuration mode. To disable the connection sequence, use the **no** form of this command.

h225 start-h245 on-connect
no h225 start-h245 on-connect

Syntax Description

on-connect	Starts the H.245 procedure upon call connection.

Command Default

By default, h225 start-h245 on-connect is disabled. In case of IP-to-IP gateway (IPIPGW), the outbound gateway echoes the same h245 address and port number sent by the remote endpoint.

Command Modes

H.323 voice-class configuration (config-voice-class)
H.323 voice-service (conf-serv-h323)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The **h225 start-245 on-connect** command ensures that the H.245 address is not sent before the call is answered (connected).

Configure this command in H.323 voice-service configuration mode to globally enable or disable the connection behavior.

Examples

The following example shows a voice class with the tag of 4 being created, which delays the exchange of H.225 messages for H.245 transport address relay until a call connection is made.

```
Router(conf-serv-h323)#h225 start-h245 on-connect
```

Related Commands

Command	Description
h225 h245-address on-connect (H.323 voice-service)	Globally delays the exchange of H.225 messages for the relay of H.245 transport addresses until call connections are made.
telephony-service ccm-compatible (H.323 voice-class)	Detects a Cisco CallManager system in the network for an individual dial peer.
telephony-service ccm-compatible (H.323 voice-service)	Detects a Cisco CallManager system in the network globally.
voice class	Enters voice-class configuration mode.

h225 timeout call-proceeding

To set the H.225 call-proceeding (T310) disconnect timer, use the **h225 timeout call-proceeding**command in either Voice service VoIP or H.323 voice class configuration mode. To revert to the default, use the **no** form of this command.

h225 timeout call-proceeding *duration*
no h225 timeout call-proceeding

Syntax Description

duration	Call-proceeding timeout, in seconds. Range: 1 to 300. Default: 60.

Command Default

60 seconds

Command Modes

For all dial peers: Voice service VoIP configuration (config-voi-srv)
For a single dial peer: H.323 voice class (config-class)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use this command to set a maximum duration for the time between call setup and call connect.

You can use this command in either of two configuration modes:

- For all peers: Use voice-service configuration mode by entering the **voice service voip** command
- For just a single dial peer: Use dial-peer configuration mode for the desired dial peer by entering the **voice class h323** command.

Examples

The following example sets the disconnect timer for all dial peers:

```
Router(config)# voice service voip
Router(config-voi-serv)# h225 timeout call-processing 5
```

The following example sets the disconnect timer for a single dial peer:

```
Router(config)# voice class h323 1
Router(config-class)# h225 timeout call-processing 5
```

Related Commands

Command	Description
h225 timeout setup	Sets a timer for the response of the outgoing SETUP message.
h225 timeout tcp call-idle	Sets a timer for an idle call connection.
h225 timeout tcp establish	Sets an H.225 TCP timer for VoIP dial peers.

Command	Description
scenario-cause	Configures new Q.850 call-disconnect cause codes for use if an H.323 call fails.

h225 timeout keepalive

To disconnect H.323 calls when a TCP keepalive timeout occurs, use the **h225 timeout keepalive** command in H.323 voice-service configuration mode. To enable H.323 calls to remain active and ignore the TCP keepalive timeout, use the no form of this command.

h225 timeout keepalive
no h225 timeout keepalive

Syntax Description

This command has no arguments or keywords.

Command Default

TCP keepalives are enabled.

Command Modes

H.323 voice-service configuration (conf-serv-h323)

Command History

Release	Modification
12.2(15)T12	This command was introduced.
12.3	This command was integrated into Cisco IOS Release 12.3.
12.3(4)T5	This command was integrated into Cisco IOS Release 12.3(4)T5.

Usage Guidelines

When using the default configuration of the **h225 timeout keepalive** command, if a TCP timeout occurs on the H.225 channel, all active calls are disconnected and corresponding H.225 TCP sockets are closed.

When the **no h225 timeout keepalive** command is configured and a timeout occurs, the H.225 TCP socket is closed for all calls; Active TDM-IP calls will be preserved, but IP to IP calls are disconnected. In both cases the H.225 TCP socket is closed.

Note This command is visible in the running configuration only when the user configures the **no** form of the command.

Examples

The following example enables TCP keepalives on H.225 VoIP call control sessions:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 timeout keepalive
```

Related Commands

Command	Description
h323	Enables H.323 voice service configuration commands.
voice service	Enters voice-service configuration mode and specifies the voice encapsulation type.

h225 timeout setup

To configure the timeout value for the response of the outgoing SETUP message, use the **h225 timeout setup** command in H.323 voice class configuration mode. To remove the timeout value, use the **no** form of this command.

h225 timeout setup *seconds*
no h225 timeout setup

Syntax Description

seconds	Timeout value for the response of the outgoing SETUP message, in seconds. Default is 15.

Command Default

15 seconds

Command Modes

H.323 voice class (config-class)

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.

Examples

The following example configures a timeout setup value of 10 seconds:

```
Router(config-class)# h225 timeout setup 10
```

Related Commands

Command	Description
h225 timeout tcp call -idle	Sets a timer for an idle call connection.
h225 timeout tcp establish	Configures the H.225 TCP timeout.

h225 timeout t302

To set the t302 timer when using overlap signaling, use the **h225 timeout t302** command in H.225 voice-service configuration mode. To return to the default overlap signaling setting, use the **no** form of this command

h225 timeout t302 *seconds*
no h225 timeout t302 *seconds*

Syntax Description

seconds	Number of seconds for timeouts. Range: 1 to 30

Command Default

The t302 timer is disabled.

Command Modes

Voice service H.323 configuration (conf-serv-h323)

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

Use this command to establish the maximum amount of time allowed to complete the dial-peer match when H.225 signal overlap is configured on the originating gateway.

Examples

The following example allows 15 seconds for the t302 timer to complete the dial-peer match before timing out:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 timeout t302 15
```

Related Commands

Command	Description
h225 signal overlap	Activates overlap signaling to the destination gateway.
h323	Enables H.323 voice service configuration commands.
voice service	Enters voice-service configuration mode and specifies the voice encapsulation type.

h225 timeout t304

To set the t304 timer when using overlap signaling, use the **h225 timeout t304** command in H.323 voice-service configuration mode. To return to the default overlap signaling setting, use the **no** form of this command.

h225 timeout t304 *seconds*
no h225 timeout t304 *seconds*

Syntax Description

seconds	Length of timeout, in seconds. The range is from 1 to 30. The default is 10.

Command Default

The timer is enabled and set to 10 seconds.

Command Modes

Voice service H.323 configuration (conf-serv-h323)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **h225 timeout t304** command to configure the maximum interdigit delay on the originating gateway when H.225 overlap signaling is configured. Configure this command for the H.323 call leg on the originating gateway. If this timer expires, the call is disconnected with a cause code 28 (invalid number).

Examples

The following example allows 12 seconds for the t304 timer to complete the dial-peer match before timing out:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 timeout t304 12
```

Related Commands

Command	Description
h225 timeout t302	Sets the t302 timer when using overlap signaling.
h225 signal overlap	Activates overlap signaling to the destination gateway.
h323	Enables H.323 voice-service configuration commands.
voice service	Enters voice-service configuration mode and specifies the voice encapsulation type.

h225 timeout tcp call-idle (H.323 voice service)

To set a timer for an idle call connection, use the **h225 timeout tcp call-idle**> command in H.323 voice service configuration mode. To reset to the default, use the no form of this command.

h225 timeout tcp call-idle {**value** *value* | **never**}
no h225 timeout tcp call-idle

Syntax Description

value *value*	Timeout value, in minutes. Range is 0 to 1440. The default is 10. If you specify 0, the timer is disabled and the TCP connection is closed immediately after all the calls are cleared.
never	The connection is maintained permanently or until the other endpoint closes it.

Command Default

10 minutes

Command Modes

Voice service H.323 configuration (conf-serv-h323)

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

This command specifies the time to maintain an established H.225 TCP connection when there are no calls on that connection. If the timer expires, the connection is closed. If the timer is running and any new call is made on that connection, the timer stops. When all the calls are cleared on that connection, the timer starts again.

Examples

The following example sets the timer for an idle call connection to 10 minutes:

```
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h225 timeout tcp call-idle value 10
```

Related Commands

Command	Description
h323	Enables H.323 voice-service configuration commands.

h225 timeout tcp establish

To set the H.225 TCP timeout value for Voice over IP (VoIP) dial peers, use the h225 timeout tcp establish command in voice class configuration mode. To reset to the default, use the no form of this command.

h225 timeout tcp establish seconds
no h225 timeout tcp establish

Syntax Description

seconds	Number of seconds for the timeout. Range is 0 to 30. The default is 15. If you specify 0, the H.225 TCP timer is disabled.

Command Default

15 seconds

Command Modes

Voice class configuration

Command History

Release	Modification
12.1(2)T	This command was introduced on the following platforms: Cisco 1700, Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 7200, Cisco AS5300, Cisco uBR900, and Cisco uBR924.

Examples

The following example sets a timeout of 10 seconds, which is associated with the H.323 voice class labeled 1:

```
voice class h323 1
 h225 timeout tcp establish 10
```

Related Commands

Command	Description
voice class h323	Establishes an H.323 voice class.

h225 timeout ntf

To enable Cisco Unified Communications Manager to interpret the calling name coming in the Display IE of H.225 facility message, use the **h225 timeout ntf** command in voice service or voice class configuration mode. To return to the default configuration, use the **no** form of this command.

h225 timeout ntf *milliseconds*
no h225 timeout ntf *milliseconds*

Syntax Description

milliseconds	Amount of time in milliseconds. Valid range is 50 to 5000.

Command Default

Disabled. The Cisco Unified Communications Manager ignores the IE and does not display the calling name on the IP phone.

Command Modes

H.323 voice-service configuration (conf-serv-h323)
Voice class configuration (config-class)

Command History

Release	Modification
12.4(11)XW	This command was introduced.
12. 4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Configure this command on the gateway to control the Q931 setup message. This command is configured in voice service or voice class configuration mode.

When Cisco Unified Communications Manager (Cisco Unified CM) is interworking with Cisco Gateways, The Cisco Unified CM can interpret the calling name coming in Display IE of H.225 Setup and H.225 Notify messages, and display the calling name on the Cisco IP Phone. Calling names sent in Display IE of the H.225 Facility message are not interpreted by default.

When the **h225 timeout ntf**command is configured on the Cisco gateway, if a Q931 Setup message with name-to-follow comes, the gateway will not send the H.225 Setup message and buffers it until the ntf timer expires, or a Q931 Facility message is received from ISDN side.

Note In the event the facility is received before the timer expires, the gateway will stop the buffer timer, extract the relevent information and send it to terming endpoint.

When a Cisco gateway is connected to ISDN switches that send name-to-follow in Q931 Setup and the calling name in subsequent Q931 Facility message, configuring the **h225 timeout ntf** command is recommended.

Examples

The following example shows how to set the ntf buffering time to 60 milliseconds in the voice servides configuration mode:

```
voice service voip
```

```
 h323
  h225 timeout ntf 60
```

The following example sshows hotto se the ntf buffering time to 1000 milliseconds in the voice class configuration mode:

```
voice class h323 1
 h225 timeout ntf 1000
```

h245 address-check

To close the TCP connection of the endpoint with the numerically smaller H.245 address when two endpoints simultaneously initiate separate H.245 connections, use the **h245 address-check** command in H.323 voice-service configuration mode. To return to the default behavior, use the **no** form of this command.

h245 address-check
no h245 address-check

Syntax Description

This command has no arguments or keywords.

Command Default

The gateway automatically closes its TCP connection when the remote side TCP connection attempts to overwrite the data on the existing gateway TCP connection.

Command Modes

H.323 voice-service configuration (conf-serv-h323)

Command History

Release	Modification
15.0(1)M2	This command was introduced.

Usage Guidelines

The **h245 address-check**command causes the gateway to use IP addresses to determine which endpoint to close when TCP connections are opened simultaneously. The gateway TCP connection is closed only if the IP address is smaller.

Examples

The following example shows how to close the TCP connection of the endpoint with the numerically smaller H.245 address when two endpoints simultaneously initiate separate H.245 connections

```
Router(conf-serv-h323)# h245 address-check
```

Related Commands

Command	Description
h323	Enables H.323 voice service configuration commands.

h245 passthru

To allow H.245 calls to pass through to the Cisco Unified CallManager when the IP-to-IP gateway sends an incorrect intercluster trunk (ICT) version, use the **h245 passthru**command in voice service configuration mode. To disable this command use, the **no**form of this command.

h245 passthru {**all** | **tcsnonstd-passthru**}
no h245 passthru {**all** | **tcsnonstd-passthru**}

Syntax Description

all	Passes non-standard codec through the IP-to-IP gateway.
tcsnonstd -passthru	Passes terminal capabilities set (TCS) non-standard parameter pass through (CCM data only).

Command Default

This command is disabled.

Command Modes

Voice service H.323 configuration (conf-serv-h323)

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

When resuming a call that was placed on hold fails on a Cisco Unified CallManager, generally the call fails on the second Cisco Unified CallManager because the IP-to-IP gateway (IPIPGW) sends an incorrect intercluster trunk (ICT) version for the first Cisco Unified CallManager to the second Cisco Unified CallManager, and because the IPIPGW drops the non-standard fields in the callproc, alert, and connect messages from the second Cisco Unified CallManager to the first Cisco Unified CallManager. To resolve this behavior configure the **h245 passthru**command

Note For IP-to-IP gateway functionality the **allow-connections h323 to h323** command must be configured.

Examples

The following example show how you configure h.245 to pass through to the Cisco Unified CallManager, regardless of the intercluster trunk (ICT) version:

```
Router(conf-serv-h323)#h245 passthru tcsnonstd-passthru
```

Related Commands

Command	Description
allow-connections	Allows connections between specific types of endpoints in a VoIP network.

h245 timeout

To set the timeout value for the Open Logical Channel (OLC) and Terminal Capability Set (TCS) messages, use the **h245 timeout** command in H.323 voice-service configuration mode. To disable the timeout value for the these messages, use the **no** form of this command

h245 timeout[**OLC***(1-30)* | **TCS***(1-45)*]
no h245 timeout

Syntax Description

OLC	The range is from 1 to 30.
TCS	The range is from 1 to 45.

Command Default

Timeout value for the OLC message is enabled and set to 4 seconds. Timeout value for the TCS message is enabled and set to 15 seconds.

Command Modes

Voice service H.323 configuration (conf-serv-h323)

Command History

Release	Modification
12.4	This command was introduced as **h245 timeout OLC**.
12.4(24)T	This command was modified. The command was renamed to **h245 timeout**. OLC became an argument and TCS argument was added.

Usage Guidelines

OLC --After the originating gateway sends an OLC message during the H.245 procedure, it waits for 4 seconds for the terminating gateway to respond with an OLC acknowledgment. This behavior is enabled by default, and the timeout value of the OLC message is set to 4 seconds.

However, sometimes when a slow link, such as a satellite link, is involved in sending messages, a delay can occur. In that case, 4 seconds are not enough to receive OLC messages, and the call fails even when the terminating gateway had responded with OLC acknowledgment. To avoid the random dropping of VoIP calls, use the h245 timeout command to change the length of time that the originating gateway waits for OLC acknowledgment from the terminating gateway.

TCS --After the gateway sends a TCS, it waits 15 seconds for a response to this TCS. The normal behavior is for the connected peer to send its own TCS, and then an acknowledgement (TCSack) to the first TCS. The gateway will set the TCS timer waiting for this TCSack. In certain cases, especially when connecting to an H320 video call, this normal 15 second timeout may not be enough. This command allows the user to configure this timeout value from any value between 1 and 45 seconds. The behavior of the timeout is not changed. If the timer expires, the gateway will send a TCSrelease, and disconnect the call

Examples

The following example sets the timeout value for the OLC message to 20 seconds and the TCS message to 20 seconds:

```
h245 timeout olc 20
h245 timeout tcs 20
```

The following example sets the timeout values back to the default settings:

```
no h245 timeout olc 20
no h245 timeout tcs 20
```

The output of the show run command does not show the default setting; however, it does include the command if the timeout value is modified:

```
voice service voip
 h323
  h245 timeout olc 20
 h245 timeout tcs 20
```

Related Commands

Command	Description
h323	Enables H.323 voice service configuration commands.

h323

To enable the H.323 voice-service configuration commands, use the **h323** command in voice service configuration mode. To disable those commands, use the **no** form of this command.

h323

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Voice service VoIP configuration (config-voi-srv)

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.

Examples

The following example enters H.323 voice-service configuration mode:

```
Router(conf-voi-serv)# h323
```

Related Commands

Command	Description
call start	Forces the H.323 Version 2 gateway to use Fast Connect or Slow Connect procedures for all H.323 calls.
h225 timeout setup	Configures the timeout value for the response of the outgoing SETUP message.
h225 timeout tcp call-idle	Sets a timer for an idle call connection.
session transport	Configures the underlying transport layer protocol for H.323 messages to be used across all VoIP dial peers.

h323 asr

To enable application-specific routing (ASR) and specify the maximum bandwidth for a proxy, use the **h323 asr**command in interface configuration mode. To remove a bandwidth setting but keep ASR enabled, use **no**form of this command.

h323 asr [**bandwidth** *max-bandwidth*]
no h323 asr [**bandwidth** *max-bandwidth*]

Syntax Description

bandwidth *max-bandwidth*	(Optional) Maximum bandwidth, in mbps on the interface. Range is from 1 to 10000000. The default is the interface bandwidth. If you specify a value greater than the interface bandwidth, the bandwidth defaults to the interface bandwidth.

Command Default

ASR is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(2)NA	This command was introduced on the 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

This command is independent of the **h323 interface** command.

Note Specifying the **no h323 asr bandwidth** *max-bandwidth command*removes the bandwidth setting but leaves ASR enabled. You must enter the **no h323 asr** command to disable ASR.

Examples

The following example enables ASR and specifies a maximum bandwidth of 10,000 kbps:

```
h323 asr bandwidth 10000
```

h323 call start

To force the H.323 Version 2 gateway to use Fast Connect or Slow Connect procedures for all H.323 calls, use the **h323 call start** command in voice-service configuration mode. To reset to the default, use the **no** form of this command.

h323 call start {**fast** | **slow**}
no h323 call start

Syntax Description

fast	Gateway uses H.323 Version 2 (Fast Connect) procedures.
slow	Gateway uses H.323 Version 1 (Slow Connect) procedures.

Command Default

fast

Command Modes

Voice-service configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco AS5300, Cisco AS5800, and Cisco MC3810.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
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

In Cisco IOS Release 12.1(3)XI and later releases, H.323 Voice over IP (VoIP) gateways by default use H.323 Version 2 (Fast Connect) for all calls including those initiating RSVP. Previously, gateways used only Slow Connect procedures for RSVP calls. To enable Cisco IOS Release 12.1(3)XI gateways to be backward compatible with earlier releases of Cisco IOS Release 12.1 T, the **h323 call start** command forces the originating gateway to initiate calls using Slow Connect.

This **h323 call start** command is configured as part of the global voice-service configuration for VoIP services. It does not take effect unless the **call start system** voice-class configuration command is configured in the VoIP dial peer.

Examples

The following example selects Slow Connect procedures for the gateway:

```
voice service voip
 h323 call start slow
```

Related Commands

Command	Description
call rsvp -sync	Enables synchronization between RSVP and the H.323 voice signaling protocol.

Command	Description
call rsvp -sync resv-timer	Sets the timer for RSVP reservation setup.
call start	Selects whether the H.323 gateway uses Fast Connect or Slow Connect procedures for the specific VoIP dial peer.
debug call rsvp -sync events	Displays the events that occur during RSVP synchronization.
show call rsvp -sync conf	Displays the RSVP synchronization configuration.
show call rsvp -sync stats	Displays statistics for calls that attempted RSVP reservation.
voice service	Enters voice-service configuration mode and specifies the voice encapsulation type.

h323 gatekeeper

To specify the gatekeeper associated with a proxy and to control how the gatekeeper is discovered, use the **h323 gatekeeper**command in interface configuration mode. To disassociate the gatekeeper, use the **no** form of this command.

h323 gatekeeper [**id** *gatekeeper-id*] {**ipaddr** *ipaddr* [*port*] | **multicast**}
no h323 gatekeeper [**id** *gatekeeper-id*] {**ipaddr** *ipaddr* [*port*] | **multicast**}

Syntax Description

id *gatekeeper -id*	(Optional) Gatekeeper name. Typically, this is a Domain Name Server (DNS) name, but it can also be a raw IP address in dotted form. If this parameter is specified, gatekeepers that have either the default or explicit flags set for the subnet of the proxy respond. If this parameter is not specified, only those gatekeepers with the default subnet flag respond.
ipaddr *ipaddr* [*port*]	The gatekeeper discovery message is unicast to this address and, optionally, the port specified.
multicast	The gatekeeper discovery message is multicast to the well-known RAS multicast address and port.

Command Default

No gatekeeper is configured for the proxy

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500 series and Cisco 3600 series.

Usage Guidelines

You must enter the **h323 interface** and **h323 h323-id**commands before using this command. The **h323 gatekeeper** command must be specified on your Cisco IOS platform or the proxy does not go online. The proxy uses the interface address as its RAS signaling address.

Examples

The following example sets up a unicast discovery to a gatekeeper whose name is unknown:

```
h323 gatekeeper ipaddr 192.168.5.2
```

The following example sets up a multicast discovery for a gatekeeper of a particular name:

```
h323 gatekeeper id gk.zone5.com multicast
```

Related Commands

Command	Description
h323 h323-id	Registers an H.323 proxy alias with a gatekeeper.
h323 interface	Specifies the interface from which the proxy takes its IP address.

h323 h323-id

To register an H.323 proxy alias with a gatekeeper, use the **h323 h323-id**command in interface configuration mode. To remove an H.323 proxy alias, use the **no** form of this command.

h323 h323-id *h323-id*
no h323 h323-id *h323-id*

Syntax Description

h323 -id	Name of the proxy. It is recommended that this name be a fully qualified e-mail ID, with the domain name being the same as that of its gatekeeper.

Command Default

No H.323 proxy alias is registered

Command Modes

Interface configuration (config-if)

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.

Usage Guidelines

Each entry registers a specified H.323 ID proxy alias to a gatekeeper. Typically, these aliases are either simple text strings or legitimate e-mail IDs.

Note You must enter the **h323 interface** command before using this command. The **h323 h323-id** command must be entered on the same interface as the **h323 gatekeeper**command. The proxy does not go online without the **h323 interface** command.

Examples

The following example registers an H.323 proxy alias called proxy1@zone5.com with a gatekeeper:

```
h323 h323-id proxy1@zone5.com
```

Related Commands

Command	Description
h323 gatekeeper	Specifies the gatekeeper associated with a proxy and controls how the gatekeeper is discovered.
h323 interface	Specifies the interface from which the proxy takes its IP address.

h323 interface

To select an interface whose IP address is used by the proxy to register with the gatekeeper, use the **h323 interface**command in interface configuration mode. To reset to the default port, use the **no**version of the command and then the **h323 interface** command.

h323 interface [*port-number*]
no h323 interface [*port-number*]

Syntax Description

port -number	(Optional) Port number that the proxy listens on for incoming call-setup requests. Range is from 1 to 65356. The default port number for the proxy is 11,720 in -isx- or -jsx- Cisco IOS images. The default port number for the proxy is 1720 in -ix- Cisco IOS images, which do not contain the VoIP gateway.

Command Default

Default port number is image dependent as described in the Syntax Description.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500 and Cisco 3600 series routers.
12.1(5)T	The ability to specify the proxy port number was added on the Cisco 2600 series, Cisco 3600 series, Cisco 7200 series and on the Cisco MC3810.

Usage Guidelines

At proxy startup, Cisco IOS software checks for the presence of the VoIP gateway subsystem. If the subsystem is found to be present, the proxy code opens and listens for call setup requests on the new port. The proxy then registers this port with the gatekeeper.

Examples

The following example configures Ethernet interface 0 for incoming call-setup requests:

```
interface ethernet0
 h323 interface
```

Related Commands

Command	Description
bandwidth	Specifies the maximum aggregate bandwidth for H.323 traffic from a zone to another zone, within a zone, or for a session in a zone.
bandwidth remote	Specifies the total bandwidth for H.323 traffic between this gatekeeper and any other gatekeeper.
h323 qos	Enables QoS on the proxy.
h323 t120	Enables the T.120 capabilities on your router and specifies bypass or proxy mode.

h323 qos

To enable quality of service (QoS) on the proxy, use the **h323 qos**command in interface configuration mode. To disable QoS, use the **no** form of this command.

h323 qos {**ip-precedence** *value* | **rsvp** {**controlled-load** | **guaranteed-qos**}}
no h323 qos {**ip-precedence** *value* | **rsvp** {**controlled-load** | **guaranteed-qos**}}

Syntax Description

ip -precedence *value*	RTP streams set their IP precedence bits to the specified *value*.
rsvp controlled -load	Controlled load class of service.
rsvp guaranteed -qos	Guaranteed QoS class of service.

Command Default

No QoS is configured

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500 and Cisco 3600 series routers.

Usage Guidelines

You must execute the **h323 interface** command before using this command.

Both IP precedence and RSVP QoS can be configured by invoking this command twice with the two different QoS forms.

Examples

The following example enables QoS on the proxy:

```
interface Ethernet0
 ip address 172.21.127.38 255.255.255.192
 no ip redirects
 ip rsvp bandwidth 7000 7000
 ip route-cache same-interface
 fair-queue 64 256 1000
 h323 interface
 h323 qos rsvp controlled-load
 h323 h323-id px1@zone1.com
 h323 gatekeeper ipaddr 172.21.127.39
```

Related Commands

Command	Description
h323 interface	Specifies the interface from which the proxy takes its IP address.

h323 t120

To enable T.120 capabilities on your router and to specify bypass or proxy mode, use the **h323 t120**command in interface configuration mode. There is no **no** form of this command.

h323 t120 {**bypass** | **proxy**}

Syntax Description

bypass	Bypass mode. In this mode, the H.245 Open Logical Channel messages for T.120 data channels are passed unmodified through the proxy, and TCP connections for T.120 are established directly between the two endpoints of the H.323 call.
proxy	Proxy mode. In this mode, T.120 features function properly.

Command Default

Bypass mode

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(5)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.

Usage Guidelines

The **no** form of this command has no function--the only possible commands are **h323 t120 bypass** and **h323 t120 proxy**.

Examples

The following example enables T.120 capabilities:

```
proxy h323
interface ethernet0
 h323 t120 proxy
```

Related Commands

Command	Description
bandwidth	Specifies the maximum aggregate bandwidth for H.323 traffic from a zone to another zone, within a zone, or for a session in a zone.
bandwidth remote	Specifies the total bandwidth for H.323 traffic between this gatekeeper and any other gatekeeper.
h323 interface	Defines which port the proxy listens on.

h323-annexg

To enable the border element (BE) on the gatekeeper and to enter BE configuration mode, use the **h323-annexg** command in gatekeeper configuration mode. To disable the BE, use the no form of this command.

h323-annexg *border-element-id* **cost** *cost* **priority** *priority*
no h323-annexg

Syntax Description

border -element-id	Identifier of the Annex G border element that you are provisioning. Possible values are any International Alphabet 5 (IA5) string, without spaces and up to 20 characters in length. The *border-element-id* argument associates the gatekeeper with the BE identifier that is configured on the BE.
cost *cost*	Cost associated with this Annex G border element. When a gatekeeper sends requests to remote zones and to the BE in its attempt to resolve an address, the remote zone or BE that resolves the address and has the lowest cost and highest priority is given preference. Range is from 1 to 99. Default is 50.
priority *priority*	Priority associated with this Annex G border element. When a gatekeeper sends requests to remote zones and to the BE in its attempt to resolve an address, the remote zone or BE that resolves the address and has the lowest cost and highest priority is given preference. Range is 1 to 99. The default is 50.

Command Default

Cost: 50 Priority: 50

Command Modes

Gatekeeper 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

The Annex G border element must be configured using the **call-router** command before the gatekeeper can be associated with the Annex G border element. The **h323-annexg** command associates the gatekeeper with a previously configured Annex G border element and indicates that the gatekeeper should interact with the BE in address resolution.

Examples

The following example enables Annex G configuration for a BE named "be20":

```
Router(config-gk)# h323-annexg be20 cost 10 priority 40
Router(config-gk-annexg)#
```

Related Commands

Command	Description
call -router	Enables the Annex G border element configuration commands.
prefix	Restricts the prefixes for which the gatekeeper should query the Annex G BE.

h323-gateway voip bind srcaddr

To designate a source IP address for the voice gateway, use the h323-gateway voip bind srcaddr command in interface configuration mode. To remove the source IP address, use the no form of the command.

h323-gateway voip bind srcaddr *ip-address*
no h323-gateway voip bind srcaddr

Syntax Description

ip -address	Source IP address, in dotted-decimal notation.

Command Default

No default behaviors or values

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced on the following platforms: Cisco 1700, Cisco 2500, Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco AS5300, and Cisco uBR924.

Usage Guidelines

You do not have to issue this command on the interface that you defined as the voice gateway interface (although it may be more convenient to do so). Use this command the interface that contains the IP address to which you want to bind.

Examples

The following example assigns a source IP address of 10.1.1.1:

```
h323-gateway voip bind srcaddr 10.1.1.1
```

h323-gateway voip h323-id

To configure the H.323 name of the gateway that identifies this gateway to its associated gatekeeper, use the **h323-gateway voip h323-id** command in interface configuration mode. To disable this defined gateway name, use the **no** form of this command.

h323-gateway voip h323-id *interface-id*
no h323-gateway voip h323-id *interface-id*

Syntax Description

interface -id	H.323 name (ID) used by this gateway when this gateway communicates with its associated gatekeeper. Usually, this ID is the name of the gateway with the gatekeeper domain name appended to the end and in name@domain-name.

Command Default

No gateway identification is defined

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the Cisco 2500 series, Cisco 3600 series, and Cisco AS5300.
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.

Examples

The following example configures Ethernet interface 0.0 as the gateway interface. In this example, the gateway ID is GW13@cisco.com.

```
interface Ethernet0/0
 ip address 172.16.53.13 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id GK15.cisco.com ipaddr 172.16.53.15 1719
 h323-gateway voip h323-id GW13@cisco.com
 h323-gateway voip tech-prefix 13#
```

Related Commands

Command	Description
h323-gateway voip id	Defines the name and location of the gatekeeper for this gateway.
h323-gateway voip interface	Configures an interface as an H.323 interface.
h323-gateway voip tech-prefix	Defines the technology prefix that the gateway registers with the gatekeeper.

h323-gateway voip id

To define the name and location of the gatekeeper for a specific gateway, use the **h323-gateway voip id** command in interface configuration mode. To disable this gatekeeper identification, use the **no** form of this command.

h323-gateway voip id *gatekeeper-id* {**ipaddr** *ip-address* [*port-number*] | **multicast**} [**priority** *number*]
no h323-gateway voip id *gatekeeper-id* {**ipaddr** *ip-address* [*port-number*] | **multicast**} [**priority** *number*]

Syntax Description

gatekeeper -id	H.323 identification of the gatekeeper. This value must exactly match the gatekeeper ID in the gatekeeper configuration. The recommended format is *name.doman-name*.
ipaddr	The gateway uses an IP address to locate the gatekeeper.
ip -address	IP address used to identify the gatekeeper.
port -number	(Optional) Port number used.
multicast	Indicates that the gateway uses multicast to locate the gatekeeper.
priority *number*	(Optional) Priority of this gatekeeper. Range is 1 to 127, 1 has the highest priority. The default is 127.

Command Default

No gatekeeper identification is defined.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the following platforms: Cisco 2500 series, Cisco 3600 series, and Cisco AS5300.
12.0(7)T	The **priority** *number* keyword and argument were added.
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 tells the H.323 gateway associated with this interface which H.323 gatekeeper to talk to and where to locate it. The gatekeeper ID configured here must exactly match the gatekeeper ID in the gatekeeper configuration.

You can configure one or two alternate gatekeepers.

The IP address of the gatekeeper does not have to be explicit; you can also use the multicast option. Multicasting saves bandwidth by forcing the network to replicate packets only when necessary. The multicast option, shown below, notifies every gatekeeper in the LAN using a universal address, 224.0.1.41.

```
h323-gateway voip id GK1 multicast
h323-gateway voip id GK2 ipaddr 172.18.193.65 1719
```

Examples

The following example configures Ethernet interface 0.0 as the gateway interface and defines a specific gatekeeper for it. In this example, the gatekeeper ID is GK15.cisco.com, and its IP address is 172.16.53.15 (using port 1719).

```
interface Ethernet0/0
 ip address 172.16.53.13 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id GK15.cisco.com ipaddr 172.16.53.15 1719
 h323-gateway voip h323-id GW13@cisco.com
 h323-gateway voip tech-prefix 13#
```

Related Commands

Command	Description
h323-gateway voip h323-id	Configures the H.323 name of the gateway that identifies this gateway to its associated gatekeeper.
h323-gateway voip interface	Configures an interface as an H.323 interface.
h323-gateway voip tech-prefix	Defines the technology prefix that the gateway registers with the gatekeeper.

h323-gateway voip interface

To configure an interface as an H.323 gateway interface, use the h323-gateway voip interface command in interface configuration mode. To disable H.323 gateway functionality for an interface, use the **no** form of this command.

h323-gateway voip interface
no h323-gateway voip interface

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the following platforms: Cisco 2500, Cisco 3600 series, and Cisco AS5300.
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.

Examples

The following example configures Ethernet interface 0.0 as the gateway interface. In this example, the **h323-gateway voip interface** command configures this interface as an H.323 interface.

```
interface Ethernet0/0
 ip address 172.16.53.13 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id GK15.cisco.com ipaddr 172.16.53.15 1719
 h323-gateway voip h323-id GW13@cisco.com
 h323-gateway voip tech-prefix 13#
```

Related Commands

Command	Description
h323 -gateway voip h323-id	Configures the H.323 name of the gateway that identifies this gateway to its associated gatekeeper.
h323 -gateway voip id	Defines the name and location of the gatekeeper for this gateway.
h323 -gateway voip tech-prefix	Defines the technology prefix that the gateway registers with the gatekeeper.

h323-gateway voip tech-prefix

To define the technology prefix that the gateway registers with the gatekeeper, use the h323-gateway voip tech-prefix command in interface configuration mode. To disable this defined technology prefix, use the **no** form of this command.

h323-gateway voip tech-prefix *prefix*
no h323-gateway voip tech-prefix *prefix*

Syntax Description

prefix	Numbers used as the technology prefixes. Each technology prefix can contain up to 11 characters. Although not strictly necessary, a pound sign (#) is frequently used as the last digit in a technology prefix. Valid characters are 0 to 9, the pound sign (#), and the asterisk (*).

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the following platforms: Cisco 2500 series, Cisco 3600 series, and Cisco AS5300.
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 defines a technology prefix that the gateway then registers with the gatekeeper. 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 it can be used like an area code for more generic routing. No standard currently defines what the numbers in a technology prefix mean. By convention, technology prefixes are designated by a pound sign (#) as the last character.

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 configures Ethernet interface 0.0 as the gateway interface. In this example, the technology prefix is defined as 13#.

```
interface Ethernet0/0
 ip address 172.16.53.13 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id GK15.cisco.com ipaddr 172.16.53.15 1719
 h323-gateway voip h323-id GW13@cisco.com
 h323-gateway voip tech-prefix 13#
```

Related Commands

Command	Description
h323 -gateway voip h323-id	Configures the H.323 name of the gateway that identifies this gateway to its associated gatekeeper.
h323 -gateway voip id	Defines the name and location of the gatekeeper for this gateway.
h323 -gateway voip interface	Configures an interface as an H.323 interface.

h323zone-id (voice source group)

To specify the zone identification for an incoming H.323 call, use the **h323zone-id** command in voice source-group configuration mode. To delete the zone ID, use the **no**form of this command.

h323zone-id *name*
no h323zone-id *name*

Syntax Description

name	Zone ID name. Maximum size is 127 alphanumeric characters.

Command Default

No default behavior or values

Command Modes

Voice source-group configuration (cfg-source-grp)

Command History

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

Usage Guidelines

Use thiscommandto specify the zone to use for incoming H.323 calls in the voice source-group definition. The zone ID name matches the source zone ID of an incoming H.323 call.

Note The SIP protocol does not support zone ID functionality.

Examples

The following example associates zone ID "5400-gw1" with incoming calls for source IP group "northcal":

```
Router(config)# voice source-group northcal
Router(cfg-source-grp)# h323zone-id 5400-gw1
```

Related Commands

Command	Description
voice source-group	Defines a source group for voice calls.

h450 h450-3 timeout

To specify timeout values for call forwarding using the ITU-T H.450.3 standard, use the **h450 h450-3 timeout**command in H.323 voice service configuration mode. To return to the default, use the **no** form of this command.

h450 h450-3 timeout T1 *milliseconds*
no h450 h450-3 timeout T1

Syntax Description

T1	Timeout value to wait for a rerouting response.
milliseconds	Number of milliseconds. Range is from 500 to 60000. Default is 5000.

Command Default

T1 timer is 5000 milliseconds.

Command Modes

H.323 voice service configuration (conf-serv-h323)

Command History

Release	Modification
12.2(11)YT	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

Use this command with Cisco IOS Telephony Service (ITS) V2.1 or a later version.

This command is primarily used when the default setting for this timer does not match your network delay parameters. Refer to the ITU-T H.450.3 specification for more information on these timers.

Examples

The following example defines a T1 timeout of 3000 milliseconds:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# h450 h450-3 timeout T1 3000
```

Related Commands

Command	Description
h323	Enables H.323 voice service configuration commands.
voice service	Enters voice-service configuration mode.

handle-replaces

To configure a Cisco IOS device to handle Session Initiation Protocol (SIP) INVITE with Replaces header messages at the SIP protocol level, use the **handle-replaces** command in SIP UA configuration mode or voice class tenant configuration mode. To return to the default handling of SIP INVITE with Replaces header messages where messages are handled at the application layer, use the **no** form of this command.

handle-replaces system
no handle-replaces

Syntax Description

system	Specifies that the default handling of SIP INVITE with Replaces header messages 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

Handling of SIP INVITE with Replaces header messages takes place at the application layer.

Command Modes

SIP UA configuration (config-sip-ua)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(22)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**.

Usage Guidelines

On Cisco IOS devices running software earlier than Cisco IOS Release 12.4(22)T, SIP INVITE with Replaces header messages (such as those associated with Call Replacement during a Consult Call transfer scenario) are handled at the SIP protocol level. Beginning with Cisco IOS Release 12.4(22)T, the default behavior is for Cisco IOS devices to handle SIP INVITE with Replaces header messages at the application layer. To configure your Cisco IOS device to handle SIP INVITE with Replaces header messages at the SIP protocol level, use the **handle-replaces**command in SIP UA configuration mode.

Examples

The following example shows how to configure fallback to legacy handling of SIP INVITE messages:

```
Router(config)# sip-ua
Router(config-sip-ua)# handle-replaces
```

The following example shows how to configure fallback to legacy handling of SIP INVITE messages in the voice class tenant configuration mode:

```
Router(config-class)# handle-replaces system
```

Related Commands

Command	Description
supplementary-service sip	Enables SIP supplementary service capabilities for call forwarding and call transfers across a SIP network.

hangup-last-active-call

To define a Feature Access Code (FAC) to access the Hangup Last Active Call feature in feature mode on analog phones connected to FXS ports, use the **hangup-last-active-call** command in STC application feature-mode call-control configuration mode. To return the code to its default, use the **no** form of this command.

hangup-last-active-call *keypad-character*
no hangup-last-active-call

Syntax Description

keypad-character	Character string of one to four characters that can be dialed on a telephone keypad (0-9, *, #). Default is #1.

Command Default

The default value is #1.

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 the Hangup Last Active Call feature from the default (#1) 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.

Note For analog phones connected to FXS ports in Cisco Unified Communications Manager Express (CME), the **keep-conference drop-last** command must be enabled on the Cisco router.

Examples

The following example shows how to change the value of the feature code for the Hangup Last Active Call feature from the default (#1). With this configuration, a phone user must press hook flash during a three-party conference to get the feature tone and then dial 11 to drop the last active call party. The conference becomes a basic call.

```
Router(config)# stcapp call-control mode feature
```

```
Router(config-stcapp-fmcode)# hangup-last-active-call 11
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.
toggle-between-two-calls	Defines FAC in feature mode to toggle between two active calls.
transfer	Defines FAC in feature mode to connect a call to a third party that the phone user dials.

header-passing

To enable the passing of headers to and from Session Initiation Protocol (SIP) INVITE, SUBSCRIBE, and NOTIFY messages, use the **header-passing** command in Voice service SIP configuration mode. To disable header passing, use the **no** form of this command.

header-passing system
no header-passing system

Syntax Description

system	Specifies that the header-passing messages 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

Voice service VoIP configuration (conf-serv-sip).

Voice class tenant configuration (config-class).

Command History

Release	Modification
12.3(4)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**.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

The purpose of the command **header-passing**, which is configured under the **voice service voip**, is to pass the data contained within SIP headers arriving at the gateway to VXML applications hosted on the gateway or third-party servers.

Without this feature, the voice applications running on the gateway cannot access the headers that are sent in SIP requests. The SIP Header Passing feature makes SIP headers, the fields which specify session details in SIP messages, available to applications.

- This command applies to all SIP VoIP dial peers configured on a gateway. It enables header passing for SIP INVITE, SUBSCRIBE and NOTIFY messages; disabling header passing affects only incoming INVITE messages.
- There is no command to enable header passing on a per-call or per-application basis.
- Enabling header passing results in a slight increase in memory and CPU utilization.

Examples

The following example shows header-passing enabled:

```
Router(conf-serv-sip)# header-passing
```

The following example shows header-passing enabled: in the voice class tenant configuration mode.

```
Router(config-class)# header-passing system
```

Related Commands

Command	Description
debug voip ccapi protoheaders	Displays messages related to protocol headers.
retry subscribe	Configures the number of retries for SUBSCRIBE messages.
show subscription sip	Displays active SIP subscriptions.
subscription maximum originate	Specifies the maximum number of outstanding subscriptions that are originated by the gateway.

history-info

To enable Session Initiation Protocol (SIP) history-info header support on Cisco IOS gateway at a global level, use the **history-info** command in voice service voip sip configuration mode or voice class tenant configuration mode. To disable SIP history-info header support, use the **no** form of this command.

history-info system
no history-info system

Syntax Description

system	Specifies that the history-info header 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

History-info header support is disabled.

Command Modes

Voice service voip sip configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(22)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**.

Usage Guidelines

Use this command to enable history-info header support at a global 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:

```
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# history-info
```

The following example enables SIP history-info header support in the voice class tenant configuration mode:

```
Router(config-class)# history-info system
```

Related Commands

Command	Description
voice-class sip history-info	Enables SIP history-info header support at the dial-peer level.

history session event-log save-exception-only

To save in history only the event logs for application sessions that have at least one error, use the **history session event-log save-exception-only** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

history session event-log save-exception-only
no history session event-log save-exception-only

Syntax Description

This command has no arguments or keywords.

Command Default

All event logs for sessions are saved to history.

Command Modes

Application configuration monitor

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application history session event-log save-exception-only** command.

Usage Guidelines

Application event logs move from active to history after an instance terminates. If you use this command, the voice gateway saves event logs only for instances that had one or more errors. Event logs for normal instances that do not contain any errors are not saved to history.

Note This command does not affect records saved to an FTP server by using the **dump event-log** command.

Examples

The following example saves an event log in history only if the instance had an error:

```
application
monitor
history session event-log save-exception-only
```

Related Commands

Command	Description
call application history session event-log save-exception-only	Saves in history only the event logs for application sessions that have at least one error.
history session max-records	Sets the maximum number of application instance records saved in history.
history session retain-timer	Sets the maximum number of minutes for which application instance records are saved in history.

history session max-records

To set the maximum number of application instance records saved in history, use the **history session max-records**command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

history session max-records *number*
no history session max-records

Syntax Description

number	Maximum number of records to save in history. Range is 0 to 2000. Default is 360.

Command Default

360

Command Modes

Application configuration monitor

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application history session max-records** command.

Usage Guidelines

This command affects the number of records that display when you use the **show call application history session-level** command.

Examples

The following example sets the maximum record limit to 500:

```
application
monitor
history session max-records 500
```

Related Commands

Command	Description
call application history session max-records	Sets the maximum number of application instance records saved in history.
history session event-log save-exception-only	Saves in history only the event logs for application sessions that have at least one error.
history session retain-timer	Sets the maximum number of minutes for which application instance records are saved in history.

history session retain-timer

To set the maximum number of minutes for which application instance records are saved in history, use the **history session retain-timer**command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

history session retain-timer *minutes*
no history session retain-timer

Syntax Description

minutes	Maximum time, in minutes, for which history records are saved. Range is 0 to 4294,967,295. Default is 15.

Command Default

15

Command Modes

Application configuration mode

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application history session retain-timer** command.

Usage Guidelines

This command affects the number of records that display when you use the **show call application history session-level** command.

To enable event logging for voice applications, use the **event-log** command.

Examples

The following example sets the maximum time to save history records to 1 hour:

```
application
monitor
history session retain-timer 60
```

Related Commands

Command	Description
call application history session retain-timer	Sets the maximum number of minutes for which application instance records are saved in history.
event-log	Enables event logging for voice application instances.
history session event-log save-exception-only	Saves in history only the event logs for application instances that have at least one error.
history session max-records	Sets the maximum number of application instance records saved in history.
show call application session-level	Displays event logs and statistics for voice application instances.

hold-resume

To enable the Hold/Resume STC application supplementary-service feature on an FXS port, use the **hold-resume** command in supplementary-service voice-port configuration mode. To disable, use the **no** form of this command.

hold-resume
no hold-resume

Syntax Description

This command has no arguments or keywords.

Command Default

Feature is disabled.

Command Modes

Supplementary-service voice-port configuration (config-stcapp-suppl-serv-port)

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 enables the Hold/Resume STC application supplementary-service feature on analog endpoints that are connected to FXS ports on a Cisco IOS voice gateway, such as a Cisco integrated services router (ISR) or Cisco VG224 Analog Phone Gateway.

Examples

The following example shows how to enable Hold/Resume on port 2/0 on a Cisco VG 224.

```
Router(config)# stcapp supplementary-services
Router(config-stcapp-suppl-serv)# port 2/0
Router(config-stcapp-suppl-serv-port)# hold-resume
Router(config-stcapp-suppl-serv-port)# end
```

Related Commands

Command	Description
stcapp supplementary-services	Enters supplementary-service configuration mode for configuring STC application supplementary-service features on an FXS port.

hopcount

To specify the maximum number of border element (BE) hops through which an address resolution request can be forwarded, use the **hopcount**command in Annex G configuration mode. To restore the default, use the no form of this command.

hopcount *hopcount-value*
no hopcount

Syntax Description

hopcount -value	Maximum number of BE hops through which an address resolution request can be forwarded. Range is from 1 to 255. The default is 7.

Command Default

7 hops

Command Modes

Annex G configuration (config-annexg)

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. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 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.

Examples

The following example sets address-resolution forwarding to a maximum of 10 hops:

```
Router(config)# call-router h323-annexg be20
Router(config-annexg)# hopcount 10
```

Related Commands

Command	Description
call -router	Enables the Annex G border element configuration commands.
show call -router status	Displays the Annex G BE status.

host (SIP URI)

To match a call based on the host field, a valid domain name, IPv4 address, IPv6 address, or the complete domain name in a Session Initiation Protocol (SIP) uniform resource identifier (URI), use the **host** command in voice URI class configuration mode. To remove the host match, use the **no** form of this command.

host {**ipv4:** *ipv4- address* |**ipv6:***ipv6:address* | **dns:***dns-name* | *hostname-pattern* }
no host

Syntax Description

ipv4: *ipv4-address*	Specifies a valid IPv4 address.
ipv6: *ipv6-address*	Specifies a valid IPv6 address.
dns: *dns-name*	Specifies a valid domain name. The maximum length of a valid domain name is 64 characters.
hostname-pattern	Cisco IOS regular expression pattern to match the host field in a SIP URI. The maximum length of a hostname pattern is 32 characters.

Command Default

The calls are not matched on the host field, IPv4 address, IPv6 address, valid domain name, or complete domain name in the SIP URI.

Command Modes

Voice URI class configuration (config-voice-uri-class)

Command History

Release	Modification
12.3(4)T	This command was introduced.
15.1(2)T	This command was modified. The **ipv4:** *ipv4-address*, **ipv6:** *ipv6-address*, and **dns:** *dns-name*argumentswere included.

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.

You can configure ten instances of the **host** command by specifying IPv4 addresses, IPv6 addresses, or domain name service (DNS) names for each instance. You can configure the **host** command specifying the *hostname-pattern*argument only once.

Examples

The following example defines a voice class that matches on the host field in a SIP URI:

```
voice class uri r100 sip
 user-id abc123
 host server1
 host ipv4:10.0.0.0
 host ipv6:[2001:0DB8:0:1:FFFF:1234::5]
 host dns:example.sip.com
 phone context 408
```

Related Commands

Command	Description
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.
user-id	Matches a call based on the user-id field in the SIP URI.
voice class uri	Creates or modifies a voice class for matching dial peers to calls containing a SIP or TEL URI.
voice class uri sip preference	Sets a preference for selecting voice classes for a SIP URI.

host-registrar

To populate the sip-ua registrar domain name or IP address value in the host portion of the diversion header and to redirect the contact header of the 302 response, use the **host-registrar** command in SIP user-agent configuration mode. To remove the sip-ua registrar domain name or IP address in the host portion of the diversion and redirect contact headers, use the **no** form of this command.

host-registrar system
no host-registrar system

Syntax Description

system	Specifies that the sip-ua registrar domain name or IP address in the host portion of the diversion and redirect contact headers 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

This command's functionality is disabled. In the default condition, diversion headers are populated with the domain name or IP address of the gateway, and redirect contact headers are populated with the dial peer session target IP address or hostname.

Command Modes

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

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(22)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**.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models under SIP user-agent configuration mode.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models under voice class tenant configuration mode.

Usage Guidelines

You must first configure the **sip-ua** command to place the router in SIP user-agent configuration mode before you can use the **host-registrar** command.

By default, the Session Initiation Protocol (SIP) gateway and Cisco Unified Communications Manager Express (Cisco Unified Communications Manager Express) populate the host portion of the diversion header with the domain name or IP address of the gateway that generates the request or response. The SIP gateway and Cisco Unified Communications Manager Express also populate the host portion of the redirect contact header with the session target IP address or hostname of the matching dial peer.

When the **host-registrar** command and the **registrar** command are both configured in SIP user-agent configuration mode, the SIP gateway or Cisco Unified Communications Manager Express populate the host portion of both the diversion and redirect contact headers with the domain name or IP address that is configured by the **registrar** command.

The **host-registrar** command should be configured along with the **registrar** command in SIP user-agent configuration mode. If the **host-registrar** command is configured without the **registrar** command, the host portion of the diversion header is populated with the domain name or IP address of the gateway and the host portion of the redirect contact header is populated with the session target IP address or hostname of the matching dial peer.

Examples

The following example shows how to configure the **host-registrar** and **registrar** commands in SIP user-agent configuration mode to specify a URL scheme with SIP security:

```
sup-ua
 retry invite 3
 retry register 3
 timers register 150
 registrar dns:example.com scheme sips
 host-registrar
```

The following example shows how to configure the **host-registrar** and **registrar** commands in the voice class tenant configuration mode:

```
Router(config-class)# host-registrar system
```

Related Commands

Command	Description
registrar	Enables SIP gateways to register E.164-numbers on behalf of analog phone voice ports (FXS), IP phone virtual voice ports (EFXS), and SCCP phones with an external SIP proxy or SIP registrar.
sip-ua	Enables SIP user-agent configuration commands and configures the user agent.

http client cache memory

To set the memory file and pool limits for the HTTP client cache, use the **http client cache memory** command in global configuration mode. To reset to the default, use the **no** form of this command.

http client cache memory {**file** *file-size* | **pool** *pool-size*}
no http client cache memory {**file** | **pool**}

Syntax Description

file *file-size*	Maximum file size, in kilobytes, allowed for caching. Any file that is larger is not cached. Range is 1 to 10000. The default is 50.
pool *pool-size*	Maximum pool size, in kilobytes, allowed for caching. Range is 0 to 100000. The default is 10000. Setting the memory pool size to 0 disables HTTP caching.

Command Default

Memory file size: 50 KB Memory pool size: 10 MB

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.3(5)	The default for the *file-size* argument was increased from 2 to 50 KB and the default of the *pool-size* argument was increased from 100 to 10000 KB.
12.3(7)T	The default changes in Cisco IOS Release 12.3(5) were integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

A larger cache size may permit caching of frequently used files, decreasing the fetching time between the client and server and increasing performance. Allocation of memory to increase file size or pool size does not reduce the amount of memory available. Cache memory is used only when needed, and afterward returns to being memory shared with other resources.

The amount of memory required for an expected level of performance depends on a number of factors, including the type of voice gateway (for example, Cisco 2600 series or Cisco AS5400).

The recommended maximum file size is 10 MB; the recommended maximum pool size is 100 MB.

The gateway might accept invalid characters such as "#" or "!" when you input the value for this command. The gateway ignores any invalid characters.

Note For more information on HTTP caching, see the specification on which it is based: RFC 2616, *Hypertext Transfer Protocol HTTP/1.1*, June 1999, IETF.

Examples

The following example sets the HTTP client cache memory pool to 50,000 KB:

```
http client cache memory pool 50000
```

The following example sets the HTTP client cache memory file to 8000 KB:

```
http client cache memory file 8000
```

Related Commands

Command	Description
http client cache refresh	Configures the refresh time for the HTTP client cache.
http client connection idle timeout	Configures the HTTP client connection.
http client response timeout	Configures the HTTP client server response.
show http client cache	Displays current HTTP client cache information.

http client cache query

To enable caching of query data returned from the HTTP server, use the **http client cache query** command in global configuration mode. To disable caching of query data, use the **no** form of this command.

http client cache query
no http client cache query

Syntax Description

This command has no arguments or keywords.

Command Default

Query data is not cached.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **show http client cache** command to display cached query data. To protect caller privacy, values of the URL attributes are masked out with asterisks (*) in the **show http client cache** command output. If you use this command to enable caching of query data, use the **http client cache memory** command to increase the size of the HTTP client cache memory pool to accommodate the cached query data.

Examples

The following example enables caching of query data returned from the HTTP server:

```
Router# http client cache query
```

Related Commands

Command	Description
http client cache memory	Sets the memory file and pool limits for the HTTP client cache.
show http client cache	Displays information about the entries contained in the HTTP client cache.

http client cache refresh

To set the time limit for how long a cached entry is considered current by the HTTP client, use the **http client cache refresh** command in global configuration mode. To reset to the default, use the **no** form of this command.

http client cache refresh *seconds*
no http client cache refresh

Syntax Description

seconds	Lifetime of a cached HTTP entry, in seconds. Range is from 1 to 864000. The default is 86400 (24 hours).

Command Default

86,400 seconds (24 hours)

Command Modes

Global configuration (config)

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 implemented on the Cisco 3640 and Cisco 3660.

Usage Guidelines

This command must be used to set the refresh time only if the HTTP server does not provide the necessary information in the HTTP header to calculate this value.

The gateway might accept invalid characters such as "#" or "!" when you input the value for this command. The gateway ignores any invalid characters.

When a request is made to an expired cached entry (that is, an entry that is the same age as or older than the refresh time), the HTTP client sends the server a conditional request for an update.

An expired entry is not automatically updated unless a request from the user hits the same cached entry. Expired entries are not cleaned up until 70 percent or more of the cache pool memory is consumed; then all expired entries that lack a user reference are deleted from the cache table.

Note For more information on HTTP caching, see the specification on which it is based: RFC 2616, *Hypertext Transfer Protocol HTTP/1.1,* June 1999, IETF.

Examples

The following example shows the HTTP client cache refresh to be 10 seconds:

```
http client cache refresh 10
```

Related Commands

Command	Description
http client cache memory	Configures the memory limits for the HTTP client cache.

Command	Description
http client connection idle timeout	Configures the HTTP client connection.
http client response timeout	Configures the HTTP client server response.
show http client cache	Displays current HTTP client cache information.

http client connection idle timeout

To set the number of seconds for which the HTTP client waits before terminating an idle connection, use the **http client connection idle timeout** command in global configuration mode. To reset to the default, use the **no** form of this command.

http client connection idle timeout *seconds*
no http client connection idle timeout

Syntax Description

seconds	How long, in seconds, the HTTP client waits before terminating an idle connection. Range is from 1 to 60. The default is 2.

Command Default

2 seconds

Command Modes

Global configuration (config)

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 implemented on the Cisco 3640 and Cisco 3660.
Cisco IOS XE Cupertino 17.7.1	Introduced support for YANG models.

Usage Guidelines

The setting of this command determines when the HTTP client is disconnected from the HTTP server, which is necessary when the server does not disconnect the client after a desirable length of time.

The default value is recommended and should normally not be changed.

In the **show http client connection** command output, this parameter is displayed as *connection idle timeout.*

The gateway might accept invalid characters such as "#" or "!" when you input the value for this command. The gateway ignores any invalid characters.

Examples

The following example sets the timeout to 40 seconds:

```
http client connection idle timeout 40
```

Related Commands

Command	Description
http client cache memory	Configures the HTTP client cache.
http client response timeout	Configures the HTTP client server response.
show http client connection	Displays current HTTP client connection information.

http client connection persistent

To enable HTTP persistent connections so that multiple files can be loaded using the same connection, use the **http client connection persistent** command in global configuration mode. To disable HTTP persistent connections, use the **no** form of this command.

http client connection persistent
no http client connection persistent

Syntax Description

This command has no arguments or keywords.

Command Default

Persistent connections are enabled

Command Modes

Global configuration (config)

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 implemented on the Cisco 3640 and Cisco 3660.
Cisco IOS XE Cupertino 17.7.1	Introduced support for YANG models.

Usage Guidelines

The setting of this command determines whether the HTTP client requests a keepalive or closed connection from the server. The HTTP server is responsible for granting or denying the keepalive connection request from the client.

Enabling persistent connections is recommended.

In the **show http client connection**command output, activation of this command is displayed as *persistent connection.*

Examples

The following example shows the HTTP client connection persistent parameter to be enabled:

```
http client connection persistent
```

Related Commands

Command	Description
http client cache memory	Configures the HTTP client cache.
http client response timeout	Configures the HTTP client server response.
show http client connection	Displays current HTTP client connection information.

http client connection timeout

To set the number of seconds for which the HTTP client waits for a server to establish a connection before abandoning its connection attempt, use the **http client connection timeout** command in global configuration mode. To reset to the default, use the **no** form of this command.

http client connection timeout *seconds*
no http client connection timeout

Syntax Description

seconds	How long, in seconds, the HTTP client waits for a server to establish a connection before abandoning its connection attempt. Range is from 1 to 60. The default is 5.

Command Default

5 seconds

Command Modes

Global configuration (config)

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 implemented on the Cisco 3640 and Cisco 3660.
Cisco IOS XE Cupertino 17.7.1	Introduced support for YANG models.

Usage Guidelines

The setting of this command determines when the HTTP client abandons its attempt to connect to the server, which is necessary when a connection to the server cannot be established after a desirable length of time.

The default value is recommended and should normally not be changed.

In the **show http client connection** command output, activation of this command is displayed as *initial socket connection timeout.*

The gateway might accept invalid characters such as "#" or "!" when you input the value for this command. The gateway ignores any invalid characters.

Examples

The following example shows the HTTP client connection timeout parameter to be 20 seconds:

```
http client connection timeout 20
```

Related Commands

Command	Description
http client cache memory	Configures the HTTP client cache.
http client response timeout	Configures the HTTP client server response.
show http client connection	Displays current HTTP client connection information.

http client cookie

To enable the HTTP client to send and receive cookies, use the **http client cookie**command in global configuration mode. To disable cookie support, use the **no** form of this command.

http client cookie
no http client cookie

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration(config)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command enables RFC 2109-compliant support with the following exceptions:

- Cookies cannot be cached.
- Maximum number of cookies that are stored for a call is 10. If this limit is reached, any subsequent cookies are discarded when they are received.
- Cookies are only maintained for the duration of the call; when a call terminates, all associated cookies are discarded.
- Secure method is not supported.

Examples

The following example enables HTTP cookie support if it was previously disabled using the **no http client cookie** command:

```
Router(config)# http client cookie
```

Related Commands

Command	Description
debug http client cookie	Displays debugging traces related to HTTP cookies.
http client cache memory	Configures the memory limits for the HTTP client cache.
http client cache refresh	Configures the refresh time for the HTTP client cache.
show http client cookie	Displays cookies that are being stored by the HTTP client.

http client post-multipart

To configure the HTTP client to generate a filename string that is not enclosed in quotation marks, use the **http client post-multipart content-disposition filename no-quote** command in global configuration mode. To return to the default, use the **no** form of this command.

http client post-multipart content-disposition filename no-quote
no http client post-multipart content-disposition filename no-quote

Syntax Description

content-disposition filename no-quote	HTTP client generates a filename string that is not enclosed in quotation marks.

Command Default

Filename string is enclosed in quotation marks.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

In a multipart HTTP POST request, the HTTP client on the router generates the filename string enclosed in quotation marks (""). Although the Multipurpose Internet Mail Extension (MIME) standard recommends that quotation marks be used, some HTTP servers conform to RFC 2068, which does not include quotation marks. Some older Hypertext Preprocessor (PHP) files require that the filename string be embedded in quotation marks. Use the **http client post-multipart content-disposition filename no-quote** command to remove the quotation marks from the filename if you do not need them.

Examples

The following example configures the HTTP client to generate filenames that are not enclosed in quotation marks in a multipart POST request:

```
Router# http client post-multipart content-disposition filename no-quote
```

http client response timeout

To configure the number of seconds for which the HTTP client waits for a server response, use the **http client response timeout** command in global configuration mode. To reset to the default, use the **no** form of this command.

http client response timeout *seconds*
no http client response timeout

Syntax Description

seconds	How long, in seconds, the HTTP client waits for a response from the server after making a request. Range is from 1 to 300. The default is 10.

Command Default

10 seconds

Command Modes

Global configuration (config)

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 implemented on the Cisco 3640 and Cisco 3660.

Usage Guidelines

This command is used to adjust the time allowed for the HTTP client to wait for the server to respond to a request before declaring a timeout error. Under normal conditions, the default of 10 seconds is sufficient. If more or less server response time is desired, use this command. For example, if your server responds slowly to the HTTP client requests, you may want to set this timer to wait longer.

In the **show running-config**command output, the value is displayed only if it is set to other than the default.

The gateway might accept invalid characters such as "#" or "!" when you input the value for this command. The gateway ignores any invalid characters.

Examples

The following example shows the HTTP client response timeout to be 5 seconds:

```
http client response timeout 5
```

Related Commands

Command	Description
show http client cache	Displays the HTTP client cache.
show http client connection	Displays the HTTP client connection.

http client secure-ciphersuite

To set the secure encryption cipher suite for the HTTP client, use the **http client secure-ciphersuite** command in global configuration mode. To reset to the default, use the **no** form of this command. All ciphers are selected by default, use the **default** form of this command.

http client secure-ciphersuite [**3des_cbc_sha**] [**aes-128-cbc-sha**] [**des_cbc_sha**] [**dhe-rsa-aes-cbc-sha2**] [**ecdhe-ecdsa-aes-gcm-sha2**] [**ecdhe-rsa-aes-cbc-sha2**] [**ecdhe-rsa-aes-gcm-sha2**] [**null_md5**] [**rc4_128_md5**] [**rc4_128_sha**] [**rsa-aes-cbc-sha2**] [**tls13-aes128-gcm-sha256**] [**tls13-aes256-gcm-sha384**] [**tls13-chacha20-poly1305-sha256**]
no http client secure-ciphersuite
default http client secure-ciphersuite

Syntax Description

3des-cbc-sha	Encryption tls_rsa_with_3des_ede_cbc_sha (TLS1.0) ciphersuite. Supported in non-secure router operation mode.
aes-128-cbc-sha	Encryption tls_rsa_with_aes_128_cbc_sha (TLS1.2 and below) ciphersuite. Supported in non-secure router operation mode.
des-cbc-sha	Encryption tls_rsa_with_des_cbc_sha (TLS1.0) ciphersuite. Supported in non-secure router operation mode.
dhe-rsa-aes-cbc-sha2	Encryption tls_rsa_with_cbc_sha2 (TLS1.2) ciphersuite. Supported in secure and non-secure router operation mode. **Note** Starting from Cisco IOS XE 26.1.1 release, this cipher (dhe-rsa-aes-cbc-sha2) is not supported. While this cipher may remain configurable within the system settings, it is no longer negotiable and will not be used for secure connections.
ecdhe-ecdsa-aes-gcm-sha2	Encryption tls_rsa_with_ecdhe-ecdsa-aes-gcm-sha2 (TLS1.2) ciphersuite. Supported in secure and non-secure router operation mode.
ecdhe-rsa-aes-cbc-sha2	Encryption tls_rsa_with_aes-cbd-sha2 (TLS1.2) ciphersuite. Supported in secure and non-secure router operation mode.
ecdhe-rsa-aes-gcm-sha2	Encryption tls_rsa_with_aes-gcm-sha2 (TLS1.2) ciphersuite. Supported in secure and non-secure router operation mode.
null-md5	Encryption tls_rsa_with_null_md5 (TLS1.0) ciphersuite. Supported in non-secure router operation mode.
rc4-128-md5	Encryption tls_rsa_with_rc4_128_md5 (TLS1.0) ciphersuite. Supported in non-secure router operation mode.

rc4-128-sha	Encryption tls_rsa_with_rc4_128_sha (TLS1.0) ciphersuite. Supported in non-secure router operation mode.
rsa-aes-cbc-sha2	Encryption tls_rsa_with_aes_cbc_sha2 (TLS1.2) ciphersuite. Supported in secure and non-secure router operation mode.
tls13-aes128-gcm-sha256	Encryption tls13_aes128_gcm_sha256 (TLS1.3) ciphersuite. Supported in secure and non-secure router operation mode.
tls13-aes256-gcm-sha384	Encryption tls13_aes256_gcm_sha384 (TLS1.3) ciphersuite. Supported in secure and non-secure router operation mode.
tls13-chacha20-poly1305-sha256	Encryption tls13_chacha20_poly1305_sha256 (TLS1.3) ciphersuite. Supported in secure and non-secure router operation mode. **Note** Starting from Cisco IOS XE 26.1.1 release, this cipher (tls13-chacha20-poly1305-sha256) is not supported. While this cipher may remain configurable within the system settings, it is no longer negotiable and will not be used for secure connections.

Command Default

Supports all cipher suites.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 26.1.1	The command is modified to indicate that the following non-complaint ciphers are not supported: • CHACHA20_POLY1305_SHA256 • DHE_RSA_WITH_AES_256_CBC_SHA
Cisco IOS XE 17.18.2	This command is modified to display security warnings for usage of legacy TLS and associated weaker ciphers.
Cisco IOS XE 17.14.1a	This command was modified to support the following TLS version 1.3 ciphers— • tls13-aes128-gcm-sha256 • tls13-aes256-gcm-sha384 • tls13-chacha20-poly1305-sha256 Introduced support for the TLS version 1.3 ciphers Yang model.
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **http client secure-ciphersuite** command to configure one or more cipher suites, or sets of encryption and hash algorithms, on the HTTP client. You must include at least one of the keywords and can include more than one. Use the **show http client secure status** command to display the cipher suites configured.



Note By default, the **http client secure-ciphersuite** command allows all ciphers to be configured, but starting from Cisco IOS XE 17.15.1a release, there's a 255 characters limitation in the CLI. Not all ciphers can be configured within this limit, so we recommend excluding weaker ciphers (null-md5, rc4-128-md5, rc4-128-sha, and des-cbc-sha) while configuring 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.

Following are the weaker ciphers configuring which a warning message is displayed:

- 3des-cbc-sha
- aes-128-cbc-sha
- des-cbc-sha
- null-md5
- rc4-128-md5
- rc4-128-sha



Note Starting from Cisco IOS XE 26.1.1 release, support for the following non-compliant ciphers has been discontinued. While these ciphers may remain configurable within the system settings, they are no longer negotiable and will not be used for secure connections.

- CHACHA20_POLY1305_SHA256
- DHE_RSA_WITH_AES_256_CBC_SHA

Examples

The following example sets the HTTP client to use the 3des_cbc_sha and null_md5 cipher suites:

```
Device(config)# http client secure-ciphersuite 3des_cbc_sha null_md5
HTTP Client Secure Ciphersuite: 3des_cbc_sha null_md5
```

Examples

The following example shows how to configure HTTP client to use the TLS v1.3 cipher suites:

```
Device(config)# http client secure-ciphersuite  tls13-aes128-gcm-sha256
tls13-aes256-gcm-sha384 tls13-chacha20-poly1305-sha256
```

```
HTTP Client Secure Ciphersuite: tls13-aes128-gcm-sha256 tls13-aes256-gcm-sha384
tls13-chacha20-poly1305-sha256
```

Examples

The following example shows how to configure HTTP client in default mode to use all the supported cipher suites:

```
Device(config)# default http client secure-ciphersuite
No TLS ciphersuite selected, default to all
HTTP Client Secure Ciphersuite: aes-128-cbc-sha rsa-aes-cbc-sha2 dhe-rsa-aes-cbc-sha2
ecdhe-rsa-aes-gcm-sha2 ecdhe-rsa-aes-cbc-sha2
ecdhe-ecdsa-aes-gcm-sha2 tls13-aes128-gcm-sha256 tls13-aes256-gcm-sha384
tls13-chacha20-poly1305-sha256
```

The following example illustrates a security warning message display for the insecure ciphers configuration:

```
Device(config-class)#http client secure-ciphersuite 3des-cbc-sha
HTTP Client Secure Ciphersuite: 3des-cbc-sha
SECURITY WARNING - Module: HTTPCLIENT, Command: http client secure-ciphersuite 3des-cbc-sha,

Reason: Weak cipher(s) are present in the command, Remediation: Use stronger cipher(s) to
enhance security

Device(config)#do sh run | sec http client secure-ciphersuite
http client secure-ciphersuite 3des-cbc-sha
```

The following example illustrates a security warning message display for **no** form of the command:

```
Device(config-class)# no http client secure-ciphersuite
No TLS ciphersuite selected, default to all
HTTP Client Secure Ciphersuite: aes-128-cbc-sha rsa-aes-cbc-sha2 dhe-rsa-aes-cbc-sha2
ecdhe-rsa-aes-gcm-sha2 ecdhe-rsa-aes-cbc-sha2
ecdhe-ecdsa-aes-gcm-sha2 tls13-aes128-gcm-sha256 tls13-aes256-gcm-sha384
tls13-chacha20-poly1305-sha256
SECURITY WARNING - Module: HTTPCLIENT, Command: no http client secure-ciphersuite, Reason:
 Weak cipher(s) are present in the command,
Remediation: Use stronger cipher(s) to enhance security

Device(config)#
Device(config)# do sh run | sec http client secure-ciphersuite
Device(config)#
```

Related Commands

Command	Description
http client secure-trustpoint	Declares the trustpoint that the HTTP client should use for HTTPS sessions.
show http client secure status	Displays the trustpoint and cipher suites that are configured in the HTTP client.

http client secure-trustpoint

To declare the trustpoint that the HTTP client will use for HTTPS (HTTP over Secure Socket Layer (SSL)) sessions, use the **http client secure-trustpoint** command in global configuration mode. To delete all identity information and certificates associated with the trustpoint, use the **no** form of this command.

http client secure-trustpoint *name*
no http client secure-trustpoint *name*

Syntax Description

name	Creates a name for the secure certification authority (CA) trustpoint.

Command Default

The Public Key Infrastructure (PKI) trustpoint configured on the router, or the primary trustpoint if more than one trustpoint is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **show http client secure status** command to display the trustpoints and cipher suites configured for the client.

Examples

The following example sets the HTTP client's secure CA trustpoint to myca:

```
Router(config)# http client secure-trustpoint myca
```

Related Commands

Command	Description
http client secure-ciphersuite	Sets the secure encryption cipher suite for the HTTP client.
show http client secure status	Displays the trustpoint and cipher suites that are configured in the HTTP client.

hunt-scheme least-idle

To enable the least-idle search method for finding an available channel in a trunk group for outgoing calls, use the **hunt-scheme least-idle**command in trunk group configuration mode. To delete the hunt scheme from the trunk group profile, use the **no** form of the command.

hunt-scheme least-idle [**both** | **even** | **odd**]
no hunt-scheme

Syntax Description

both	(Optional) Searches both even- and odd-numbered channels.
even	Searches for an idle even-numbered channel with the shortest idle time. If no idle even-numbered channel is available, an odd-numbered channel with the longest idle time is sought.
odd	Searches for an idle odd-numbered channel with the shortest idle time. If no idle odd-numbered channel is available, an even-numbered channel with the longest i dle time is sought.

Command Default

Hunt scheme: least-used Channel number: **both**

Command Modes

Trunk group configuration (config-trunkgroup)

Command History

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

Usage Guidelines

Use the least-idle hunt scheme in situations where you want to reuse the most recently selected channel.

The least-idle hunt scheme looks for the channel that has just become available. The software looks at all the channels in the trunk group, regardless of member precedence, and selects the channel that has most recently come into the available queue.

If no channels are available at the time of the call request, the software returns a cause code determined by the application configured on the inbound dial peer.

If the **even** quantifier is set, the even-numbered channel with the shortest idle time is selected. If the **odd** quantifier is set, the odd-numbered channel with the shortest idle time is selected. If **both**is set, the most recently available channel, regardless of channel number, is selected.

Examples

The following example searches for an even-numbered idle channel having the shortest idle time within a trunk group:

```
Router(config)# trunk group northwestsales
Router(config-trunk-group)# hunt-scheme least-idle even
```

Related Commands

Command	Description
hunt-scheme longest-idle	Enables the longest-idle hunt scheme.

Command	Description
trunk group	Initiates a trunk group profile.

hunt-scheme least-used

To enable the least used search method for finding an available channel in a trunk group for outgoing calls, use the **hunt-scheme least-used**command in trunk group configuration mode. To delete the hunt scheme from the trunk group profile, use the **no** form of the command.

hunt-scheme least-used [**both** | **even** | **odd** [**up** | **down**]]
no hunt-scheme

Syntax Description

both	Searches both even- and odd-numbered channels.
even	Searches for an idle even-numbered channel. If no idle even-numbered channels are available, an odd-numbered channel is sought.
odd	Searches for an idle odd-numbered channel. If no idle odd-numbered channels are available, an even-numbered channel is sought.
up	Searches channels in ascending order based within a trunk group member. Used with **even**, **odd**, **both**.
down	Searches channels in descending order within a trunk group member. Used with **even**, **odd**, **both**.

Command Default

Hunt scheme: least-used Channel number: both Direction: up

Command Modes

Trunk group configuration (config-trunkgroup)

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

The least-used search method selects an idle channel from a trunk group member that has the highest number of available channels at the time that the hunt request is initiated. The high number of unused channels indicates that the trunk group member has not been very active in comparison with other trunk group members.

After selecting the trunk group member, the software searches the channels by direction and then by channel number:

- If **even up**is set, the software searches the trunk group members in ascending order of preference to determine which member has the highest number of available even-numbered channels. If no available even-numbered channel is found, the software searches the members again in ascending order for the member that has the highest number of available odd-numbered channels.
- If **odd up**is set, the software searches the trunk group members in ascending order of preference to determine which member has the highest number of available odd-numbered channels. If no available odd-numbered channel is found, the software searches the members again in ascending order for the member that has the highest number of available even-numbered channels.

- If **even down**is set, the software searches in descending order of preference to determine which member has the highest number of available even-numbered channels. If no available even-numbered channel is found, the software searches the members again in descending order for the member that has the highest number of available odd-numbered channels.
- If **odd down**is set, the software searches in descending order of preference to determine which member has the highest number of available odd-numbered channels. If no available odd-numbered channel is found, the software searches the members again in descending order for the member that has the highest number of available even-numbered channels.

If no channel is available in any of the trunk group members, the software returns the standard "no service" message.

Examples

The following example searches in ascending order for an even-numbered idle channel in a trunk group member having the highest number of available channels:

```
Router(config)# trunk group northwestsales
Router(config-trunk-group)# hunt-scheme least-used even up
```

Related Commands

Command	Description
trunk group	Initiates a trunk group profile.

hunt-scheme longest-idle

To enable the longest-idle search method for finding an available channel in a trunk group for outgoing calls, use the **hunt-scheme longest-idle**command in trunk group configuration mode. To delete the hunt scheme from the trunk group profile, use the **no** form of this command.

hunt-scheme longest-idle [**both** | **even** | **odd**]
no hunt-scheme

Syntax Description

both	Searches both even- and odd-numbered channels.
even	Searches for an idle even-numbered channel with the longest idle time. If no idle even-numbered channel is available, an odd-numbered channel with the shortest idle time is sought.
odd	Searches for an idle odd-numbered channel with the longest idle time. If no idle odd-numbered channel is available, an even-numbered channel with the shortest idle time is sought.

Command Default

Hunt scheme: least-used Channel number: both

Command Modes

Trunk group configuration (config-trunkgroup)

Command History

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

Usage Guidelines

The longest-idle hunt schemes attempts to route a call using a channel from the trunk group member that has been idle for the longest time.

If the **even** qualifier is set, the search looks for an even-numbered idle channel from the trunk group member that has been idle the longest. If no even-numbered idle channel is found, the search looks for an odd-numbered idle channel from the trunk group member that has the shortest idle time.

If the **odd** qualifier is set, the search begins looking for an odd-numbered channel from the trunk group member that has been idle the longest. If no odd-numbered idle channel is found, the search looks for an even-numbered idle channel from the trunk group member that has the shortest idle time.

If the **both** qualifier is set, the search looks for any (odd or even) idle channel in the trunk group member that has been idle the longest.

If no channel is available in any of the trunk group members, the software returns the standard "no service" message.

Examples

The following example searches in ascending order for an even-numbered idle channel in the trunk group member having the largest idle time:

```
Router(config)# trunk group northwestsales
Router(config-trunk-group)# hunt-scheme longest-idle even
```

Related Commands

Command	Description
hunt-scheme least-idle	Enables the least-idle hunt scheme.
trunk group	Initiates a trunk group profile.

hunt-scheme random

To enable the random search method for finding an available channel in a trunk group for outgoing calls, use the **hunt-scheme random**command in trunk group configuration mode. To delete the hunt scheme from the trunk group profile, use the **no** form of this command.

hunt-scheme random
no hunt-scheme

Syntax Description

This command has no arguments or keywords.

Command Default

Hunt scheme: least-used

Command Modes

Trunk group configuration (config-trunkgroup)

Command History

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

Usage Guidelines

The random search method selects trunk group member at random for an idle channel. After the trunk group member is selected, a channel is chosen at random. If that channel is not available, another trunk group member is chosen at random, and one of its channels is randomly chosen.

If no channel is available, the software returns the standard "no service" message.

Examples

The following example searches trunk group members in random order for an idle channel:

```
Router(config)# trunk group northwestsales
Router(config-trunk-group)# hunt-scheme random
```

Related Commands

Command	Description
trunk group	Initiates a trunk group profile.

hunt-scheme round-robin

To enable the round robin search method for finding an available channel in a trunk group for outgoing calls, use the **hunt-scheme** command in trunk group configuration mode. To delete the hunt scheme from the trunk group profile, use the **no** form of this command.

hunt-scheme round-robin [**both** | **even** | **odd** [**up** | **down**]]
no hunt-scheme

Syntax Description

both	Searches for an idle channel among both even- and odd-numbered channels at the same precedence.
even	Searches for an idle even-numbered channel. If no idle even-numbered channel is available, an odd-numbered channel is used.
odd	Searches for an idle odd-numbered channel. If no idle odd-numbered channel is available, an even-numbered channel is used.
up	Searches channels in ascending order based within a trunk group member. Used with **even**, **odd**, **both**.
down	Searches channels in descending order within a trunk group member. Used with **even**, **odd**, **both**.

Command Default

Hunt scheme: least-used Channel number: both

Command Modes

Trunk group configuration (config-trunkgroup)

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

The round-robin hunt scheme searches trunk group members one after the other for an idle channel. The history of the most recently used trunk group member is saved to identify the next trunk group member to use for a new idle channel request. This method tries to balance the load of channel use across trunk group members.

For example, suppose a trunk group has three trunk group members: A, B, and C. Trunk group member A has the highest preference, B has the next highest, and C has the lowest. The software starts the search with A:

- If A has an idle channel, that channel is used, and the next request for an idle channel starts with B.
- If A does not have an idle channel, the search moves to B:
- If B has an idle channel, that channel is used, and the next request for an idle channel starts with C.
- If B does not have an idle channel, the search moves to C:
- If C has an idle channel, that channel is used, and the next request for an idle channel starts with A.

- If C does not have an idle channel, the search returns to A.

If none of the trunk group members has an idle channel available for the current channel request, the software returns the standard "no service" message.

Compare this hunt scheme with **hunt-scheme sequential**, in which the next request for an idle channel always starts with the first trunk group member of the trunk group, regardless of where the last idle channel was found.

If the **even** qualifier is set, the search looks for an even-numbered idle channel starting with the trunk group member having the highest preference. If no even-numbered idle channel is found, the search looks for an even-numbered idle channel in the next trunk group member. If no even-numbered idle channel is found in any trunk group member, the search repeats the process for an odd-numbered channel.

If the **odd** qualifier is set, the search begins looking for an odd-numbered channel, and if none is found in any of the trunk group members, the search repeats the process for an even-numbered channel.

If the **both** qualifier is set, the search looks for any idle channel in the trunk group member.

Examples

The following example searches for an even-numbered idle channel starting with the trunk group member next in order after the previously used member:

```
Router(config)# trunk group northwestregion
Router(config-trunk-group)# hunt-scheme round-robin even
```

Related Commands

Command	Description
hunt-scheme sequential	Enables a "sequential idle channel" hunt scheme.
trunk group	Initiates a trunk group profile definition.

hunt-scheme sequential

To specify the sequential search method for finding an available channel in a trunk group for outgoing calls, use the **hunt-scheme sequential**command in trunk group configuration mode. To delete the hunt scheme from the trunk group profile, use the **no** form of this command.

hunt-scheme sequential [**both** | **even** | **odd** [**up** | **down**]]
no hunt-scheme

Syntax Description

both	Searches both even- and odd-numbered channels.
even	Searches for an idle even-numbered channel. If no idle even-numbered channel is available, an odd-numbered channel is sought.
odd	Searches for an idle odd-numbered channel. If no idle odd-numbered channel is available, an even-numbered channel is sought.
up	Searches channels in ascending order based within a trunk group member. Used with **even**, **odd**, **both**.
down	Searches channels in descending order within a trunk group member. Used with **even**, **odd**, **both**.

Command Default

Hunt scheme: least-used Channel number: both Direction: up

Command Modes

Trunk group configuration (config-trunkgroup)

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

The sequential hunt scheme selects an idle channel, starting with the trunk group member that has the highest preference within the trunk group. Regardless of where the last idle channel was found, an idle channel request starts searching with this highest-preference trunk group member.

For example, suppose a trunk group has three trunk group members: A, B, and C. Trunk group member A has the highest preference, B has the next highest, and C has the lowest. The software starts the search with trunk group A:

- If A has an idle channel, that channel is used, and the next request for an idle channel starts with A.
- If A does not have an idle channel, the search moves to B:
- If B has an idle channel, that channel is used, and the next request for an idle channel starts with A.
- If B does not have an idle channel, the search moves to C:
- If C has an idle channel, that channel is used, and the next request for an idle channel starts with A.
- If C does not have an idle channel, the software returns the standard "no service" message.

Compare this hunt scheme with **hunt-scheme round-robin**, where the next request for an idle channel starts with the next unused trunk group member of the trunk group.

If the **even** qualifier is set, the search looks for an even-numbered idle channel starting with the trunk group member having the highest preference. If no even-numbered idle channel is found, the search looks for an even-numbered idle channel in the next trunk group member. If no even-numbered idle channel is found, the search repeats the process for an odd-numbered idle channel.

If the **odd** qualifier is set, the search begins looking for an odd-numbered channel, starting with the trunk group member having the highest preference. If none is found in any of the trunk group members, the search repeats the process for an even-numbered channel.

If the **both** qualifier is set, the search looks for any idle channel in the trunk group member.

Use the sequential hunt scheme in situations that benefit from a predictable channel allocation. In addition, if one end of the routing path is defined with sequential even up and the other end with sequential odd up, glare conditions are avoided.

Examples

The following example searches in ascending order for an even-numbered idle channel starting with the trunk group member of highest precedence:

```
Router(config)# trunk group northwestsales
Router(config-trunk-group)# hunt-scheme sequential even up
```

Related Commands

Command	Description
hunt-scheme round-robin	Enables a round-robin hunt scheme.
trunk group	Initiates a trunk group profile definition.

huntstop

To disable all dial-peer hunting if a call fails when using hunt groups, use the **huntstop** command in dial-peer configuration mode. To reenable dial-peer hunting, use the **no** form of this command.

huntstop
no huntstop

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
12.0(5)T	This command was introduced on the 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.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

After you enter this command, no further hunting is allowed if a call fails on the specified dial peer.

Note This command can be used with all types of dial peers.

Examples

The following example shows how to disable dial-peer hunting on a specific dial peer:

```
dial peer voice 100 vofr
 huntstop
```

The following example shows how to reenable dial-peer hunting on a specific dial peer:

```
dial peer voice 100 vofr
 no huntstop
```

Related Commands

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



icpif through irq global-request

- icpif, on page 409
- id, on page 410
- idle-voltage, on page 411
- ignore, on page 412
- ignore (interface), on page 414
- image encoding, on page 416
- image resolution, on page 418
- impedance, on page 420
- inband-alerting, on page 422
- inbound ttl, on page 424
- incoming alerting, on page 425
- incoming called-number (call filter match list), on page 427
- incoming called-number (dial peer), on page 429
- incoming calling-number (call filter match list), on page 432
- incoming dialpeer, on page 434
- incoming media local ipv4, on page 435
- incoming media remote ipv4, on page 436
- incoming port, on page 437
- incoming secondary-called-number, on page 440
- incoming signaling local ipv4, on page 442
- incoming signaling remote ipv4, on page 443
- incoming uri, on page 444
- index (voice class), on page 447
- info-digits, on page 449
- information-type, on page 451
- inject guard-tone, on page 453
- inject pause, on page 454
- inject tone, on page 455
- input gain, on page 457
- intensity, on page 459
- interface (RLM server), on page 460
- interface Dchannel, on page 462
- interface event-log dump ftp, on page 463

- interface event-log error only, on page 466
- interface event-log max-buffer-size, on page 467
- interface max-server-records, on page 469
- interface stats, on page 470
- interop-handling permit request-uri userid none , on page 471
- ip address trusted, on page 472
- ip circuit, on page 474
- ip dhcp-client forcerenew, on page 476
- ip precedence (dial-peer), on page 477
- ip qos defending-priority, on page 478
- ip qos dscp, on page 480
- ip qos policy-locator, on page 483
- ip qos preemption-priority, on page 486
- ip rtcp report interval, on page 488
- ip rtcp sub-rtcp, on page 489
- ip udp checksum, on page 490
- ip vrf, on page 491
- ip vrf forwarding, on page 492
- irq global-request, on page 493

icpif

To specify the Calculated Planning Impairment Factor (ICPIF) for calls sent by a dial peer, use the **icpif** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

icpif *number*
no icpif

Syntax Description

number	Integer, expressed in equipment impairment factor units, that specifies the ICPIF value. Range is 0to 55. The default is 20.

Command Default

20

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced on the 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.
12.2(8)T	The number default value for this command was changed from 30 to 20.

Usage Guidelines

This command is applicable only to VoIP dial peers.

Use this command to specify the maximum acceptable impairment factor for the voice calls sent by the selected dial peer.

Examples

The following example disables the **icpif** command:

```
dial-peer voice 10 voip
 icpif 0
```

id

To configure the local identification (ID) for a neighboring border element (BE), use the **id** command in Annex G neighbor border element (BE) configuration mode. To remove the local ID, use the **no** form of this command.

id *neighbor-id*
no id *neighbor-id*

Syntax Description

neighbor -id	ID for a neighboring BE. The identification ID must be an International Alphabet 5 (IA5) string and cannot include spaces. This identifier is local and is not related to the border element ID.

Command Default

No default behavior or values

Command Modes

Annex G neighbor BE configuration (config-annexg-neigh)

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. This command is not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 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.

Examples

The following example configures the local ID for a neighboring BE. The identifier is 2333.

```
Router(config-annexg-neigh)# id 2333
```

The following example shows the the error response when an undefined neighbor ID is entered:

```
Router(config-annexg-neigh)#no id def

% Entry not valid, id not configured.
To deconfigure id under different neighbor you have to expilicitly go into that neighbor
and deconfigure the id.
```

Related Commands

Command	Description
advertise (annex G)	Controls the type of descriptors that the BE advertises to its neighbors.
port	Configures the port number of the neighbor that is used for exchanging Annex G messages.
query -interval	Configures the interval at which the local BE queries the neighboring BE.

idle-voltage

To specify the idle voltage on a Foreign Exchange Station (FXS) voice port, use the **idle-voltage** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

idle-voltage {**high** | **low**}
no idle-voltage

Syntax Description

high	The talk-battery (tip-to-ring) voltage is high (-48V) when the FXS port is idle.
low	The talk-battery (tip-to-ring) voltage is low (-24V) when the FXS port is idle.

Command Default

The idle voltage is -24V

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.0(4)T	This command was introduced on the Cisco MC3810.

Usage Guidelines

Some fax equipment and answering machines require a -48V idle voltage to be able to detect an off-hook condition in a parallel phone.

If the idle voltage setting is **high**, the talk battery reverts to -24V whenever the voice port is active (off hook).

Examples

The following example sets the idle voltage to -48V on voice port 1/1:

```
voice-port 1/1
 idle-voltage high
```

The following example restores the default idle voltage (-24V) on voice port 1/1:

```
voice-port 1/1
 no idle-voltage
```

Related Commands

Command	Description
show voice port	Displays voice port configuration information.

ignore

To configure the North American E&M or E&M MELCAS voice port to ignore specific receive bits, use the **ignore** command in voice-port configuration mode. To reset to the default, use the no form of this command.

ignore {**rx-a-bit** | **rx-b-bit** | **rx-c-bit** | **rx-d-bit**}
no ignore {**rx-a-bit** | **rx-b-bit** | **rx-c-bit** | **rx-d-bit**}

Syntax Description

rx -a-bit	Ignores the receive A bit.
rx -b-bit	Ignores the receive B bit.
rx -c-bit	Ignores the receive C bit.
rx -d-bit	Ignores the receive D bit.

Command Default

The default is mode-dependent:

- North American E&M:
  - The receive B, C, and D bits are ignored
  - The receive A bit is not ignored
- E&M MELCAS:
  - The receive A bit is ignored
  - The receive B, C, and D bits are not ignored

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the 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 **ignore** command applies to E&M digital voice ports associated with T1/E1 controllers. Repeat the command for each receive bit to be configured. Use this command with the **define** command.

Examples

To configure voice port 1/1 to ignore receive bits A, B, and C and to monitor receive bit D, enter the following commands:

```
voice-port 1/1
 ignore rx-a-bit
 ignore rx-b-bit
 ignore rx-c-bit
 no ignore rx-d-bit
```

To configure voice port 1/0/0 to ignore receive bits A, C, and D and to monitor receive bit B, enter the following commands:

```
voice-port 1/0/0
 ignore rx-a-bit
 ignore rx-c-bit
 ignore rx-d-bit
 no ignore rx-b-bit
```

Related Commands

Command	Description
condition	Manipulates the signaling bit pattern for all voice signaling types.
define	Defines the transmit and receive bits for North American E&M and E&M MELCAS voice signaling.
show voice port	Displays configuration information for voice ports.

ignore (interface)

To configure the serial interface to ignore the specified serial signals as the line up/down indicator, use the **ignore**command in interface configuration mode. To restore the default, use the **no** form of this command.

DCE Asynchronous Mode
ignore [**dtr** | **rts**]
no ignore [**dtr** | **rts**]

DCE Synchronous Mode
ignore [**dtr** | **local-loopback** | **rts**]
no ignore [**dtr** | **local-loopback** | **rts**]

DTE Asynchronous Mode
ignore [**cts** | **dsr**]
no ignore [**cts** | **dsr**]

DTE Synchronous Mode
ignore [**cts** | **dcd** | **dsr**]
no ignore [**cts** | **dcd** | **dsr**]

Syntax Description

dtr	Specifies that the DCE ignores the Data Terminal Ready (DTR) signal.
rts	Specifies that the DCE ignores the Request To Send (RTS) signal.
local-loopback	Specifies that the DCE ignores the local loopback signal.
cts	Specifies that the DTE ignores the Clear To Send (CTS) signal.
dsr	Specifies that the DTE ignores the Data Set Ready (DSR) signal.
dcd	Specifies that the DTE ignores the Data Carrier Detect (DCD) signal.

Command Default

The **no** form of this command is the default. The serial interface monitors the serial signal as the line up/down indicator.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745 routers.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.

Usage Guidelines

Serial Interfaces in DTE Mode

When the serial interface is operating in DTE mode, it monitors the DCD signal as the line up/down indicator. By default, the attached DCE device sends the DCD signal. When the DTE interface detects the DCD signal, it changes the state of the interface to up.

SDLC Multidrop Environments

In some configurations, such as a Synchronous Data Link Control (SDLC) multidrop environment, the DCE device sends the DSR signal instead of the DCD signal, which prevents the interface from coming up. Use this command to tell the interface to monitor the DSR signal instead of the DCD signal as the line up/down indicator.

Examples

The following example shows how to configure serial interface 0 to ignore the DCD signal as the line up/down indicator:

```
Router(config)# interface serial 0
Router(config-if)# ignore dcd
```

Related Commands

Command	Description
debug serial lead-transition	Activates the leads status transition debug capability for all capable ports.
show interfaces serial	Displays information about a serial interface.

image encoding

To specify an encoding method for fax images associated with a Multimedia Mail over IP (MMoIP) dial peer, use the **image encoding**command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

image encoding {**mh** | **mr** | **mmr** | **passthrough**}
no image encoding {**mh** | **mr** | **mmr** | **passthrough**}

Syntax Description

mh	Modified Huffman image encoding. This is the IETF standard.
mr	Modified Read image encoding.
mmr	Modified Modified Read image encoding.
passthrough	The image is not modified by an encoding method.

Command Default

Passthrough encoding

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.

Usage Guidelines

Use this command to specify an encoding method for e-mail fax TIFF images for a specific MMoIP dial peer. This command applies primarily to the on-ramp MMoIP dial peer. Although you can optionally create an off-ramp dial peer and configure a particular image encoding value for that off-ramp call leg, store-and-forward fax ignores the off-ramp MMoIP setting and sends the file using Modified Huffman encoding.

There are four available encoding methods:

- Modified Huffman (MH)--One-dimensional data compression scheme that compresses data in only one direction (horizontal). Modified Huffman compression does not allow the transmission of redundant data. This encoding method produces the largest image file size.
- Modified Read (MR)--Two-dimensional data compression scheme (used by fax devices) that handles the data compression of the vertical line and that concentrates on the space between lines and within given characters.

- Modified Modified Read (MMR)--Data compression scheme used by newer Group 3 fax devices. This encoding method produces the smallest possible image file size and is slightly more efficient than Modified Read.
- Passthrough--No encoding method is applied to the image--meaning that the image is encoded by whatever encoding method is used by the fax device.

The IETF standard for sending fax TIFF images is Modified Huffman encoding with fine or standard resolution. RFC 2301 requires that compliant receivers support TIFF images with MH encoding and fine or standard resolution. If a receiver supports features beyond this minimal requirement, you might want to configure the Cisco AS5300 universal access server to send enhanced-quality documents to that receiver.

The primary reason to use a different encoding scheme from MH is to save network bandwidth. MH ensures interoperability with all Internet fax devices, but it is the least efficient of the encoding schemes for sending fax TIFF images. For most images, MR is more efficient than MH, and MMR is more efficient than MR. If you know that the recipient is capable of receiving more efficient encodings than just MH, store-and-forward fax allows you to send the most efficient encoding that the recipient can process. For end-to-end closed networks, you can choose any encoding scheme because the off-ramp gateway can process MH, MR, and MMR.

Another factor to consider is the viewing software. Many viewing applications (for example, those that come with Windows 95 or Windows NT) are able to display MH, MR, and MMR. Therefore you should decide, on the basis of the viewing application and the available bandwidth, which encoding scheme is right for your network.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following example selects Modified Modified Read as the encoding method for fax TIFF images sent by MMoIP dial peer 10:

```
dial-peer voice 10 mmoip
 image encoding mmr
```

Related Commands

Command	Description
image resolution	Specifies a particular fax image resolution for a specific MMoIP dial peer.

image resolution

To specify a particular fax image resolution for a specific multimedia mail over IP (MMoIP) dial peer, use the **image resolution**command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

image resolution {**fine** | **standard** | **superfine** | **passthrough**}
no image resolution {**fine** | **standard** | **superfine** | **passthrough**}

Syntax Description

fine	Configures the fax TIFF image resolution to be 204-by-196 pixels per inch.
standard	Configures the fax TIFF image resolution to be 204-by-98 pixels per inch.
superfine	Configures the fax TIFF image resolution to be 204-by-391 pixels per inch.
passthrough	Indicates that the resolution of the fax TIFF image is not altered.

Command Default

passthrough

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750 access router.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600, Cisco 3725, and Cisco 3745.

Usage Guidelines

Use thiscommand to specify a resolution (in pixels per inch) for e-mail fax TIFF images sent by the specified MMoIP dial peer. This command applies primarily to the on-ramp MMoIP dial peer. Although you can optionally create an off-ramp dial peer and configure a particular image resolution value for that off-ramp call leg, store-and-forward fax ignores the off-ramp MMoIP setting and sends the file using fine resolution.

This command enables you to increase or decrease the resolution of a fax TIFF image, thereby changing not only the resolution but also the size of the fax TIFF file. The IETF standard for sending fax TIFF images is Modified Huffman encoding with fine or standard resolution. The primary reason to configure a different resolution is to save network bandwidth.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following example selects fine resolution (204-by-196 pixels per inch) for e-mail fax TIFF images associated with MMoIP dial peer 10:

```
dial-peer voice 10 mmoip
 image encoding mh
 image resolution fine
```

Related Commands

Command	Description
image encoding	Specifies an encoding method for fax images associated with an MMoIP dial peer.

impedance

To specify the terminating impedance of a voice-port interface, use the **impedance** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

impedance {**600c** | **600r** | **900c** | **900r** | **complex1** | **complex2** | **complex3** | **complex4** | **complex5** | **complex6**}
no impedance {**600c** | **600r** | **900c** | **900r** | **complex1** | **complex2** | **complex3** | **complex4** | **complex5** | **complex6**}

Syntax Description

600c	600 ohms + 2.15uF[1].
600r	Resistive 600-ohm termination.
900c	900 ohms + 2.15uF[2].
900r	Resistive 900-ohm termination.
complex1	220 ohms + (820 ohms || 115 nF)[3].
complex2	270 ohms + (750 ohms || 150 nF)[4].
complex3	370 ohms + (620 ohms || 310 nF)[5].
complex4	600r, line = 270 ohms + (750 ohms || 150 nF)[6].
complex5	320 + (1050 ohms || 230 nF), line = 12 Kft[7].
complex6	600r, line = 350 + (1000 ohms || 210 nF)[8].

1 The plus symbol (+) indicates serial. The double pipe (||) indicates parallel.
2 The plus symbol (+) indicates serial. The double pipe (||) indicates parallel.
3 The plus symbol (+) indicates serial. The double pipe (||) indicates parallel.
4 The plus symbol (+) indicates serial. The double pipe (||) indicates parallel.
5 The plus symbol (+) indicates serial. The double pipe (||) indicates parallel.
6 The plus symbol (+) indicates serial. The double pipe (||) indicates parallel.
7 The plus symbol (+) indicates serial. The double pipe (||) indicates parallel.
8 The plus symbol (+) indicates serial. The double pipe (||) indicates parallel.

Command Default

600r

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
11.3(1)T	This command was introduced on Cisco 3600 series.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T and support was added for the **complex3**, **complex4**, **complex5**, and **complex6** keywords on the Cisco 2600XM series, Cisco 2691, Cisco 2800 series, Cisco 3662 (telco models), Cisco 3700 series, and Cisco 3800 series.

Usage Guidelines

Use thiscommand to specify the terminating impedance of analog telephony interfaces. The impedance value must match the specifications from the telephony system to which it is connected. Different countries often have different standards for impedance. CO switches in the United States are predominantly 600r. PBXs in the United States are 600r or 900c.



Note The values in the syntax description represents the full set of impedances. Not all modules support the full set of impedance values shown here. To determine which impedance values are available on your modules, enter impedance ? in the command-line interface to see a list of the values you can configure.

If the impedance is set incorrectly (if there is an impedance mismatch), a significant amount of echo is generated (which could be masked if the **echo-cancel** command has been enabled). In addition, gains might not work correctly if there is an impedance mismatch.

Configuring the impedance on a voice port changes the impedance on both voice ports of a VPM card. This voice port must be shut down and then opened for the new value to take effect.

Examples

The following example configures an FXO voice port on the Cisco 3600 series router for an impedance of 600 ohms (real):

```
voice-port 1/0/0
impedance 600r
shutdown/no shutdown
```

The following example configures an E&M voice port on a Cisco 2800 for an impedance of complex3:

```
voice-port 1/1
impedance complex3
shutdown/no shutdown
```

Related Commands

Command	Description
voice-port	Enters voice-port configuration mode.
echo-cancel enable	Enables the cancellation of voice that is sent out the interface and received back on the same interface.

inband-alerting

To enable inband alerting, use the **inband-alerting**command in the SIP user agent configuration mode. To disable inband alerting, use the no form of this command.

inband-alerting
no inband-alerting

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.1(3)T	This command was limited to enabling and disabling inband alerting.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was introduced on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

If inband alerting is enabled, the originating gateway can open an early media path (upon receiving a 180 or 183 message with a SDP body). Inband alerting allows the terminating gateway or switch to feed tones or announcements before a call is connected. If inband alerting is disabled, local alerting is generated on the originating gateway.

To reset this command to the default value, use the **default** command.

Examples

The following example disables inband alerting:

```
Router(config)# sip-ua
Router(config-sip-ua)# no inband-alerting
```

Related Commands

Command	Description
default	Sets a command to its default.
exit	Exits the SIP user agent configuration mode.
max-forwards	Specifies the maximum number of hops for a request.
no	Negates a command or set its defaults.
retry	Configures the SIP signaling timers for retry attempts.

Command	Description
timers	Configures the SIP signaling timers.
transport	Enables SIP UA transport for TCP/UDP.

inbound ttl

To set the inbound time-to-live value, use the **inbound ttl**command in Annex G neighbor service configuration mode. To reset to the default, use the **no**form of this command.

inbound ttl *ttl-value*
no inbound ttl

Syntax Description

ttl -value	Inbound time-to-live (TTL) value, in seconds. Range is 0 to 2147483. When set to 0, the service relationship does not expire. The default is 120.

Command Default

120 seconds

Command Modes

Annex G neighbor service configuration (config-nxg-neigh-svc)

Command History

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

Usage Guidelines

Service relationships are defined to be unidirectional. Establishing a service relationship between border element A and border element B entitles A to send requests to B and expect responses. For B to send requests to A and expect responses, a second service relationship must be established. From A's perspective, the service relationship that B establishes with A is designated the "inbound" service relationship. Use thiscommand to indicate the duration of the relationship between border elements that participate in a service relationship.

Examples

The following example sets the inbound time-to-live value to 420 seconds (7 minutes):

```
Router(config-nxg-neigh-svc)#

inbound ttl 420
```

Related Commands

Command	Description
access-policy	Requires that a neighbor be explicitly configured.
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 the total time that a border element attempts delivery.
service-relationship	Establishes a service relationship between two border elements.
shutdown	Enables or disables the border element.

incoming alerting

To instruct an FXO ground-start voice port to modify its means of detecting an incoming call, use the **incoming alerting** command in voice-port configuration mode. To return to the default call detection method, use the **no** form of this command.

incoming alerting ring-only
no incoming alerting

Syntax Description

ring-only	Count incoming rings to detect incoming calls to the voice port that should be answered by the router.

Command Default

The FXO ground-start voice port detects an incoming call either by detecting the ring voltage applied to the line by the PSTN central office (CO) or by detecting that tip-ground is present for greater than about 7 seconds.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Cisco IOS Release	Modification
12.4(4)XC	This command was introduced.

Usage Guidelines

This command is valid only on FXO ports that have been configured with the **signal ground-start** command.

This command is necessary when two Cisco Unified CallManager Express (Cisco Unified CME) routers are used to provide redundant failover for incoming PSTN FXO ground-start lines. The voice ports for these trunk lines are wired in parallel between the two routers. The primary router is set to answer incoming calls after the first ring by default. The secondary router is set to answer incoming calls after 2 or 3 rings using the **ring number**command in voice-port configuration mode. As long as the primary router is operating, then the secondary router will not see enough rings to trigger it to answer the call. When the primary router is not operating, the secondary router has to be able to detect incoming ring signals so that it can answer calls. The default method of incoming call detection is not appropriate for voice ports on a secondary Cisco Unified CME router. The **incoming alerting ring-only** command must be used to modify the incoming call detection logic so that the voice port counts the number of incoming call rings instead of using the default call detection method.

Examples

The following example sets ring-only as the detection method for incoming calls on voice port 3/0/0, which is an FXO ground-start voice port.

```
Router(config)# voice-port 3/0/0
Router(config-voiceport)# signal ground-start
Router(config-voiceport)# incoming alerting ring-only
```

Related Commands

Command	Description
ring number	Specifies the maximum number of rings to be detected before an incoming call is answered by the router.

Command	Description
signal	Specifies the type of signaling for a voice port.

incoming called-number (call filter match list)

To configure debug filtering for incoming called numbers, use the **incoming called-number** command in call filter match list configuration mode. To disable, use the **no** form of this command.

incoming called-number {[**+**]} *string* {[**T**]}
no incoming called-number {[**+**]} *string* {[**T**]}

Syntax Description

+	(Optional) Character that indicates an E.164 standard number.
string	Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: • The asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit (this character is used as a wildcard). • Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage. • Plus sign (+), which indicates that the preceding digit occurred one or more times. **Note** The plus sign used as part of a digit string is different from the plus sign that can be used in front of a digit string to indicate that the string is an E.164 standard number. • Circumflex (^), which indicates a match to the beginning of the string. • Dollar sign ($), which matches the null string at the end of the input string. • Backslash symbol (\), which is followed by a single character, and matches that character. Can be used with a single character with no other significance (matching that character). • Question mark (?), which indicates that the preceding digit occurred zero or one time. • Brackets ([ ]), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters from 0 to 9 are allowed in the range. • Parentheses (( )), which indicate a pattern and are the same as the regular expression rule.
T	(Optional) Control character that indicates that the **destination-pattern** value is a variable-length dial string. Using this control character enables the router to wait until all digits are received before routing the call.

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 incoming called number 5550123:

```
call filter match-list 1 voice
 incoming called-number 5550123
```

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.
incoming calling-number	Configure debug filtering for incoming calling numbers.
incoming dialpeer	Configure debug filtering for the incoming dial peer.
incoming secondary-called-number	Configure debug filtering for incoming called numbers from the second stage of a two-stage scenario.
outgoing called-number	Configure debug filtering for outgoing called numbers.
outgoing calling-number	Configure debug filtering for outgoing calling numbers.
outgoing dialpeer	Configure debug filtering for the outgoing dial peer.
show call filter match-list	Display call filter match lists.

incoming called-number (dial peer)

To specify a digit string that can be matched by an incoming call to associate the call with a dial peer, use the **incoming called-number**command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

incoming called-number {[+]} *string* {[**T**]}
no incoming called-number {[+]} *string* {[**T**]}

Syntax Description

+	(Optional) Character that indicates an E.164 standard number.
string	Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: • The asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit (this character is used as a wildcard). • Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage. • Plus sign (+), which indicates that the preceding digit occurred one or more times. **Note** The plus sign used as part of a digit string is different from the plus sign that can be used in front of a digit string to indicate that the string is an E.164 standard number. • Circumflex (^), which indicates a match to the beginning of the string. • Dollar sign ($), which matches the null string at the end of the input string. • Backslash symbol (\), which is followed by a single character, and matches that character. Can be used with a single character with no other significance (matching that character). • Question mark (?), which indicates that the preceding digit occurred zero or one time. • Brackets ([ ]), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters from 0 to 9 are allowed in the range. • Parentheses (( )), which indicate a pattern and are the same as the regular expression rule.
T	(Optional) Control character that indicates that the **destination-pattern** value is a variable-length dial string. Using this control character enables the router to wait until all digits are received before routing the call.

Command Default

No incoming called number is defined

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3NA	This command was implemented on the Cisco AS5800.
12.0(4)XJ	This command was modified for store-and-forward fax.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)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.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

When a Cisco device is handling both modem and voice calls, it needs to be able to identify the service type of the call--meaning whether the incoming call to the server is a modem or a voice call. When the access server handles only modem calls, the service type identification is handled through modem pools. Modem pools associate calls with modem resources based on the dialed number identification service (DNIS). In a mixed environment, in which the server receives both modem and voice calls, you need to identify the service type of a call by using this command.

If you do not use this command, the server attempts to resolve whether an incoming call is a modem or voice call on the basis of the interface over which the call arrives. If the call comes in over an interface associated with a modem pool, the call is assumed to be a modem call; if a call comes in over a voice port associated with a dial peer, the call is assumed to be a voice call.

By default, there is no called number associated with the dial peer, which means that incoming calls are associated with dial peers by matching calling number with answer address, call number with destination pattern, or calling interface with configured interface.

Use this command to define the destination telephone number for a particular dial peer. For the on-ramp POTS dial peer, this telephone number is the DNIS number of the incoming fax call. For the off-ramp MMoIP dial peer, this telephone number is the telephone number of the destination fax machine.

This command applies to both VoIP and POTS dial peers and to on-ramp and off-ramp store-and-forward fax functions.

This command is also used to provide a matching VoIP dial peer on the basis of called number when fax or modem pass-through with named signaling events (NSEs) is defined globally on a terminating gateway.

You can ensure that all calls will match at least one dial peer by using the following commands:

```
Router(config)# dial-peer voice tag voip
Router(config-dial-peer)# incoming called-number.
```

Examples

The following example configures calls that come into the router with a called number of 555-0163 as being voice calls:

```
dial peer voice 10 pots
 incoming called-number 5550163
```

The following example sets the number (310) 555-0142 as the incoming called number for MMoIP dial peer 10:

```
dial-peer voice 10 mmoip
 incoming called-number 3105550142
```

incoming calling-number (call filter match list)

To configure debug filtering for incoming calling numbers, use the **incoming calling-number** command in call filter match list configuration mode. To disable, use the **no** form of this command.

incoming calling-number {[+]} *string* {[**T**]}
no incoming calling-number {[+]} *string* {[**T**]}

Syntax Description

+	(Optional) Character that indicates an E.164 standard number.
string	Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: • The asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit (this character is used as a wildcard). • Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage. • Plus sign (+), which indicates that the preceding digit occurred one or more times. **Note** The plus sign used as part of a digit string is different from the plus sign that can be used in front of a digit string to indicate that the string is an E.164 standard number. • Circumflex (^), which indicates a match to the beginning of the string. • Dollar sign ($), which matches the null string at the end of the input string. • Backslash symbol (\), which is followed by a single character, and matches that character. Can be used with a single character with no other significance (matching that character). • Question mark (?), which indicates that the preceding digit occurred zero or one time. • Brackets ([ ]), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters from 0 to 9 are allowed in the range. • Parentheses (( )), which indicate a pattern and are the same as the regular expression rule.
T	(Optional) Control character that indicates that the **destination-pattern** value is a variable-length dial string. Using this control character enables the router to wait until all digits are received before routing the call.

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 incoming calling number 5550125:

```
call filter match-list 1 voice
 incoming calling-number 5550125
```

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.
incoming called-number (call filter match list)	Configure debug filtering for incoming called numbers.
incoming dialpeer	Configure debug filtering for the incoming dial peer.
incoming secondary-called-number	Configure debug filtering for incoming called numbers from the second stage of a two-stage scenario.
outgoing called-number	Configure debug filtering for outgoing called numbers.
outgoing calling-number	Configure debug filtering for outgoing calling numbers.
outgoing dialpeer	Configure debug filtering for the outgoing dial peer.
show call filter match-list	Display call filter match lists.

incoming dialpeer

To configure debug filtering for the incoming dial peer, use the **incoming dialpeer** command in call filter match list configuration mode. To disable, use the **no** form of this command.

incoming dialpeer *tag*
no incoming dialpeer *tag*

Syntax Description

tag	Digits that define a specific dial peer. Valid entries are 1 to 2,147,483,647.

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 incoming dial peer 12:

```
call filter match-list 1 voice
 incoming dialpeer 12
```

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.
incoming called-number (call filter match list)	Configure debug filtering for incoming called numbers.
incoming calling-number	Configure debug filtering for incoming calling numbers.
incoming port	Configure debug filtering for the incoming port.
incoming secondary-called-number	Configure debug filtering for incoming called numbers from the second stage of a two-stage scenario.
outgoing called-number	Configure debug filtering for outgoing called numbers.
outgoing calling-number	Configure debug filtering for outgoing calling numbers.
outgoing dialpeer	Configure debug filtering for the outgoing dial peer.
outgoing port	Configure debug filtering for the outgoing port.
show call filter match-list	Display call filter match lists.

incoming media local ipv4

To configure debug filtering for the incoming media local IPv4 addresses for the voice gateway receiving the media stream, use the incoming media local ipv4 command in call filter match list configuration mode. To disable, use the **no** form of this command.

incoming media local ipv4 *ip_address*
no incoming media local ipv4 *ip_address*

Syntax Description

ip_address	IP address of the local voice gateway

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 incoming media on the local voice gateway, which has IP address 192.168.10.255:

```
call filter match-list 1 voice
 incoming media local ipv4 192.168.10.255
```

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.
incoming media remote ipv4	Configure debug filtering for the incoming media IPv4 addresses for calls to the IP side from the remote IP device.
incoming port	Configure debug filtering for the incoming port.
outgoing media local ipv4	Configure debug filtering for the outgoing media IPv4 addresses for calls to the IP side from the local voice gateway.
outgoing media remote ipv4	Configure debug filtering for the outgoing media IPv4 addresses for calls to the IP side from the remote IP device.
outgoing port	Configure debug filtering for the outgoing port.
show call filter match-list	Display call filter match lists.

incoming media remote ipv4

To configure debug filtering for the incoming media remote IPv4 addresses for the voice gateway receiving the media stream, use the incoming media remote ipv4 command in call filter match list configuration mode. To disable, use the **no** form of this command.

incoming media remote ipv4 *ip_address*
no incoming media remote ipv4 *ip_address*

Syntax Description

ip_address	IP address of the remote IP device

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 incoming media on the remote IP device, which has IP address 192.168.10.255:

```
call filter match-list 1 voice
 incoming media remote ipv4 192.168.10.255
```

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.
incoming media local ipv4	Configure debug filtering for the incoming media IPv4 addresses for calls to the IP side from the local voice gateway.
incoming port	Configure debug filtering for the incoming port.
outgoing media local ipv4	Configure debug filtering for the outgoing media IPv4 addresses for calls to the IP side from the local voice gateway
outgoing media remote ipv4	Configure debug filtering for the outgoing media IPv4 addresses for calls to the IP side from the remote IP device.
outgoing port	Configure debug filtering for the outgoing port.
show call filter match-list	Display call filter match lists.

incoming port

To configure debug filtering for the incoming port, use the **incoming port** command in call filter match list configuration mode. To disable, use the **no** form of this command.

Cisco 2600, Cisco 3600, and Cisco 3700 Series
incoming port {*slot-number subunit-number /port* | *slot/port/ds0-group- no***}**
incoming 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)
incoming port *slot-number subunit-number /port*
no incoming port *slot-number subunit-number /port*

Cisco AS5300
incoming port *controller-number* **D**
no incoming port *controller-number* **:D**

Cisco AS5400
incoming port *card port* **:D**
no incoming port *card port* **:D**

Cisco AS5800
incoming port {*shelf /slot /port* **:D** | *shelf /slot /parent /port* **:D**}
no incoming port {*shelf /slot /port* **:D** | *shelf /slot /parent /port* **:D**}

Cisco MC3810
incoming port *slot /port*
no incoming port *slot /port*

Syntax Description

slot-number	Number of the slot in the router in which the VIC is installed. Valid entries are 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 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.

card	Specifies the T1 or E1 card. Valid entries for the *card* argument are 1 to 7.

port	Specifies the voice port number. Valid entries are 0 to 7.
:D	Indicates the D channel associated with ISDN PRI.

shelf	Specifies the T1 or E1 controller on the T1 card, or the T1 controller on the T3 card. Valid entries for the *shelf* argument are 0 to 9999.
slot	Specifies the T1 or E1 controller on the T1 card, or the T1 controller on the T3 card. Valid entries for the *slot* argument are 0 to 11.
port	Specifies the voice port number. • T1 or E1 controller on the T1 card --Valid entries are 0 to 11. • T1 controller on the T3 card--Valid entries are 1 to 28.
:*port*	Specifies the value for the *parent* argument. The valid entry is 0.
:D	Indicates the D channel associated with ISDN PRI.

slot	The *slot* argument specifies the number slot in the router in which the VIC is installed. The only valid entry is 1.
port	The *port* variable specifies the voice port number. Valid interface ranges are as follows: • T1--ANSI T1.403 (1989), Telcordia TR-54016. • E1-- ITU G.703. • Analog Voice--Up to six ports (FXS, FXO, E & M). • Digital Voice-- Single T1/E1 with cross-connect drop and insert, CAS and CCS signaling, PRI QSIG. • Ethernet--Single 10BASE-T. • Serial--Two five-in-one synchronous serial (ANSI EIA/TA-530, EIA/TA-232, EIA/TA-449; ITU-T V.35, X.21, Bisync, Polled async).

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 incoming port 1/1/1 on a Cisco 3660 voice gateway:

```
call filter match-list 1 voice
 incoming port 1/1/1
```

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.
outgoing port	Configure debug filtering for the outgoing port.
show call filter match-list	Display call filter match lists.

incoming secondary-called-number

To configure debug filtering for incoming called numbers from the second stage of a two-stage scenario, use the incoming secondary-called-number command in call filter match list configuration mode. To disable, use the **no** form of this command.

incoming secondary-called-number *string*
no incoming secondary-called-number *string*

Syntax Description

string	Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 to 9, the letters A to D, and the following special characters: • The asterisk (*) and pound sign (#) that appear on standard touchtone dial pads. On the Cisco 3600 series routers only, these characters cannot be used as leading characters in a string (for example, *650). • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit (this character is used as a wildcard). On the Cisco 3600 series routers, the period cannot be used as a leading character in a string (for example, .650). • Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage. • Plus sign (+), which indicates that the preceding digit occurred one or more times. **Note** The plus sign used as part of a digit string is different from the plus sign that can be used in front of a digit string to indicate that the string is an E.164 standard number. • Circumflex (^), which indicates a match to the beginning of the string. • Dollar sign ($), which matches the null string at the end of the input string. • Backslash symbol (\), which is followed by a single character; matches that character. Can be used with a single character with no other significance (matching that character). • Question mark (?), which indicates that the preceding digit occurred zero or one time. • Brackets ([ ]), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters 0 to 9 are allowed in the range. • Parentheses ( ), which indicate a pattern and are the same as the regular expression rule.

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.

Usage Guidelines

Two-stage dialing occurs when the voice gateway presents a dial-tone before accepting digits. When a voice call comes into the Cisco IOS voice gateway, the voice port on the router is seized inbound by a PBX or CO switch. The voice gateway then presents a dial tone to the caller and collects digits until it can identify an outbound dial-peer. Dial-peer matching is done digit-by-digit whether the digits are dialed with irregular intervals by humans or in a regular fashion by telephony equipment sending the precollected digits. The voice gateway attempts to match a dial-peer after each digit is received.

Examples

The following example shows the voice call debug filter set to match incoming secondary called number 5550156:

```
call filter match-list 1 voice
 incoming secondary-called-number 5550156
```

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.
incoming called-number (call filter match list)	Configure debug filtering for incoming called numbers.
incoming calling-number	Configure debug filtering for incoming calling numbers.
incoming dialpeer	Configure debug filtering for the incoming dial peer.
outgoing called-number	Configure debug filtering for outgoing called numbers.
outgoing calling-number	Configure debug filtering for outgoing calling numbers.
outgoing dialpeer	Configure debug filtering for the outgoing dial peer.
show call filter match-list	Display call filter match lists.

incoming signaling local ipv4

To configure debug filtering for the incoming signaling local IPv4 addresses for the gatekeeper managing the signaling, use the incoming signaling local ipv4 command in call filter match list configuration mode. To disable, use the **no** form of this command.

incoming signaling local ipv4 *ip_address*
no incoming signaling local ipv4 *ip_address*

Syntax Description

ip_address	IP address of the local voice gateway

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 incoming signaling on the local voice gateway, which has IP address 192.168.10.255:

```
call filter match-list 1 voice
 incoming signaling local ipv4 192.168.10.255
```

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.
incoming port	Configure debug filtering for the incoming port.
incoming signaling remote ipv4	Configure debug filtering for the incoming signaling IPv4 addresses for calls to the IP side from the remote IP device.
outgoing port	Configure debug filtering for the outgoing port.
outgoing signaling local ipv4	Configure debug filtering for the outgoing signaling IPv4 addresses for calls to the IP side from the local voice gateway.
outgoing signaling remote ipv4	Configure debug filtering for the outgoing signaling IPv4 addresses for calls to the IP side from the remote IP device.
show call filter match-list	Display call filter match lists.

incoming signaling remote ipv4

To configure debug filtering for the incoming signaling remote IPv4 addresses for the gatekeeper managing the signaling, use the incoming signaling remote ipv4 command in call filter match list configuration mode. To disable, use the **no** form of this command.

incoming signaling remote ipv4 *ip_address*
no incoming signaling remote ipv4 *ip_address*

Syntax Description

ip_address	IP address of the remote IP device

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 incoming signaling on the remote IP device, which has IP address 192.168.10.255:

```
call filter match-list 1 voice
 incoming signaling remote ipv4 192.168.10.255
```

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.
incoming port	Configure debug filtering for the incoming port.
incoming signaling local ipv4	Configure debug filtering for the incoming signaling IPv4 addresses for calls to the IP side from the local voice gateway.
outgoing port	Configure debug filtering for the outgoing port.
outgoing signaling local ipv4	Configure debug filtering for the outgoing signaling IPv4 addresses for calls to the IP side from the local voice gateway.
outgoing signaling remote ipv4	Configure debug filtering for the outgoing signaling IPv4 addresses for calls to the IP side from the remote IP device.
show call filter match-list	Display call filter match lists.

incoming uri

To specify the voice class used to match a VoIP dial peer to the uniform resource identifier (URI) of an incoming call, use the **incoming uri** command in dial peer voice configuration mode. To remove the URI voice class from the dial peer, use the **no** form of this command.

H.323 Session Protocol
incoming uri {**called** | **calling**} *tag*
no incoming uri {**called** | **calling**}

Session Initiation Protocol (SIP) Session Protocol
incoming uri {**from** | **request** | **to** | **via**} *tag*
no incoming uri {**from** | **request** | **to** | **via**}

Syntax Description

called	Destination URI in the H.225 message of an H.323 call.
calling	Source URI in the H.225 message of an H.323 call.
tag	Alphanumeric label that uniquely identifies the voice class. This *tag* argument must be configured with the **voice class uri** command.
from	From header in an incoming SIP Invite message.
request	Request-URI in an incoming SIP Invite message.
to	To header in an incoming SIP Invite message.
via	Via header in an incoming SIP Invite message.

Command Default

No voice class is specified.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.3(4)T	This command was introduced.
15.1(2)T	This command was modified. The **via**keyword was included.

Usage Guidelines

- Before you use this command, configure the voice class by using the **voice class uri** command.
- The keywords depend on whether the dial peer is configured for SIP with the **session protocol sipv2** command. The **from**, **request**, **to**, and **via** keywords are available only for SIP dial peers. The **called** and **calling** keywords are available only for dial peers using H.323.
- This command applies rules for dial peer matching. The tables below show the rules and the order in which they are applied when the **incoming uri** command is used. The gateway compares the dial-peer command to the call parameter in its search to match an inbound call to a dial peer. All dial peers are

searched based on the first match criterion. Only if no match is found does the gateway move on to the next criterion.

Table 14: Dial-Peer Matching Rules for Inbound URI in SIP Calls

Match Order	Cisco IOS Command	Incoming Call Parameter
1	**incoming uri via**	Via URI
2	**incoming uri request**	Request-URI
3	**incoming uri to**	To URI
4	**incoming uri from**	From URI
5	**incoming called-numbe r**	Called number
6	**answer-address**	Calling number
7	**destination-pattern**	Calling number
8	**carrier-id source**	Carrier-ID associated with the call

Table 15: Dial-Peer Matching Rules for Inbound URI in H.323 Calls

Match Order	Cisco IOS Command	Incoming Call Parameter
1	**incoming uri called**	Destination URI in H.225 message
2	**incoming uri calling**	Source URI in H.225 message
3	**incoming called-number**	Called number
4	**answer-address**	Calling number
5	**destination-pattern**	Calling number
6	**carrier-id source**	Source carrier-ID associated with the call



Note Calls using an E.164 number, rather than a URI, use the dial-peer matching rules that existed prior to Cisco IOS Release 15.1(2)T. For information, see the*Dial Peer Configuration on Voice Gateway Routers* document, Cisco IOS Voice Configuration Library.

- You can use this command multiple times in the same dial peer with different keywords. For example, you can use **incoming uri called** and **incoming uri calling** in the same dial peer. The gateway then selects the dial peer based on the matching rules described in the tables above.

Examples

The following example matches on the destination telephone URI in incoming H.323 calls by using the ab100 voice class:

```
dial-peer voice 100 voip
 incoming uri called ab100
```

The following example matches on the incoming via URI for SIP calls by using the ab100 voice class:

```
dial-peer voice 100 voip
 session protocol sipv2
 incoming uri via ab100
```

Related Commands

Command	Description
answer-address	Specifies the calling number to match for a dial peer.
debug voice uri	Displays debugging messages related to URI voice classes.
destination-pattern	Specifies the telephone number to match for a dial peer.
dial-peer voice	Enters dial peer voice configuration mode to create or modify a dial peer.
incoming called-number	Specifies the incoming called number matched to a dial peer.
session protocol	Specifies the session protocol in the dial peer for calls between the local and remote router.
show dialplan incall uri	Displays which dial peer is matched for a specific URI in an incoming voice call.
voice class uri	Creates or modifies a voice class for matching dial peers to calls containing a SIP or TEL URI.

index (voice class)

To define one or more numbers for a voice class called number, or a range of numbers for a voice class called number pool, use the **index** command in voice class configuration mode. To remove the number or range of numbers, use the **no** form of this command.

index *number called-number*
no index *number called-number*

Syntax Description

number	Digits that identify this index. Range is 1 to 2147483647.
called-number	Specifies a called number, or a range of called numbers, in E.164 format.

Command Default

No index is configured.

Command Modes

Voice class configuration (config-voice-class)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command to define one or more numbers for a voice class called number, or a range of numbers for a voice class called number pool. You can define multiple indexes for any inbound or outbound voice class called number or voice class called number pool.

When defining a range of numbers for a called number pool:

- The range of numbers must be in E.164 format.
- The beginning number and ending number must be the same length.
- The last digit of each number must be 0 to 9.
- Leading '+' (if used) must be defined from in the range of called numbers.

Examples

The following example shows the configuration for indexes in voice class called number pool 100:

```
voice class called number pool 100
 index 1 4085550100 - 4085550111 (Range of called numbers are 4085550100 up to 4085550111)
 index 2 +3227045000
```

The following example shows configuration for indexes in voice class called number outbound 222:

```
voice class called number outbound 222
 index 1 4085550101
 index 2 4085550102
 index 2 4085550103
```

Related Commands

Command	Description
voice class called number	One or more called numbers configured for a voice class.

info-digits

To automatically add the two-digit prefix to the beginning of a dialed number string associated with the given POTS dial peer, use the **info-digits** command in dial-peer configuration mode. To specify that the two-digit prefix is "00" use the default info-digits form of this command. To prevent the router from automatically adding the two-digit prefix to the beginning of the POTS dial peer, use the no form of this command.

info-digits *prefix-number*
default info-digits
no info-digits

Syntax Description

prefix-number	Specifies the two-digit prefix that the router will automatically add to the dialed number string for the given POTS dial peer to identify the type of phone originating the call. This value cannot contain any more or less than two digits. Valid values include: • 00--Regular line • 01--4- and 8-party • 06--Hotel or Motel • 07--Coinless • 10--Test call • 27--Coin • 95--Test call **Note** Values 12 through 19 cannot be assigned because of conflicts with international 20 Automatic Identification of Outward listed directory number sent.

Command Default

The dialed number string is added with 00, indicating that the dialed number string originates from a regular line.

Command Modes

Dial-peer configuration (config-dialpeer)

Command History

Release	Modification
12.2(1)T	This command was introduced.
12.3(7)T	This command was modified. The default behavior was changed to add the dialed number string the with 00.

Usage Guidelines

This command adds a two-digit prefix to the dialed number string for the POTS dial peer that will enable you to dynamically redirect the outgoing call. The info-digits command is only available for POTS dial peers tied to a voice-port that corresponds to Feature Group-D (FGD) Exchange Access North American (EANA) signaling that provides specific call services such as emergency 911 calls in the United States. Configuring the **info-digit** command for other voice port types is not advised and may yield undesirable results.

Examples

The following example adds the information number string 91 to the beginning of the dialed number string for POTS dial peer 10:

```
dial-peer voice 10 pots
 info-digits 91
```

information-type

To select a specific information type for a Voice over IP (VoIP) or plain old telephone service (POTS) dial peer, use the **information-type**command in dial peer configuration mode. To remove the current information type setting, use the **no** form of this command. To return to the default configuration, use the **no** form of this command.

information-type {**fax** | **voice** | **video**}
no information-type

Syntax Description

fax	The information type is set to store-and-forward fax.
voice	The information type is set to voice. This is the default.
video	The information type is set to video.

Command Default

Voice

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(4)XJ	This command was modified for store-and-forward fax.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.4(11)T	The **video** keyword was added.

Usage Guidelines

The **fax** keyword applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following example shows the configuration for information type fax for VoIP dial peer 10:

```
dial-peer voice 10 voip
 information-type fax
```

The following example shows the configuration for information type video for POTS dial peer 22:

```
dial-peer voice 22 pots
 information-type video
```

Related Commands

Command	Description
isdn integrate calltype all	Enables integrated mode (for data, voice, and video) on ISDN BRI or PRI interfaces.

inject guard-tone

To play out a guard tone with the voice packet, use the **inject guard-tone** command in voice-class configuration mode. To remove the guard tone, use the **no** form of this command.

inject guard-tone *frequency amplitude* [**idle**]
no inject guard-tone *frequency amplitude* [**idle**]

Syntax Description

frequency	Frequency, in Hz, of the tone to be injected. Range is integers from 1 to 4000.
amplitude	Amplitude, in dBm, of the tone to be injected. Range is integers from -50 to -3.
idle	(Optional) Play out the inverse of the guard tone when there are no voice packets. Idle tone and guard tone are mutually exclusive.

Command Default

No guard tone is injected.

Command Modes

Voice-class configuration (config-voice-class)

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 **inject guard-tone** command has an effect 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 guard tone is played out with the voice packet to keep the radio channel up. Guard tones of 1950 Hz and 2175 Hz can be filtered out before the voice packet is sent from the digital signal processor (DSP) to the network using the **digital-filter** command.

Examples

The following example configures a guard tone of 1950 Hz and -10 dBm to be played out with voice packets:

```
voice class tone-signal tone1
 inject guard-tone 2175 -30
```

Related Commands

Command	Description
digital-filter	Specifies the digital filter to be used before the voice packet is sent from the DSP to the network.

inject pause

To specify a pause between injected tones, use the **inject pause** command in voice-class configuration mode. To remove the pause, use the **no** form of this command.

inject pause *index milliseconds*
no inject pause *index milliseconds*

Syntax Description

index	Order of pauses and tones. Range is integers from 1 to 10.
milliseconds	Duration, in milliseconds, of the pause between injected tones. Range is integers from 10 to 500.

Command Default

milliseconds : 0 milliseconds

Command Modes

Voice-class configuration (config-voice-class)

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 **inject pause** 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 specify the pause between injected tones specified with the **inject tone** command. Use the *index* argument of this command in conjunction with the *index* argument of the inject tone command to specify the order of the pauses and tones.

Examples

The following example configures a pause of 100 milliseconds after the injected tone:

```
voice class tone-signal 100
 inject tone 1 2000 0 200
 inject pause 2 100
```

Related Commands

Command	Description
inject tone	Specifies a wakeup or frequency selection tone to be played out before the voice packet.

inject tone

To specify a wakeup or frequency selection tone to be played out before the voice packet, use the **inject tone** command in voice-class configuration mode. To remove the tone, use the **no** form of this command.

inject tone *index frequency amplitude duration*
no inject tone *index frequency amplitude duration*

Syntax Description

index	Order of pauses and tones. Range is integers from 1 to 10.
frequency	Frequency, in Hz, of the tone to be injected. Range is integers from 1 to 4000.
amplitude	Amplitude, in dBm, of the tone to be injected. Range is integers from -30 to 3.
duration	Duration, in milliseconds, of the tone to be injected. Range is integers from 10 to 500.

Command Default

No tone is injected.

Command Modes

Voice-class configuration (config-voice-class)

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 **inject tone** 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 with the **inject pause** command to configure wakeup and frequency selection tones. Use the *index* argument of this command in conjunction with the *index* argument of the **inject pause** command to specify the order of the pauses and tones.

If you configure injected tones with this command, be sure to use the **timing delay-voice tdm** command to configure a delay before the voice packet is played out. The delay must be equal to the sum of the durations of the injected tones and pauses in the tone-signal voice class.

Examples

The following example configures a frequency selection tone to be played out before the voice packet:

```
voice class tone-signal 100
 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 pause	Specifies a pause between injected tones.

Command	Description
timing delay-voice tdm	Specifies the delay before a voice packet is played out.

input gain

To configure a specific input gain value or to enable automatic gain control, use the **input gain** command in voice-port configuration mode. To disable the selected value of the inserted gain, use the **no** form of this command.

input gain {*decibels* | **auto-control** [*auto-dBm*]}
no input gain {*decibels* | **auto-control** [*auto-dBm*]}

Syntax Description

decibels	The gain, in decibels (dB), to be inserted at the receiver side of the interface. The range is integers from –6 to 14. The default is 0 decibels.
auto-control	Enables automatic gain control.
auto-dBm	(Optional) The target speech level, in decibels per milliwatt (dBm), to be achieved at the receiver side of the interface. The range is integers from –30 to 3. The default is –9 dBm.

Command Default

Automatic gain control is disabled.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
11.3(1)T	This command was introduced.
11.3(1)MA	This command was implemented on the Cisco MC3810.
12.3(4)XD	This command was modified. The range of values for the *decibels* argument was increased.
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 modified. The **auto-control** keyword and *auto-dBm* argument were added.

Usage Guidelines

A system-wide loss plan must be implemented by using both the **input gain** and **output attenuation** commands. You must consider other equipment (including PBXs) in the system when you create a loss plan. The default value for the **input gain** command assumes that a standard transmission loss plan is in effect; that is, there is typically a minimum attenuation of –6 dB between phones, especially if echo cancellers are present. Connections are implemented to provide 0 dB of attenuation when the **input gain** and **output attenuation** commands are configured with the default value of 0 dB.

You cannot increase the gain of a signal to the public switched telephone network (PSTN), but you can decrease it. If the voice level is too high, you can decrease the volume by either decreasing the input gain or by increasing the output attenuation.

You can increase the gain of a signal coming into the device. If the voice level is too low, use the **input gain** command to increase the input gain.

Typical Land Mobile Radio (LMR) signaling systems send 0 dB out and expect –10 dB in. Setting the output attenuation to 10 dB is typical. Output attenuation should be adjusted to provide the voice level required by the radio to produce correct transmitter modulation.

The **auto-control** keyword and *auto-dBm* argument are available on an ear and mouth (E&M) voice port only if the signal type for that port is LMR. The **auto-control** keyword enables automatic gain control, which is performed by the digital signal processor (DSP). Automatic gain control adjusts speech to a comfortable volume when it becomes too loud or too soft. Radio network loss and other environmental factors could cause the speech level arriving at a device from an LMR system to be very low. You can use automatic gain control to ensure that the speech is played back at a more comfortable level. Because the gain is inserted digitally, the background noise can also be amplified. Automatic gain control is implemented as follows:

- Output level: –9 dB
- Gain range: –12 dB to 20 dB
- Attack time (low to high): 30 milliseconds
- Attack time (high to low): 8 seconds

Examples

The following example shows insertion of a 3-dB gain at the receiver side of the interface in the Cisco 3600 series router:

```
port 1/0/0
 input gain 3
```

Related Commands

Command	Description
output attenuation	Configures a specific output attenuation value or enables automatic gain control for a voice port.

intensity

To configure the intensity or depth of the noise reduction process, use the **intensity** command in media profile configuration mode. To disable the configuration, use the **no** form of this command.

intensity *level*
no intensity *level*

Syntax Description

level	Intensity level. The range is from 0 to 6.

Command Default

Intensity of noise reduction is not configured.

Command Modes

Media profile configuration (cfg-mediaprofile)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.2(3)T	This command was modified. Support for the Cisco Unified Border Element (Cisco UBE) was added.

Usage Guidelines

Use the **intensity** command to configure the intensity or depth of the noise reduction process. You must create a media profile for noise reduction and then configure the intensity level.

Examples

The following example shows how to create a media profile to configure noise reduction parameters:

```
Device> enable
Device# configure terminal
Device(config)# media profile nr 200
Device(cfg-mediaprofile)# intensity 2
Device(cfg-mediaprofile)# end
```

Related Commands

Command	Description
media profile nr	Creates a media profile to configure noise reduction parameters.
noisefloor	Configures the noise level, in dBm, above which NR will operate.

interface (RLM server)

To define the IP addresses of the Redundant Link Manager (RLM) server, use the **interface** command in interface configuration mode. To disable this function, use the **no** form of this command.

interface *name-tag*
no interface *name-tag*

Syntax Description

name -tag	Name to identify the server configuration so that multiple entries of server configuration can be entered.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(7)	This command was introduced.

Usage Guidelines

Each server can have multiple entries of IP addresses or aliases.

Examples

The following example configures the access-server interfaces for RLM servers "Loopback1" and "Loopback2":

```
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
 interface Loopback2
 ip address 10.1.1.2 255.255.255.255
rlm group 1
 server r1-server
 link address 10.1.4.1 source Loopback1 weight 4
 link address 10.1.4.2 source Loopback2 weight 3
```

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP addresses of the server.

Command	Description
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under the RLM group.
timer	Overwrites the default setting of timeout values.

interface Dchannel

To specify an ISDN D-channel interface and enter interface configuration mode, use the **interface Dchannel** command in global configuration mode.

interface Dchannel *interface-number*

Syntax Description

interface -number	Specifies the ISDN interface number. **Note** The *interface-number* argument depends on which controller the **rlm-group** subkeyword in the **pri-group timeslots**controller configuration command uses. For example, if the Redundant Link Manager (RLM) group is configured using the **controller e1 2/3** command, the D-channel interface command will be **interface Dchannel 2/3**.

Command Default

No D-channel interface is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)B	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

This command is used specifically in Voice over IP (VoIP) applications that require release of the ISDN PRI signaling time slot for RLM configurations.

Examples

The following example configures a D-channel interface for a Signaling System 7 (SS7)-enabled shared T1 link:

```
controller T1 1
 pri-group timeslots 1-3 nfas_d primary nfas_int 0 nfas_group 0 rlm-group 0
 channel group 23 timeslot 24
 end
! D-channel interface is created for configuration of ISDN parameters:
interface Dchannel1
 isdn T309 4000
 end
```

Related Commands

Command	Description
pri -group timeslots	Specifies an ISDN PRI group on a channelized T1 or E1 controller, and releases the ISDN PRI signaling time slot for environments that require that SS7-enabled VoIP applications share all slots in a PRI group.

interface event-log dump ftp

To enable the gateway to write the contents of the interface event log buffer to an external file, use the **interface event-log dump ftp** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

interface event-log dump ftp *server* [*:port*] */file* **username** *username* **password** { [*encryption-type*] } *password*
no interface event-log dump ftp *server* [*:port*] */file* **username** *username* **password** { [*encryption-type*] } *password*

Syntax Description

server	Name or IP address of FTP server where the file is located.
port	(Optional) Specific port number on server.
file	Name and path of file.
username	Username required to access file.
encryption-type	(Optional) The Cisco proprietary algorithm used to encrypt the password. Values are 0 or 7. To disable encryption enter 0; to enable encryption enter 7. If you specify 7, you must enter an encrypted password (a password already encrypted by a Cisco router).
password	Password required to access file.

Command Default

Interface event log buffer is not written to an external file.

Command Modes

Application configuration monitor

Command History

Release	Modification
Cisco IOS XE 26.2.1	This command is modified to display warning message for insecure protocol usage.
12.3(14)T	This command was introduced to replace the **call application interface event-log dump ftp** command.

Usage Guidelines

This command enables the gateway to automatically write the interface event log buffer to the named file when the buffer becomes full. The default buffer size is 4 KB. To modify the size of the buffer, use the **interface event-log max-buffer-size** command. To manually flush the event log buffer, use the **interface dump event-log** command in privileged EXEC mode.

Note Enabling the gateway to write event logs to FTP could adversely impact gateway memory resources in some scenarios, for example, when:

- The gateway is consuming high processor resources and FTP does not have enough processor resources to flush the logged buffers to the FTP server.

- The designated FTP server is not powerful enough to perform FTP transfers quickly
- Bandwidth on the link between the gateway and the FTP server is not large enough
- The gateway is receiving a high volume of short-duration calls or calls that are failing

You should enable FTP dumping only when necessary and not enable it in situations where it might adversely impact system performance.

Warning Starting with Cisco IOS XE 26.2.1, a warning message is displayed when insecure protocols such as HTTP, FTP, or TFTP are used, as they do not provide encryption or authentication. Use secure alternatives such as HTTPS, SFTP, or SCP instead.

Examples

The following example specifies that interface event log are written to an external file named int_elogs.log on a server named ftp-server:

```
application
monitor
interface event-log dump ftp ftp-server/elogs/int_elogs.log username myname password 0
mypass
```

Examples

The following example specifies that application event logs are written to an external file named int_elogs.log on a server with the IP address of 10.10.10.101:

```
application
monitor
interface event-log dump ftp 10.10.10.101/elogs/int_elogs.log username myname password 0
mypass
```

Examples

The following example shows the warning message being displayed for the usage of insecure FTP protocol:

```
application
monitor
interface event-log dump ftp 10.10.10.101/elogs/int_elogs.log username myname password 0
mypass
SECURITY WARNING - Module: APPLICATION_MONITOR,
Command: interface event-log dump ftp 10.10.10.101/elogs/int_elogs.log username myname
password 0 *,
Reason: No encryption is configured,
Description: Application monitor interface event log configured with plaintext password and
 insecure FTP - vulnerable to credential theft,
Remediation: Transition to secure file transfer methods using SCP, SFTP, HTTPS protocols
```

Related Commands

Command	Description
call application interface event-log dump ftp	Enable the gateway to write the contents of the interface event log buffer to an external file.

Command	Description
interface dump event-log	Flushes the event log buffer for application interfaces to an external file.
interface event-log	Enables event logging for external interfaces used by voice applications.
interface event-log max-buffer-size	Sets the maximum size of the event log buffer for each application interface.
interface max-server-records	Sets the maximum number of application interface records that are saved.
show call application interface	Displays event logs and statistics for application interfaces.

interface event-log error only

To restrict event logging to error events only for application interfaces, use the **interface event-log error-only** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

interface event-log error-only
no interface event-log error-only

Syntax Description

This command has no arguments or keywords.

Command Default

All events are logged.

Command Modes

Application configuration monitor

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application interface event-log error only** command.

Usage Guidelines

This command limits the severity level of the events that are logged; it does not enable logging. You must use this command with the **interface event-log** command, which enables event logging for all application interfaces.

Examples

The following example enables event logging for error events only:

```
application
monitor
interface event-log error-only
```

Related Commands

Command	Description
call application interface event-log error-only	Restricts event logging to error events only for application interfaces.
interface event-log	Enables event logging for external interfaces used by voice applications.
interface event-log max-buffer-size	Sets the maximum size of the event log buffer for each application interface.
interface max-server-records	Sets the maximum number of application interface records that are saved.
show call application interface	Displays event logs and statistics for application interfaces.

interface event-log max-buffer-size

To set the maximum size of the event log buffer for each application interface, use the **interface event-log max-buffer-size**command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

interface event-log max-buffer-size *kbytes*
no interface event-log max-buffer-size

Syntax Description

kbytes	Maximum buffer size, in kilobytes. Range is 1 to 10. Default is 4.

Command Default

4 KB

Command Modes

Application configuration monitor

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application interface event-log max-buffer-size** command.

Usage Guidelines

If the event log buffer reaches the limit set by this command, the gateway allocates a second buffer of equal size. The contents of both buffers is displayed when you use the **show call application interface** command. When the first event log buffer becomes full, the gateway automatically appends its contents to an external FTP location if the **interface event-log dump ftp** command is used.

A maximum of two buffers are allocated for an event log. If both buffers are filled, the first buffer is deleted and another buffer is allocated for new events (buffer wraps around). If the **interface event-log dump ftp** command is configured and the second buffer becomes full before the first buffer is dumped, event messages are dropped and are not recorded in the buffer.

Examples

The following example sets the maximum buffer size to 8 KB:

```
application
monitor
interface event-log max-buffer-size 8
```

Related Commands

Command	Description
call application interface event-log max-buffer-size	Sets the maximum size of the event log buffer for each application interface.
interface dump event-log	Flushes the event log buffer for application interfaces to an external file.
interface event-log dump ftp	Enables the gateway to write the contents of the interface event log buffer to an external file.

Command	Description
interface max-server-records	Sets the maximum number of application interface records that are saved.
show call application interface	Displays event logs and statistics for application interfaces.

interface max-server-records

To set the maximum number of application interface records that are saved, use the **interface max-server-records** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

interface max-server-records *number*
no interface max-server-records

Syntax Description

number	Maximum number of records to save. Range is 1 to 100. Default is 10.

Command Default

10

Command Modes

Application configuration monitor

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application interface max-server-records** command.

Usage Guidelines

Only the specified number of records from the most recently accessed servers are kept.

Examples

The following example sets the maximum saved records to 50:

```
application
monitor
interface max-server-records 50
```

Related Commands

Command	Description
call application interface max-server-records	Sets the maximum number of application interface records that are saved.
interface event-log	Enables event logging for external interfaces used by voice applications.
interface event-log max-buffer-size	Sets the maximum size of the event log buffer for each application interface.
show call application interface	Displays event logs and statistics for application interfaces.

interface stats

To enable statistics collection for application interfaces, use the **interface stats** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

interface stats
no interface stats

Syntax Description

This command has no arguments or keywords.

Command Default

Statistics collection is disabled.

Command Modes

Application configuration monitor

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application interface stats** command.

Usage Guidelines

To display the interface statistics enabled by this command, use the **show call application interface** command. To reset the interface counters to zero, use the **clear call application interface** command.

Examples

The following example enables statistics collection for application interfaces:

```
application
monitor
interface stats
```

Related Commands

Command	Description
call application interface stats	Enables statistics collection for application interfaces.
clear call application interface	Clears application interface statistics or event logs.
interface event-log	Enables event logging for external interfaces used by voice applications.
show call application interface	Displays event logs and statistics for application interfaces.
stats	Enables statistics collection for voice applications.

interop-handling permit request-uri userid none

To enable interop handling, execute **interop-handling** command in sip-ua mode. To disable, use **no** form of this command.

interop-handling permit request-uri userid none [system]

no interop-handling permit request-uri userid none

Syntax Description

request uri	request-uri related interoperability.
user-id	userid of the request-uri
none	no userid present in the request-uri.
system	Specifies that the interop-handling 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 UA configuration

voice class tenant configuration

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.

Usage Guidelines

Executing this command enables interop-handling.

Example

```
Device> enable
Device# configure terminal
Device(config)# sip-ua
Device(config-sip-ua)# interop-handling permit request-uri userid none
```

In voice class tenant mode:

```
Device> enable
Device# configure terminal
Device(config)# voice class tenant 1
Device(config-class)# interop-handling permit request-uri userid none
```

ip address trusted

To set up toll-fraud prevention support on a device, use the **ip address trusted** command in voice-service configuration mode. To disable the setup, use the **no** form of this command.

ip address trusted {**authenticate | call-block cause** *code* **| list**}
no ip address trusted {**authenticate | call-block cause | list**}

Syntax Description

authenticate	Enables IP address authentication on incoming H.323 or Session Initiation Protocol (SIP) trunk calls.
call-block cause *code*	Enables issuing a cause code when an incoming call is rejected on the basis of failed IP address authentication. By default, the device issues a call-reject (21) cause code.
list	Enables manual addition of IPv4 and IPv6 addresses to the trusted IP address list.

Command Default

Toll-fraud prevention support is enabled.

Command Modes

Voice service configuration (conf-voi-serv)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

Use the **ip address trusted** command to modify the default behavior of a device, which is to not trust a call setup from a VoIP source. With the introduction of this command, the device checks the source IP address of the call setup before routing the call.

A device rejects a call if the source IP address does not match an entry in the trusted IP address list that is a trusted VoIP source. To create a trusted IP address list, use the **ip address trusted list** command in voice service configuration mode, or use the IP addresses that have been configured using the **session target** command in dial peer configuration mode. You can issue a cause code when an incoming call is rejected on the basis of failed IP address authentication.

Examples

The following example displays how to enable IP address authentication on incoming H.323 or SIP trunk calls for toll-fraud prevention support.:

```
Device(config)# voice service voip
Device(conf-voi-serv)# ip address trusted authenticate
```

The following example displays the number of rejected calls:

```
Device# show call history voice last 1 | inc Disc

DisconnectCause=15
DisconnectText=call rejected (21)
DisconnectTime=343939840 ms
```

The following example displays the error message code and the error description:

```
Device# show call history voice last 1 | inc Error

InternalErrorCode=1.1.228.3.31.0
```

The following example displays the error description:

```
Device# show voice iec description 1.1.228.3.31.0

IEC Version: 1
Entity: 1 (Gateway)
Category: 228 (User is denied access to this service)
Subsystem: 3 (Application Framework Core)
Error: 31 (Toll fraud call rejected)
Diagnostic Code: 0
```

The following example shows how to issue a cause code when an incoming call is rejected on the basis of failed IP address authentication:

```
Device(config)# voice service voip
Device(conf-voi-serv)# ip address trusted call-block cause call-reject
```

The following example displays how to enable the addition of IP addresses to a trusted IP address list:

```
Device(config)# voice service voip
Device(conf-voi-serv)# ip address trusted list
```

Related Commands

Command	Description
debug voip ccapi inout	Traces the execution path through the call control API.
show call history voice	Displays the call history table for voice calls.
show ip address trusted list	Displays a list of valid IP addresses for incoming H.323 or SIP trunk calls.
voice iec syslog	Enables viewing of internal error codes as they are encountered in real time.

ip circuit

To create carrier IDs on an IP virtual trunk group, and create a maximum capacity for the IP group, use the **ip circuit** command. To remove a trunk group or maximum capacity, use the **no** form of the command.

ip circuit {**carrier-id** *carrier-name* [**reserved-calls** *reserved*] | **max-calls** *maximum-calls* | **default** {**only** | **name** *carrier-name*}}
no ip circuit {**carrier-id** *carrier-name* | **default** {**only** | **name** *carrier-name*}}

Syntax Description

carrier -id	Sets the IP circuit associated with a specific carrier.
carrier-name	Defines an IP circuit using the specified name as the circuit ID.
reserved-calls *reserved*	(Optional) Specifies the maximum number of calls for the circuit ID. Default value is 200.
max -calls *maximum-calls*	Sets the number of maximum aggregate H.323 IP circuit carrier call legs. Default value is 1000.
default only	Creates a single carrier using the default carrier name.
default name	Changes the default circuit name.
carrier-name	Default carrier name.

Command Default

If this command is not specified, no IP carriers and no maximum call leg values are defined.

Command Modes

H.323 voice-service configuration (conf-serv-h323)

Command History

Release	Modification
12.2(13)T3	This command was introduced.

Usage Guidelines

You can use the **ip circuit** command only when no calls are active. You can define multiple carrier IDs, and the ordering does not matter. IP circuit default only is mutually exclusive with defining carriers with circuit carrier id.

If **ip circuit default only** is specified, the maximum calls value is set to 1000.

Examples

The following example specifies a default circuit and maximum number of calls:

```
voice service voip
 no allow-connections any to pots
 no allow-connections pots to any
 allow-connections h323 to h323
 h323
  ip circuit max-calls 1000
  ip circuit default only
```

The following example specifies a default carrier and incoming source carrier:

```
voice service voip
 no allow-connections any to pots
 no allow-connections pots to any
 allow-connections h323 to h323
  h323
   ip circuit carrier-id AA reserved-calls 200

   ip circuit max-calls 1000
```

Related Commands

Command	Description
show crm	Displays some of the values set by this command.
voice-source group	Assigns a name to a set of source IP group characteristics, which are used to identify and translate an incoming VoIP call.

ip dhcp-client forcerenew

To enable forcerenew-message handling on the DHCP client when authentication is enabled, use the **ip dhcp-client forcerenew** command in global configuration mode. To disable the forced authentication, use the **no** form of this command.

ip dhcp-client forcerenew
no ip dhcp-client forcerenew

Syntax Description

This command has no arguments or keywords.

Command Default

Forcerenew messages are dropped.

Command Modes

Global configuration (config)

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

DHCP forcerenew handling is not enabled until the CLI is configured.

Examples

The following example shows how to enable DHCP forcerenew-message handling on the DHCP client:

```
Router(config)# ip dhcp-client forcerenew
```

Related Commands

Command	Description
ip dhcp client authentication key-chain	Specifies the key chain to be used in DHCP authentication requests.
ip dhcp client authentication mode	Specifies the type of authentication to be used in DHCP messages on the interface.
key chain	Identifies a group of authentication keys for routing protocols.

ip precedence (dial-peer)

To set IP precedence (priority) for packets sent by the dial peer, use the **ip precedence**command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

ip precedence *number*
no ip precedence *number*

Syntax Description

number	Integer specifying the IP precedence value. Range is 0to 7. A value of 0 means that no precedence (priority) has been set. The default is 0.

Command Default

The default value for this command is zero (0)

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)NA	This command was introduced on the following platforms: Cisco 2500 series, Cisco 3600 series, and Cisco AS5300.

Usage Guidelines

Use this command to configure the value set in the IP precedence field when voice data packets are sent over the IP network. This command should be used if the IP link utilization is high and the quality of service for voice packets needs to have a higher priority than other IP packets. This command should also be used if RSVP is not enabled and the user would like to give voice packets a higher priority than other IP data traffic.

This command applies to VoIP peers.

Examples

The following example sets the IP precedence to 5:

```
dial-peer voice 10 voip
 ip precedence 5
```

ip qos defending-priority

To configure the Resource Reservation Protocol (RSVP) defending priority value for determining quality of service (QoS), use the **ip qos defending-priority**command in dial peer configuration mode. To disable RSVP defending priority as a QoS factor, use the **no** form of this command.

ip qos defending-priority *defending-pri-value*
no ip qos defending-priority

Syntax Description

defending-pri-value	The RSVP defending priority value for determining QoS priorities. Valid entries are from 0 to 65535.

Command Default

The RSVP defending priority value is disabled and is not a factor in determining QoS.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

To configure the RSVP defending priority value, use the **ip qos defending-priority** command in dial peer configuration mode. The defending priority value is passed to the QoS module during reservation initiation. In a situation where there is not enough bandwidth available to support all calls, this setting enables an existing call to avoid being preempted by a new call unless the preemption priority of the new call is higher than the defending priority of the existing call.

Examples

The following example shows how to specify the RSVP defending priority value:

```
dial-peer voice 100 voip
 ip qos defending-priority 1111
```

Related Commands

Command	Description
acc-qos	Defines the acceptable QoS for inbound and outbound calls on a VoIP dial peer.
ip qos dscp	Configures the DSCP value for QoS.
ip qos policy-locator	Configures the application ID of RSVP.
ip qos preemption-priority	Configures the RSVP preemption priority.
ip rsvp policy preempt	Enables RSVP to take bandwidth from lower-priority reservations and give it to new, higher-priority reservations.
req-qos	Requests a particular QoS using RSVP to be used in reaching a specified dial peer in VoIP.

Command	Description
show-sip-ua calls	Displays the active UAC and UAS information for SIP calls on a Cisco IOS device.
voice-class sip rsvp-fail-policy	Configures RSVP failure policies.

ip qos dscp

To configure the differentiated services code point (DSCP) value for quality of service (QoS), use the **ip qos dscp** command in dial peer configuration mode. To disable DSCP as a QoS factor, set the DSCP value to **default** (which sets the value to the 000000 bit pattern). To set DSCP values to their default settings, use the **no**form of this command.

ip qos dscp {*dscp-valueset-afset-cs* | **default** | **ef**} {**signaling** | **media** [**rsvp-pass** | **rsvp-fail**] | **video** [**rsvp-none** | **rsvp-pass** | **rsvp-fail**]}
no ip qos dscp {*dscp-valueset-afset-cs* | **default** | **ef**} {**signaling** | **media** [**rsvp-pass** | **rsvp-fail**] | **video** [**rsvp-none** | **rsvp-pass** | **rsvp-fail**]}

Syntax Description

dscp-value	DSCP value. Valid entries are from 0 to 63.	
set-af	An assured forwarding bit pattern as the DSCP value:	
	• **af11** --bit pattern 001010 • **af12** --bit pattern 001100 • **af13** --bit pattern 001110 • **af21** --bit pattern 010010 • **af22** --bit pattern 010100 • **af23** --bit pattern 010110	• **af31** --bit pattern 011010 • **af32** --bit pattern 011100 • **af33** --bit pattern 011110 • **af41** --bit pattern 100010 • **af42** --bit pattern 100100 • **af43** --bit pattern 100110
set-cs	C lass-selector code point as the DSCP value:	
	• **cs1** --code point 1 (precedence 1) • **cs2** --code point 2 (precedence 2) • **cs3** --code point 3 (precedence 3) • **cs4** --code point 4 (precedence 4)	• **cs5** --code point 5 (precedence 5) • **cs6** --code point 6 (precedence 6) • **cs7** --code point 7 (precedence 7)
default	Specifies the default bit pattern 000000 as the DSCP value.	
ef	Specifies the expedited forwarding bit pattern 101110 as the DSCP value.	
signaling	Specifies that the DSCP value applies to signaling packets.	

media	Specifies that the DSCP value applies to media packets (voice and fax).
rsvp-pass	(Optional) Specifies that the DSCP value applies to packets with successful Resource Reservation Protocol (RSVP) reservations.
rsvp-fail	(Optional) Specifies that the DSCP value applies to packets (media or video) with failed RSVP reservations.
video	Specifies that the DSCP value applies to video packets. This option is valid only for Cisco Unified Communications Manager Express (Cisco Unified CME) on a Cisco Unified Border Element.
rsvp-none	(Optional) Specifies that the DSCP value applies to video packets with no RSVP reservations (valid only for video packets.)

Command Default

The DSCP default values are as follows:

- The default DSCP value for all signaling packets is **af31**.
- The default DSCP value for all media (voice and fax) packets is **ef**.
- The default DSCP value for all video packets is **af41**.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.2(2)T	This command was introduced. It replaced the **ip precedence** (dial peer) command
12.3(4)T	This command was modified. Keywords were added to support DSCP configuration for video streams.
12.4(22)T	This command was modified. Keywords were added to apply a DSCP value to media (voice and fax) packets with a specified (successful or failed) RSVP connection.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

To configure voice, signaling, and video traffic priorities, use the **ip qos dscp** command in dial peer configuration mode. The recommended value for media (voice and fax) packets is **ef;**for signaling packets, the recommended value is **af31**; and for video packets, it is **af41** (all defaults).

Additionally, before you can specify RSVP QoS, you must first use the **ip rsvp bandwidth** command to enable RSVP on the IP interface.

Examples

The following example shows how to set the DSCP value to a class-selector code point value of 1 and apply that DSCP setting to media (voice and fax) payload packets with no RSVP configured:

```
dial-peer voice 1 voip
 ip qos dscp cs1 media
```

The following example shows how to set the DSCP value to the expedited forwarding bit pattern and apply that DSCP setting to media (voice and fax) payload packets with a successful RSVP connection:

```
dial-peer voice 1 voip
ip qos dscp ef media rsvp-pass
```

The following example shows how to set the DSCP value to an assured forwarding code point value of 22 and apply that DSCP setting to all signaling packets:

```
dial-peer voice 1 voip
ip qos dscp af22 signaling
```

The following example shows how to set the DSCP value to an assured forwarding code point value of 43 and apply that DSCP setting to video packets with a successful RSVP connection:

```
dial-peer voice 100 voip
 ip qos dscp af43 video rsvp-pass
```

Related Commands

Command	Description
call rsvp-sync	Enables synchronization between RSVP signaling and the voice signaling protocol.
ip qos defending-priority	Configures the RSVP defending priority value.
ip qos policy-locator	Configures the application ID of RSVP.
ip qos preemption-priority	Configures the RSVP preemption priority value.
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp signalling dscp	Configures the DSCP settings to be used on RSVP messages on an interface.

ip qos policy-locator

To configure a quality of service (QoS) policy-locator (application ID) used to deploy Resource Reservation Protocol (RSVP) policies for specifying bandwidth reservations on Cisco IOS Session Initiation Protocol (SIP) devices, use the **ip qos policy-locator**command in dial peer configuration mode. To delete an application policy, use the **no** form of this command.

ip qos policy-locator {**video** | **voice**} [**app** *app-string*] [**guid** *guid-string*] [**sapp** *subapp-string*] [**ver** *version-string*]
no ip qos policy-locator {**video** | **voice**} [**app** *app-string*] [**guid** *guid-string*] [**sapp** *subapp-string*] [**ver** *version-string*]

Syntax Description

video	Specifies that the application ID applies to RSVP for video streams.
voice	Specifies that the application ID applies to RSVP for voice streams.
app	(Optional) Specifies an application.
app-string	Application ID. Consists of 1 to 31 alphanumeric characters.
guid	(Optional) Specifies a globally unique identifier (GUID).
guid-string	GUID. Consists of 1 to 31 alphanumeric characters.
sapp	(Optional) Specifies a subapplication.
sapp-string	Subapplication ID. Consists of 1 to 31 alphanumeric characters.
ver	(Optional) Specifies a version.
ver-string	Version ID. Consists of 1 to 15 alphanumeric characters.

Command Default

No policy is specified.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

In Cisco IOS software, the RSVP can process and accept requests by referring to multiple bandwidth pools. To enhance the granularity of local policy match criteria on Cisco IOS SIP devices, bandwidth pools can include policies based on application IDs. You can use these application-specific IDs to reserve bandwidth for each until specified bandwidth limits are reached.

To prevent one application type from consuming all bandwidth, RFC 2872 , Application and Sub Application Identity Policy Element for Use with RSVP , allows for the creation of separate bandwidth reservation pools. For example, an RSVP reservation pool can be created for voice traffic and another for video traffic so that reservations tagged with these application IDs can then be matched to the interface bandwidth pools using RSVP local policies. To limit bandwidth per application, though, you must configure a bandwidth limit for

each application and configure each with a reservation flag that associates the application with the appropriate bandwidth limit.

Before you can configure bandwidth limits for any application-specific policy, however, you must create application IDs. To create application IDs (application-specific reservation profiles), use the **ip qos policy-locator**command in dial peer configuration mode. After creating the necessary application IDs, you can then use the appropriate commands listed in the "Related Commands" section to configure bandwidth reservation. However, this feature is available only on supported devices that are running Cisco IOS Release 12.4(22)T or a later release.

For more information about configuring SIP RSVP features, see the "Configuring SIP RSVP Features" chapter in the Cisco IOS SIP Configuration Guide. For more general information about the application-specific policy feature, see the "Configuring RSVP" chapter in the RSVP section of the "Signaling" part in the Cisco IOS Quality of Service Solutions Configuration Guide.

Examples

The following example shows how to configure a policy for the application ID:

```
dial-peer voice 100 voip
 ip qos policy-locator voice app MyApp1 sapp MySubApp4
```

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 preemption-priority	Configures the RSVP preemption priority value.
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp policy default-reject	Configures blocking or passing of all messages that do not match any existing RSVP policies.
ip rsvp policy identity	Defines RSVP application IDs used to deploy RSVP policies.
ip rsvp policy preempt	Enables RSVP to take bandwidth from lower-priority reservations and give it to new, higher-priority reservations.
maximum (local policy)	Configures a local policy that limits RSVP resources.
preempt-priority	Configures RSVP QoS priorities to be inserted into PATH and RESV messages when they are not signaled from an upstream or downstream neighbor or local client application.
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.

Command	Description
voice-class sip rsvp-fail-policy	Specifies the action that takes place when RSVP negotiation fails.

ip qos preemption-priority

To configure the Resource Reservation Protocol (RSVP) preemption priority value for determining quality of service (QoS), use the **ip qos preemption-priority**command in dial peer configuration mode. To disable RSVP preemption priority as a QoS factor, use the **no** form of this command.

ip qos preemption-priority *preemption-pri-value*
no ip qos preemption-priority

Syntax Description

preemption-pri-value	The RSVP preemption priority value for determining QoS priorities. Valid entries are from 0 to 65535.

Command Default

The RSVP preemption priority value is disabled and is not a factor in determining QoS.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

To configure an RSVP preemption priority value, use the **ip qos preemption-priority**command in dial peer configuration mode. The preemption priority value is passed to the QoS module during reservation initiation. In a situation where there is not enough bandwidth available to support all calls, this setting enables a new call to preempt an existing call unless the defending priority of the existing call is higher than the preemption priority of the new call.

Examples

The following example shows how to specify the RSVP preemption priority value:

```
dial-peer voice 100 voip
 ip qos preemption-priority 1111
```

Related Commands

Command	Description
acc-qos	Defines the acceptable QoS for inbound and outbound calls on a VoIP dial peer.
ip qos dscp	Configures the DSCP value for QoS.
ip qos policy-locator	Configures the application ID of RSVP.
ip qos defending-priority	Configures the defending priority value of RSVP.
ip rsvp policy preempt	Enables RSVP to take bandwidth from lower-priority reservations and give it to new, higher-priority reservations.
req-qos	Requests a particular QoS using RSVP to be used in reaching a specified dial peer in VoIP.

Command	Description
show-sip-ua calls	Displays the active UAC and UAS information for SIP calls on a Cisco IOS device.
voice-class sip rsvp-fail-policy	Configures RSVP failure policies.

ip rtcp report interval

To configure the average reporting interval between subsequent Real-Time Control Protocol (RTCP) report transmissions, use the **ip rtcp report interval**command in global configuration mode. To reset to the default, use the **no** form of this command.

ip rtcp report interval *value*
no ip rtcp report interval

Syntax Description

value	Average interval for RTCP report transmissions, in ms. Range is 1 to 65535. Default is 5000.

Command Default

5000 ms

Command Modes

Global configuration (config)

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, Cisco AS5400, and Cisco AS5800.

Usage Guidelines

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.

For more information about RTCP, see RFC 1889, RTP: A Transport Protocol for Real-Time Applications.

Examples

The following example sets the reporting interval to 5000 ms:

```
Router(config)# ip rtcp report interval 5000
```

Related Commands

Command	Description
debug ccsip events	Displays all SIP SPI event tracing and traces the events posted to SIP SPI from all interfaces.
timer receive-rtcp	Enables the RTCP timer and configures a multiplication factor for the RTCP timer interval.

ip rtcp sub-rtcp

To specify sub-Real-Time Control Protocol (RTCP) message types, use the **ip rtcp sub-rtcp**command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip rtcp sub-rtcp *message-type number*
no ip rtcp sub-rtcp *message-type*

Syntax Description

message-type	Message type. For more information, use the question mark (?) online help function.
number	Message number. The range is from 209 to 255. The default is 209. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

RTP payload type is set to the default value 209.

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 specify sub-RTCP message typess:

```
Router# configure terminal
Router(config)# ip rtcp sub-rtcp message-type 210
```

Related Commands

Command	Description
ip rtcp report interval	Configures the average reporting interval between subsequent RTCP report transmissions.

ip udp checksum

To calculate the UDP checksum for voice packets sent by the dial peer, use the **ip udp checksum**command in dial-peer configuration mode. To disable this feature, use the **no** form of this command.

ip udp checksum
no ip udp checksum

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

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

Usage Guidelines

Use this command to enable UDP checksum calculation for each of the outbound voice packets. This command is disabled by default to speed up the transmission of the voice packets. If you suspect that the connection has a high error rate, you should enable this command to prevent corrupted voice packets forwarded to the digital signal processor (DSP).

This command applies to VoIP peers.

Note To maintain performance and scalability of the Cisco AS5850 when using images before Cisco IOS Release 12.3(4)T, enable no more than 10% of active calls with UDP checksum.

Examples

The following example calculates the UDP checksum for voice packets sent by dial peer 10:

```
dial-peer voice 10 voip
 ip udp checksum
```

Related Commands

Command	Description
loop -detect	Enables loop detection for T1 for Voice over ATM, Voice over Frame Relay, and Voice over HDLC.

ip vrf

To configure a VPN routing and forwarding (VRF) routing table, use the **ip vrf** command in global configuration mode or router configuration mode. To remove a VRF routing table, use the **no** form of this command.

ip vrf *vrf-name*
no ip vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

No VRFs are defined.

Command Modes

Global configuration

Router configuration

Command History

Release	Modification
Cisco IOS 12.0(5)T	This command was introduced.

Example

```
Device# enable
Device# configure terminal
Device(config)# ip vrf VRF1
```

ip vrf forwarding

To associate a VPN routing and forwarding (VRF) instance with an interface or subinterface, use the **ip vrf forwarding** command in global configuration mode or interface configuration mode. To disassociate a VRF, use the **no** form of this command.

ip vrf forwarding *vrf-name*
no ip vrf forwarding *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

The default for an interface is the global routing table.

Command Modes

Global configuration

Interface configuration

Command History

Release	Modification
Cisco IOS 12.0(5)T	This command was introduced.

Usage Guidelines

Use this command to associate an interface with a VRF. Executing this command on an interface removes the IP address. The IP address should be reconfigured.

Example

```
Device# enable
Device# configure terminal
Device(config)# interface GigabitEthernet0/1
Device(config-if)# ip vrf forwarding VRF1
```

irq global-request

To configure the gatekeeper to send information-request (IRQ) messages with the call-reference value (CRV) set to zero, use the **irq global-request** command in gatekeeper configuration mode. To disable the gatekeeper from sending IRQ messages, use the **no** form of this command.

irq global-request
no irq global-request

Syntax Description

This command has no arguments or keywords.

Command Default

The gatekeeper sends IRQ messages with the CRV set to zero.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3600 series.

Usage Guidelines

Use this command to disable the gatekeeper from sending an IRQ message with the CRV set to zero when the gatekeeper requests the status of all calls after its initialization. Disabling IRQ messages can eliminate unnecessary information request response (IRR) messages if the reconstruction of call structures can be postponed until the next IRR or if the call information is no longer required because calls are terminated before the periodic IRR message is sent. Disabling IRQ messages is advantageous if direct bandwidth control is not used in the gatekeeper.

Examples

The following example shows that IRQ messages are not sent from the gatekeeper:

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

Related Commands

Command	Description
timer irr period	Configures the IRR timer.



isdn bind-l3 through ixi transport http

- isdn bind-l3, on page 497
- isdn bind-l3 (Interface BRI), on page 498
- isdn bind-l3 ccm-manager, on page 500
- isdn bind-l3 iua-backhaul, on page 501
- isdn contiguous-bchan, on page 503
- isdn dpnss, on page 504
- isdn gateway-max-interworking, on page 506
- isdn global-disconnect, on page 507
- isdn gtd, on page 509
- isdn ie oli, on page 510
- isdn integrate calltype all, on page 511
- isdn network-failure-cause, on page 513
- isdn outgoing display-ie, on page 516
- isdn protocol-emulate, on page 518
- isdn rlm-group, on page 520
- isdn skipsend-idverify, on page 522
- isdn spoofing, on page 525
- isdn supp-service calldiversion, on page 526
- isdn supp-service mcid, on page 527
- isdn supp-service name calling, on page 528
- isdn supp-service tbct, on page 530
- isdn t-activate, on page 532
- isdn tei-negotiation (interface), on page 534
- iua, on page 537
- ivr asr-server, on page 539
- ivr autoload mode, on page 541
- ivr prompt memory, on page 543
- ivr autoload url, on page 545
- ivr contact-center, on page 547
- ivr language link, on page 550
- ivr prompt cutoff-threshold, on page 551
- ivr prompt streamed, on page 552
- ivr record cpu flash, on page 554

- ivr record jitter, on page 555
- ivr record memory session, on page 557
- ivr record memory system, on page 558
- ivr tts-server, on page 559
- ivr tts-voice-profile, on page 561
- ixi application cme, on page 562
- ixi application mib, on page 564
- ixi transport http, on page 566

isdn bind-l3

To configure an ISDN D-channel serial interface for signaling backhaul and associate it with a session set, use the **isdn bind-l3** command in interface configuration mode. To disable signaling backhaul on an ISDN D-channel serial interface, use the **no** form of this command.

isdn bind-l3 *set-name*
no isdn bind-l3

Syntax Description

set -name	Session set with which you are associating a D-channel interface.

Command Default

The ISDN D channel is not configured for signaling backhaul and is not associated with a session set

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco IAD2420 series. 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 following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Examples

The following example configures T1 signaling channel serial 0:23 for signaling backhaul and associate the D channel with the session set named "Set1":

```
Router(config)# interface s0:23
Router(config-if)# isdn bind-L3 set1
Router(config-if)# exit
```

The following example configures E1 signaling channel serial 0:15 for signaling backhaul and associates the D channel with the session set named "Set3":

```
Router(config)# interface s0:15
Router(config-if)# isdn bind-L3 set3
Router(config-if)# exit
```

isdn bind-l3 (Interface BRI)

To cause a Basic Rate Interface (BRI) port to bind ISDN Layer 3 protocol to either a regular gateway (GW) q931 stack or a Cisco CallManager Transmission Control Protocol (TCP) backhaul application and, if the latter, to operate in Media Gateway Control Protocol (MGCP) mode for backhaul, use the **isdn bind l3** command in interface configuration mode. To disable binding and reset the BRI to Session Application mode for backhaul, use the **no** form of this command.

isdn bind-l3 {**q931** | **ccm-manager service mgcp**}
no isdn bind-l3 {**q931** | **ccm-manager service mgcp**}

Syntax Description

q931	Regular GW q931 stack. This is the default.
ccm manager service mgcp	Cisco CallManager TCP backhaul application. You must also select MGCP service mode for backhaul.

Command Default

If the command is not used, the BRI port uses Session Application mode and binding is disabled. If the command is used with no keywords, q931 is assumed.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(15)ZJ	This command was integrated into Cisco IOS Release 12.2(15)ZJ on the Cisco 26xxXM, Cisco 2691, Cisco 3640, Cisco 3640A, Cisco 3660, and Cisco 37xx.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.

Usage Guidelines

This command reinitializes the BRI interface, including the two B-channel voice ports within the BRI, to support MGCP-backhaul call control. It also binds ISDN Q931 Layer 3 to the Cisco CallManager.

This command is visible when the BRI voice interface card (VIC) is present. The BRI VIC provides narrowband digital-voice connectivity in the voice network module on the Cisco 2600 series and Cisco 3600 series.

Before you use this command to enable binding, disable any active calls on the BRI interface by using the **shutdown (voice port)** command. You need not shut down the interface if no active calls are present or to configure L3 binding.

The combined ccm-manager service mgcp keywords are available only for supported BRI interfaces.

The **q931** keyword is available only for supported BRI interfaces. This keyword is not available for ISDN PRI interfaces.

Examples

The following example sets binding for BRI interface slot 1, port 0:

```
Router (config-if)# isdn bind-l3 q931
```

Related Commands

Command	Description
ccm-manager config	Supplies the local MGCP voice gateway with the IP address or logical name of the TFTP server from which to download XML configuration files and enable the download of the configuration.
debug ccm-manager	Displays debugging information about the Cisco CallManager.
show ccm-manager	Displays a list of Cisco CallManager servers, their current status, and their availability.
show ccm-manager fallback-mgcp	Displays the status of the MGCP gateway fallback feature.
show mgcp	Displays values for MGCP parameters.
shutdown (voice-port)	Takes voice ports for a specific VIC offline.

isdn bind-l3 ccm-manager

To bind Layer 3 of the ISDN PRI interface of the Media Gateway Control Protocol (MGCP) voice gateway to the Cisco CallManager for PRI Q.931 signaling backhaul support, use the **isdn bind-l3 ccm-manager**command in interface configuration mode. To disable this binding, use the no form of this command.

isdn bind-l3 ccm-manager
no isdn bind-l3 ccm-manager

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(2)XN	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco Voice Gateway 200 (Cisco VG200).
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2, and implemented on the Cisco IAD2420.

Usage Guidelines

This command enables ISDN PRI backhaul on an MGCP-enabled voice gateway.

Note While the ISDN PRI is configured as MGCP, the Layer 3 binding cannot revert to Q.931.

Examples

The following example binds PRI Layer 3 to the Cisco CallManager:

```
isdn bind-l3 ccm-manager
```

isdn bind-l3 iua-backhaul

To specify ISDN backhaul using Stream Control Transmission Protocol (SCTP) for an interface and to bind Layer 3 to DUA for DPNSS backhaul, use the **isdn bind-l3 iua-backhaul**command in interface configuration mode. To disable the backhaul capability, use the **no** form of this command.

isdn bind-l3 iua-backhaul [*application-server-name*]
no isdn bind-l3 iua-backhaul

Syntax Description

application-server-name	(Optional) Name of the application server (AS) to use for backhauling the interface.

Command Default

No default behavior or values

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.2(4)T	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 and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco IAD2420 series. The Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.2(15)ZJ	The capability to bind Layer 3 to DUA for DPNSS backhaul was added.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

DPNSS is not configured for backhaul and is not associated with a session set.

Examples

The following example configures DUA for DPNSS backhaul using an AS called "as1:"

```
Router(config-if)# isdn bind-l3 iua-backhaul as1
```

The following example configures T1 signaling channel serial 0:23 for signaling backhaul and associates the D channel with the session set named "set1":

```
Router(config)# interface s0:23
Router(config-if)# isdn bind-l3 set1
```

The following example configures E1 signaling channel serial 0:15 for signaling backhaul and associates the D channel with the session set named "set3":

```
Router(config)# interface s0:15
Router(config-if)# isdn bind-l3 set3
```

The following example shows IUA backhaul on the application server "as1":

```
interface Serial1/0:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 isdn bind-L3 iua-backhaul as1
```

Related Commands

Command	Description
as	Defines an AS for backhaul.
asp	Defines an ASP for backhaul.

isdn contiguous-bchan

To configure contiguous bearer channel handling on an E1 PRI interface, use the **isdn contiguous-bchan**command in interface configuration mode. To disable the contiguous B-channel handling, use the **no**form of this command.

isdn contiguous-bchan
no isdn contiguous-bchan

Syntax Description

This command has no arguments or keywords.

Command Default

Contiguous B channel handling is disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(7)XK	This command was introduced on the following platforms: Cisco 2500 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use this command to specify contiguous bearer channel handling so that B channels 1 to 30, skipping 16, map to time slots 1 to 31. This is available for E1 PRI interfaces only, when the **primary-qsig** or **primary-dms100** switch type option is configured by using the **isdn switch-type** command.

Examples

The following example shows the configuration on the E1 interface of a Cisco 3660 router E1 interface:

```
interface Serial5/0:15
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-qsig
 isdn overlap-receiving
 isdn incoming-voice voice
 isdn contiguous-bchan
```

Related Commands

Command	Description
isdn switch -type	Configures the **primary-qsig**or **primary-dms100**switch type for PRI support.

isdn dpnss

To indicate whether ISDN DPNSS is to act as PBX A or PBX B, or revert to Layer 2, use the **isdn dpnss** command in interface configuration mode. To reset to the default, use the **no** form of this command.

isdn dpnss [**pbxA** | **layer 2** [**retry max-count** *range*] [**timers** [**Tretry** *timer-value*] [**Ttest** *timer-value*]] [**test frame**]]
no isdn dpnss [**pbxA** | **layer 2** [**retry max-count** *range*] [**timers** [**Tretry** *timer-value*] [**Ttest** *timer-value*]] [**test frame**]]

Syntax Description

pbxA	(Optional) Enables DPNSS to act as PBX A.
layer 2	(Optional) Reverts to Layer 2.
retry max-count *range*	(Optional) Selects the number of times a frame will be retried if unacknowledged. The max-count value can be any number from 0 to 64. Default is 4
timers	(Optional) Selects DPNSS timers, which can be **Tretry** or **Ttest**.
Tretry *timer-value*	(Optional) Sets the Tretry timer in ms and seconds. Valid retry time values range from 5 ms to 10 seconds. Default is 500 ms.
Ttest *timer-value*	(Optional) Sets the Ttest timer in minutes. When the Ttest timer expires, frames are sent on all the DLCs. Valid test time values range from 1 to 60. Default is 5.
test frame	(Optional) Allows test frames to be sent periodically.

Command Default

PBX B

Command Modes

Interface configuration

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.

Usage Guidelines

Before you try to implement the **isdn dpnss layer2 test frame** command, make sure the ISDN switch type is configured (using the **isdn switch-type (PRI)** command) as PRIMARY-DPNSS. If you enter the **isdn dpnss layer2 test frame** command for a switch type that is not DPNSS, the router is forced into a reload.

Examples

The following example sets ISDN DPNSS to act as PBX A:

```
Router(config-if)# isdn dpnss pbxA
```

The following example sets the Tretry and Ttest timers:

```
Router(config-if)# isdn dpnss layer2 timers Tretry 500 Ttest 5
```

The following example selects the number of times a frame will be retried if unacknowledged:

```
Router(config-if)# isdn dpnss layer2 retry max-count 4
```

The following example allows test frames to be sent periodically:

```
Router(config-if)# isdn dpnss layer2 test frame
```

Related Commands

Command	Description
isdn bind-l3 iua-backhaul	Binds Layer 3 for DPNSS to DUA.
isdn switch-type (PRI)	Specifies the central office switch type on the ISDN interface.

isdn gateway-max-interworking

To prevent an H.323 gateway from checking for ISDN protocol compatibility and dropping information elements (IEs) in call messages, use the **isdn gateway-max-interworking**commandglobal configuration mode. To reset to the default, use the **no** form of this command.

isdn gateway-max-interworking
no isdn gateway-max-interworking

Syntax Description

This command has no arguments or keywords.

Command Default

The gateway checks for protocol compatibility.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)XI	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)XA	This command was implemented on the Cisco AS5400 and Cisco AS5350.
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

If this command is enabled on an originating H.323 gateway, the information elements (IEs) in call messages to the terminating gateway are not checked for end-to-end protocol compatibility. If this command is enabled on a terminating gateway, IEs are not checked in the reverse direction. If this command is not enabled, and the ISDN protocols are not compatible on the originating and terminating gateways, the gateway drops all IEs, including the progress indicator. The gateway then inserts a progress indicator of 1 into all Progress messages.

Examples

The following example enables maximum interworking:

```
isdn gateway-max-interworking
```

isdn global-disconnect

To allow passage of RELEASE and RELEASE COMPLETE messages over a voice network, use the **isdn global-disconnect** command in interface configuration mode. To disallow passage of RELEASE and RELEASE COMPLETE messages, use the **no** form of this command.

isdn global-disconnect
no isdn global-disconnect

Syntax Description

This command has no arguments or keywords.

Command Default

RELEASE and RELEASE COMPLETE messages terminate locally; they are not passed over the voice network.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.
12.4(15)XY	Support was added for SIP voice networks.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **isdn global-disconnect** command works with ISDN interfaces configured for Q-signaling (QSIG) tunneling using the bri-qsig or pri-qsig ISDN switch type (in either primary or secondary mode). This command must be enabled on both IP to time-division multiplexing (IP-TDM) gateways in a toll-bypass scenario where RELEASE and RELEASE COMPLETE messages need to be transparently passed end-to-end and in both directions.

Enabling the **isdn global-disconnect** command allows passage of the RELEASE and RELEASE COMPLETE messages (including information element (IE) content) end-to-end across a voice network between PBXs. Use the **no** form of this command to prevent RELEASE and RELEASE COMPLETE messages from being passed across the network.

Examples

The following example shows the configuration on the T1 PRI interface of a Cisco 3660 router:

```
interface Serial5/0:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-qsig
 isdn global-disconnect
 isdn overlap-receiving
 isdn incoming-voice voice
```

Related Commands

Command	Description
isdn protocol -emulate	Configures the interface to serve as either the QSIG secondary or the QSIG primary (must be the opposite setting as that set on the PBX.)
isdn switch-type (BRI)	Specifies the central office switch type on an ISDN BRI.
isdn switch-type (PRI)	Specifies the central office switch type or enables support of QSIG or Q.931 signaling on an ISDN PRI.
signaling forward	Specifies tunneling for QSIG, Q.931, H.225, and ISUP messages globally for a SIP or H.323 gateway.
signaling forward (dial-peer)	Specifies tunneling for QSIG, Q.931, H.225, and ISUP messages for a specific dial peer on a SIP or H.323 gateway.

isdn gtd

To enable generic transparency descriptor (GTD) mapping for information elements (IEs) sent in ISDN Setup messages, use the isdn gtd command in interface configuration mode. To disable GTD mapping, use the **no** form of this command.

isdn gtd
no isdn gtd

Syntax Description

This command has no arguments or keywords.

Command Default

GTD mapping is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the isdn gtd command to enable parameter mapping for the following ISDN IEs to corresponding GTD parameters:

- Originating Line Information--OLI
- Bearer Capability--USI and TMR
- Called Party Number--CPN
- Calling Party Number--CGN
- Redirecting Number--RGN, OCN and RNI

The following GTD parameters, which have no corresponding ISDN IEs, are also supported:

- Calling Party Category--CPC
- Forward Call Indicators--FCI
- Protocol Name--PRN

Examples

The following example enables GTD parameter mapping:

```
isdn gtd
```

isdn ie oli

To configure the value of the Originating Line Information (OLI) information element (IE) identifier when the gateway receives ISDN signaling from an MCI switch, use the isdn ie oli command in interface configuration mode. To disable the OLI IE identifier, use the **no** form of this command.

isdn ie oli *value*
no isdn ie oli *value*

Syntax Description

value	Hexadecimal number specifying the value that indicates OLI information from the MCI switch. Range is 00-7F.

Command Default

This command is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the isdn ie oli command to configure gateway support for the MCI ISDN variant by specifying the IE value that indicates OLI information.

Examples

The following example configures the OLI IE value to a hex value of 7A:

```
isdn ie oli 7A
```

Related Commands

Command	Description
isdn gtd	Enables GTD parameter mapping for ISDN IEs.

isdn integrate calltype all

To enable integrated mode on an ISDN PRI interface, use the **isdn integrate calltype all** command in interface configuration mode. To disable integrated mode, use the **no** form of this command.

isdn integrate calltype all
no isdn integrate calltype all

Syntax Description

This command has no arguments or keywords.

Command Default

Integrated mode is disabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

Configure this command from a PRI interface only. This command is not supported from a BRI interface.

Any incoming calls from an interface that has been configured for integrate calltype all is rejected with cause-code **invalid number 0x1C** if inbound dial-peer is not selected.

Examples

In the following example, the interface is shut down.

```
Router(config)# interface Serial4/1:15
Router(config-if)# shutdown
```

In the following example, integrated mode is enabled.

```
Router(config)# interface Serial4/1:15
Router(config-if)# isdn integrate calltype all
% This command line will enable the Serial Interface to "integrated service" mode.
% The "isdn incoming-voice voice" setting will be removed from the interface.
% Continue? [confirm]
```

When you confirm, the default incoming-voice configuration is removed from the interface, and the interface is now in integrated service mode. The interface does not reset back to voice mode if an incoming call is originated from the interface.

In the following example, the interface is set to active.

```
Router(config)# interface Serial4/1:15
Router(config-if)# no shutdown
```

Related Commands

Command	Description
dial-peer data	Creates a data dial peer and enters dial-peer configuration mode.

Command	Description
dial-peer search	Optimizes voice or data dial-peer searches.
isdn incoming-voice	Routes all incoming voice calls to the modem and determine how they will be treated.

isdn network-failure-cause

To specify the cause code to pass to the PBX when a call cannot be placed or completed because of internal network failures, use the **isdn network-failure-cause** command in interface configuration mode. To disable use of this cause code, use the **no** form of this command.

isdn network-failure-cause *value*
no isdn network-failure-cause *value*

Syntax Description

value	Number, from 1 to 127. See the table below for a list of failure cause code values.

Command Default

No default behavior or values

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.

Usage Guidelines

The PBX can reroute calls based on the cause code returned by the router.

This command allows the original cause code to be changed to the value specified if the original cause code is not one of the following:

- NORMAL_CLEARING (16)
- USER_BUSY (17)
- NO_USER_RESPONDING (18)
- NO_USER_ANSWER (19)
- NUMBER_CHANGED (22)
- INVALID_NUMBER_FORMAT (28)
- UNSPECIFIED_CAUSE (31)
- UNASSIGNED_NUMBER (1)

The table below describes the cause codes.

Table 16: ISDN Failure Cause Codes

Failure Cause Code	Meaning
1	Unallocated or unassigned number.
2	No route to specified transit network.
3	No route to destination.

Failure Cause Code	Meaning
6	Channel unacceptable.
7	Call awarded and being delivered in an established channel.
16	Normal call clearing.
17	User busy.
18	No user responding.
19	No answer from user (user alerted).
21	Call rejected.
22	Number changed.
26	Nonselected user clearing.
27	Destination out of order.
28	Invalid number format.
29	Facility rejected.
30	Response to status enquiry.
31	Normal, unspecified.
34	No circuit/channel available.
38	Network out of order.
41	Temporary failure.
42	Switch congestion.
43	Access information discarded.
44	Requested channel not available.
45	Preempted.
47	Resources unavailable, unspecified.
49	Quality of service unavailable.
50	Requested facility not subscribed.
52	Outgoing calls barred.
54	Incoming calls barred.
57	Bearer capability not authorized.
58	Bearer capability not available now.

Failure Cause Code	Meaning
63	Service or option not available, unspecified.
65	Bearer capability not implemented.
66	Channel type not implemented.
69	Requested facility not implemented.
70	Only restricted digital information bearer capability is available.
79	Service or option not implemented, unspecified.
81	Invalid call reference value.
82	Identified channel does not exist.
83	Suspended call exists, but this call ID does not.
84	Call ID in use.
85	No call suspended.
86	Call with requested call ID is cleared.
88	Incompatible destination.
91	Invalid transit network selection.
95	Invalid message, unspecified.
96	Mandatory information element missing.
97	Message type nonexistent or not implemented.
98	Message not compatible with call state or message type nonexistent or not implemented.
99	Information element nonexistent or not implemented.
100	Invalid information element contents.
101	Message not compatible with call state.
102	Recovery on timer expiry.
111	Protocol error, unspecified.
127	Interworking, unspecified.

Examples

The following example specifies a cause code to pass to a PBX when a call cannot be placed or completed of internal network failures:

```
isdn network-failure-cause 28
```

isdn outgoing display-ie

To enable the display information element to be sent in the outgoing ISDN message if provided by the upper layers, such as voice or modem. To disable the displaying of the information element in the outgoing ISDN message, use the no form of this command.

isdn outgoing display-ie
no isdn outgoing display-ie

Syntax Description

There are no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

The **isdn outoing display-ie** command is direction dependent, such as network-to-user or user-to-network. Not all ISDN switch types support the **isdn outgoing display-ie** command. The following shows the direction dependency by switch type, and this command can be used to override the dependency:

- ETSI (NTT, NET3,and NET5)--Only network-to-user
- DMS--Both ways
- TS014--Only network-to-user
- TS013--Only network-to-user
- 1TR6--Only network-to-user

Note The 4ESS, 5ESS, NI1, and NI2 switch types are not supported in any direction.

Note When the **isdn protocol-emulate** command is switched between network and user, this command reverts to its default value. The **isdn outoing display-ie** command must be enabled again.

Examples

The following is a running configuration, showing how the the **isdn outgoing display-ie** command is used on a specified serial interface:

```
Router# show running-config interface serial0:23
interface Serial0:23
 no ip address
```

```
dialer idle-timeout 999999
isdn switch-type primary-ni
isdn protocol-emulate network
isdn T310 30000
isdn outgoing display-ie
```

Related Commands

Command	Description
isdn protocol-emulate	Configures an ISDN data or voice port to emulate network or user functionality.

isdn protocol-emulate

To emulate the network side of an ISDN configuration for a PRI Net5 or PRI NTT switch type, use the **isdn protocol-emulate** command in interface configuration mode. To disable ISDN emulation, use the **no** form of this command.

isdn protocol-emulate {**network** | **user**}
no isdn protocol-emulate {**network** | **user**}

Syntax Description

network	Network side of an ISDN configuration.
user	User side of an ISDN configuration.

Command Default

No default behavior or values

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 concentrator.
12.1(1)T	This command was introduced in the T train.
12.2(2)XB	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 implemented on the Cisco IAD2420 series. This command is not supported on the access servers in this release.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.3	This command was enhanced to support network emulation capability on the Lucent 4ESS, 5ESS, and Nortel DMS-100 ISDN switch types. These switch types can be configured as a network, but no additional changes were made and not all network side features are supported.
12.3(8)T	Added support for the PRI NTT switch type.

Usage Guidelines

- The current ISDN signaling stack can emulate the ISDN network side, but it does not conform to the specifications of the various switch types in emulating the network side.
- This command enables the Cisco IOS software to replicate the public switched network interface to a Private Branch Exchange (PBX).
- To emulate NT (network) or TE (user) functionality, use this command to configure the layer 2 and layer 3 port protocol of a BRI voice port or a PRI interface.

- Use this command to configure the Cisco AS5300 PRI interface. To disable QSIG signaling, use the **no** form of this command; the layer 2 and layer 3 protocol emulation defaults to **user**.
- This feature is supported for the PRI Net5 and PRI NTT switch types.

Examples

The following example configures the interface (configured for Net5) to emulate the network-side ISDN:

```
Router(config)# int s0:15
Router(config-if)# isdn protocol-emulate network
```

The following example configures the layer 2 and layer 3 function of T1 PRI interface 23:

```
interface serial 1:23
 isdn protocol-emulate network
```

The following example configures the layer 2 and layer 3 function of a BRI voice port:

```
interface bri 1
 isdn protocol-emulate user
```

The following example configures the layer 2 and layer 3 function of an E1 PRI interface:

```
interface serial 4:23
 isdn protocol-emulate user
```

Related Commands

Command	Description
isdn bchan-number-order	Configures an ISDN PRI interface to make outgoing call selection in ascending, descending, or round-robin order.
isdn logging	Enables logging of ISDN syslog messages.
isdn switch-type (PRI)	Specifies the central office switch type on the ISDN PRI interface.
network-clock-priority	Specifies the clock-recovery priority for the BRI voice ports in a BVM.
pri-group nec-fusion	Configures the NEC PBX to support FCCS.
show cdapi	Displays the CDAPI.
show rawmsg	Displays the raw messages owned by the required component.

isdn rlm-group

To specify a Redundant Link Manager (RLM) group number for ISDN to use, enter the **isdn rlm-group**command in controller configuration mode. To disable this function, use the **no** form of this command.

isdn rlm-group *number*
no isdn rlm-group *number*

Syntax Description

number	Number of the RLM group. Valid range is from 0 to 5.

Command Default

No RLM group is specified and the ISDN D channel is reserved for signaling information.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.4(16)	This command was removed from the Cisco IOS software code on the Cisco 2800 series and Cisco 3800 series platforms.
12.4(15)T	This command was removed from the Cisco IOS software code on the Cisco 2800 series and Cisco 3800 series platforms.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

RLM delivers ISDN Q.921 frames over an IP network. RLM affects D-channel signaling only; it does not affect the B channels. The time slot assigned originally to the D channel is freed and used as a B channel because D signaling occurs over the IP network.

The **isdn rlm-group** command allows RLM to be used to transport the D-channel information (signaling) over Ethernet.

The **isdn rlm-group** is supported only on the Cisco AS5300, AS5350, AS5400, and AS5850 series access servers. This command is not supported on Cisco 1800 series, 2800 series, 3700 series, and 3800 series platforms.

Prior to Cisco IOS Releases 12.4(16) and 12.4(15)T, the **isdn rlm-group** command could be entered on Cisco 2800 series and 3800 series platforms even though it was not supported. In some conditions, this could cause the router to reload. Effective with Cisco IOS Releases 12.4(16) and 12.4(15)T, the **isdn rlm-group** command is no longer available on the Cisco 2800 series and 3800 series platforms.

Examples

The following example defines RLM group 1:

```
interface Serial0:23
 ip address 10.0.0.1 255.0.0.0
 encapsulation ppp
 dialer map ip 10.0.0.2 name map1 1111111
```

```
dialer load-threshold 1 either
dialer-group 1
isdn switch-type primary-ni
isdn incoming-voice modem
isdn rlm-group 1
ppp authentication chap
ppp multilink
hold-queue 75 in
```

Related Commands

Command	Description
clear interface virtual-access	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole RLM group.
retry keepalive	Allows consecutive keepalive failures a specified amount of time before the link is declared down.
server (RLM)	Defines the IP addresses of the server.
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under the RLM group.
timer	Overwrites the default setting of timeout values.

isdn skipsend-idverify

To stop the user side of a BRI interface from sending ID verify information, use the **isdn skipsend-idverify** command in interface configuration mode. To restore the user-side notification, use the **no** form of this command.

isdn skipsend-idverify
no isdn skipsend-idverify

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the user side sends the ID verify information. The **no** form of this command is in effect by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(3)XI	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

For user-side BRI interfaces, you can send ID verify messages to confirm the status of a particular terminal endpoint identifier (TEI) when there is doubt about whether the TEI is in use (for example, after a Layer 1/Layer 2 flap). ID is the TEI value.

For network-side BRI interfaces, the command should always be set. In some cases, the command will automatically be configured after the BRI network-side protocol emulation is set. If not, you can manually configure the command on the network-side BRI interface. After the command has been configured either automatically or manually, it cannot be further changed. A network-side BRI interface should always be set so that it does not send ID verify information.

Examples

The following example shows user-side output, with the default in effect, so the ID verify is sent:

```
Router# show isdn status br0/0
Global ISDN Switchtype = basic-net3
ISDN BRI0/0 interface
        dsl 0, interface ISDN Switchtype = basic-net3
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 95, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 0 CCBs = 0
    The Free Channel Mask:  0x80000003
    Total Allocated ISDN CCBs = 0
```

The following sample output shows network-side output, with the default in effect:

```
Ovld02#show isdn status
Global ISDN Switchtype = basic-net3
```

```
ISDN BRI0/1/0:0 interface
        dsl 0, interface ISDN Switchtype = basic-qsig
         **** User side configuration ****
    Layer 1 Status:
        DEACTIVATED
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = TEI_ASSIGNED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 0 CCBs = 0
    The Free Channel Mask:  0x80000003
ISDN BRI0/1/1:0 interface
        dsl 1, interface ISDN Switchtype = basic-net3
    Layer 1 Status:
        SHUTDOWN
    Layer 2 Status:
        Layer 2 NOT Activated
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 1 CCBs = 0
    The Free Channel Mask:  0x00000000
ISDN Serial0/3/0:23 interface
        ******* Network side configuration *******
        dsl 2, interface ISDN Switchtype = primary-qsig
         **** Network side configuration ****
 --More--
Mar 31 17:29:43.447 CST: %SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement
will be required in    Layer 1 Status:
        DEACTIVATED
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = TEI_ASSIGNED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 2 CCBs = 0
    The Free Channel Mask:  0x00000000
    Number of L2 Discards = 0, L2 Session ID = 0
    Total Allocated ISDN CCBs = 0
```

The following sample output shows the BRI interface with the **isdn skipsend-idverify** command in effect (so the ID verify will *not* be sent):

```
Router# show run interface br0/0
Building configuration...
Current configuration : 185 bytes
!
interface BRI0/0
 no ip address
 encapsulation ppp
 no ip mroute-cache
 isdn switch-type basic-net3
 isdn point-to-point-setup
 isdn incoming-voice voice
 isdn skipsend-idverify
end
```

The following example shows the return to default so that the ID verify will be sent:

```
Router# configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#interface br0/0
router(config-if)#no isdn skipsend-idverify
router(config-if)#
```

The following output shows that the skip send has been removed (so the ID verify information *will* be sent):

```
Router# show run interface br0/0
Building configuration...
Current configuration : 161 bytes
!
interface BRI0/0
 no ip address
 encapsulation ppp
 no ip mroute-cache
 isdn switch-type basic-net3
 isdn point-to-point-setup
 isdn incoming-voice voice
end
```

This configuration example shows the warning message that appears when the command is applied or when the **no** form of the command is entered on a network-side BRI interface:

```
Router# configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#int br1/1
router(config-if)#isdn skipsend-idverify
% Network side should never send ID VERIFY  <---- warning message
router(config-if)#
```

Related Commands

Command	Description
interface bri	Specifies the interface and enters interface configuration mode.

isdn spoofing

To enable ISDN spoofing so that loss of Layer 1 or Layer 2 connectivity of the ISDN BRI interface is not detected by the Trunk Group Resource Manager (TGRM) or similar application, use the **isdn spoofing** command in interface configuration mode. To disable ISDN spoofing so the TGRM or similar application can detect when the BRI interface is not operational (when the Layer 1 or Layer 2 connection is down), use the **no** form of this command.

isdn spoofing
no isdn spoofing

Syntax Description

This command has no arguments or keywords.

Command Default

The ISDN BRI interface is spoofing, which means that applications always see the BRI interface connection as operational (unless the interface has been manually shut down [ADMINDOWN state]).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The ISDN BRI interface is spoofing by default. Spoofing makes the ISDN BRI interface available (up) for operation (for dialing in ISDN), even if the interface is down. For an ISDN BRI interface to be set to a down condition, the interface must be manually shut down (IDBS_ADMINDOWN state). Spoofing enables upper layers to dial out even when the interface is down.

Some upper layer modules, such as TGRM and similar applications, allow dial-out only if the channel is available. If the record for TGRM or similar application is notified of the actual status of BRI, then the TGRM or similar application can dial out accordingly. In this case, the **no isdn spoofing** command is appropriate.

Note ISDN spoofing can be applied only to BRI interfaces--it does not apply to PRI interfaces.

Examples

The following example shows how to configure an ISDN BRI interface to disable ISDN spoofing:

```
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface bri0/0

Router(config-if)# no isdn spoofing
```

Related Commands

Command	Description
interface bri	Configures a BRI interface and enters interface configuration mode.
show isdn status	Displays the status of all ISDN interfaces or a specific ISDN interface.

isdn supp-service calldiversion

To ensure that all calls on an ISDN serial interface can be traced if diverted, use the **isdn supp-service calldiversion** command in interface configuration mode. To disable tracing of diverted ISDN calls, use the **no** form of this command.

isdn supp-service calldiversion
no isdn supp-service calldiversion

Syntax Description

This command has no arguments or keywords.

Command Default

VoIP calls, when diverted, are not traceable and are translated into a Redirection Information Element (RedirectionIE).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

You must explicitly specify an ISDN serial interface. The D channel is always the :23 channel for T1 and the :15 channel for E1.

To enable traceability, the call diversion service requires that a VoIP call (when diverted) translates into a divertingLegInformation2 IE instead of a RedirectionIE. When the **isdn supp-service calldiversion** command is configured, the redirecting information coming from the application is packed in the Facility Information Element (FAC IE) as DiversionLeg2 information and sent in the outgoing SETUP message.

The **isdn supp-service calldiversion** command works only for NET5 switches.

Examples

The following example shows how to configure the primary NET5 switch so that the call diversion tracing service is enabled:

```
interface serial3:23
 no ip address
 isdn switch-type primary-net5
 isdn supp-service calldiversion
```

Related Commands

Command	Description
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller for ISDN PRI, CAS, or robbed-bit signaling.

isdn supp-service mcid

To enable an ISDN serial interface for Malicious Caller Identification (MCID), use the **isdn supp-service mcid** command in interface configuration mode. To disable MCID functionality, use the **no** form of this command.

isdn supp-service mcid
no isdn supp-service mcid

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The ISDN interface must use the NET5 switch type, which is set using the **isdn switch-type primary-net5** command. Protocol emulation must be set to user, which is the default for the **isdn protocol-emulate** command. This command is valid only at the ISDN interface level.

Examples

The following configuration example shows MCID enabled for the PRI:

```
interface serial0:23
 isdn switch-type primary-net5
 ip address 10.10.10.0. 255.255.255.0
 isdn supp-service mcid
 isdn T-Activate 5000
```

Related Commands

Command	Description
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller for ISDN PRI, channel-associated signaling, or robbed-bit signaling.
isdn protocol-emulate	Configures the PRI interface to serve as either the primary (user) or the secondary (network).
isdn switch-type	Specifies the central office switch type on the ISDN interface.
isdn t-activate	Specifies how long the ISDN serial interface must wait for the malicious caller to be identified.

isdn supp-service name calling

To set the calling name display parameters sent out on an ISDN serial interface, use the **isdn supp-service name calling** command in interface configuration mode. To disable calling name delivery, use the **no** form of this command.

isdn supp-service name calling [**ie** | **operation-value-tag** | **profile** {**Network Extension operation-value-tag** {**ecma** | **iso** | **local**} | **ROSE**}]
no isdn supp-service name calling

Syntax Description

ie	(Optional) Specifies that the value of the calling name information element (ie) is to be sent.
operation-value-tag	(Optional) Specifies that the operation value tag for the calling name is to be sent.
profile	(Optional) Specifies that a particular protocol profile is to be sent.
Network-Extension	Specifies the networking extension (0x9F).
ecma	Specifies that the European Computer Manufacturers' Association (ECMA) object identifier (OID) global value (protocol profile 0x06 04 2B 0C 09 00) is to be sent.
iso	Specifies that the International Standards Organization (ISO) OID global value (protocol profile 0x06 05 28 EC 2C 00 00) is to be sent.
local	Specifies that the local OID global value (protocol profile 0x02 01 00) is to be sent.
ROSE	(Optional) Specifies that the Remote Operations Service Element (ROSE) value (protocol profile 0x91) is to be sent.

Command Default

Calling name delivery is disabled, so no calling-name display parameters are set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(15)T1	The **ie**, **operation-value-tag**, **profile**, **Network Extension**, **ecma**, **iso**, **local**, and **ROSE** keywordswere added.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You must explicitly specify an ISDN serial interface. The D channel is always the :23 channel for T1 and the :15 channel for E1.

Under the serial interface (interface serial command), the **isdn supp-service name calling** command must be configured so that when the calling name comes in the Facility Information Element (IE) of the ISDN setup message, the gateway sends the calling name to the Cisco Unified Communications Manager as a Display IE. If the **isdn supp-service name calling** command is not configured under the ISDN serial interface, the calling

name in the FacilityIE is sent as user-to-user data to the Cisco Unified Communications Manager without the display data.

Beginning with Cisco IOS Release 12.4(15)T1, the **ie**, **operation-value-tag**, **profile**, **Network Extension**, **ecma**, **iso**, **local**, and **ROSE** keywords were added to provide more specific information in defining calling name information that is to be sent.

Examples

The following example shows the H.323 Display feature without buffering for ISDN trunks being configured at the voice service level:

```
voice service voip
 h323
 h225 display-ie ccm-compatible
```

The following example shows the H.323 Display feature without buffering for ISDN trunks being configured at the voice class level:

```
voice class h323 1
 h225 display-ie ccm-compatible [system]
```

The following example shows the H.323 name display information on ISDN trunks:

```
interface Serial0/3/0:23
 no ip address
 encapsulation hdlc
 isdn switch-type primary-ni
 isdn incoming-voice voice
 isdn map address *. plan isdn type unknown
 isdn supp-service name calling
 isdn bind-l3 ccm-manager
 no cdp enable
```

Related Commands

Command	Description
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller for ISDN PRI, channel-associated signaling, or robbed-bit signaling.

isdn supp-service tbct

To enable ISDN Two B-Channel Transfer (TBCT) on PRI trunks, use the **isdn supp-service tbct** command in interface or trunk group configuration mode. To reset to the default, use the **no** form of this command.

isdn supp-service tbct [**notify-on-clear** | **tbct-with-crflg**]
no isdn supp-service tbct

Syntax Description

notify -on-clear	(Optional) ISDN switch notifies the gateway whenever a transferred call is cleared.
tbct-with-crflg	(Optional) Includes the call reference flag while sending a TBCT request.

Command Default

TBCT is disabled.

Command Modes

Interface configuration (config-if)
Trunk-group configuration (config-trunkgroup)

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

This command enables TBCT for a specific PRI when used in interface configuration mode. This command configures TBCT for all PRIs in a trunk group when used in trunk-group configuration mode.

The **notify-on-clear** keyword is necessary for the gateway to track billing. This keyword is supported only for user-side ISDN interfaces. You must configure the ISDN switch to send a notify message when a call is cleared.

On some PBX switches, the call reference flag (including the call reference value of the other call) is mandatory. To include the call reference flag in a TBCT request, use the **tbct - with - crflg** keyword. The call reference flag can be 00 or 80. So, for example, if the call reference value is 02, the call reference flag is 0002 or 8002.

Examples

The following example shows how to enable TBCT for interface 0:23:

```
interface Serial0:23
 isdn supp-service tbct
```

The following example shows how to enable TBCT for trunk group 1:

```
trunk group 1
 isdn supp-service tbct
```

The following example shows how to include the call reference flag in TBCT requests for trunk group 1:

```
trunk group 1
 isdn supp-service tbct tbct-with-crflg
```

Related Commands

Command	Description
call application voice transfer mode	Specifies the call-transfer behavior of a TCL or VoiceXML application.
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.
tbct max calls	Sets the maximum number of active calls that can use TBCT.
trunk group	Enters trunk-group configuration mode to define or modify a trunk group.

isdn t-activate



Note Effective with Cisco IOS Release 12.4(11)T, the **isdn t-activate** command is replaced by the **isdn timer** command. See the **isdn timer** command for more information.

To specify how long the gateway waits for a response from the Public Switched Telephone Network (PSTN) after sending a Malicious Call Identification (MCID) request, use the **isdn t-activate** command in interface configuration mode. To disable the timer, use the **no** form of this command.

isdn t-activate *milliseconds*
no isdn t-activate *milliseconds*

Syntax Description

milliseconds	Number of milliseconds (ms) that the router waits for a response from the PSTN after sending a MCID request. Range is 1000 to 15000. Default is 4000; 5000 is recommended.

Command Default

The default wait period is 4000 ms.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(11)T	This command was replaced by the **isdn timer** command.

Usage Guidelines

This command starts a timer when the voice gateway sends a Facility message to the PSTN. If a response is not received within the specified time, the Tool Command Language (TCL) Interactive Voice Response (IVR) script for MCID is notified. Depending on how the script is written, it could reinvoke MCID or perform some other action, such as playing a message if the MCID attempt fails. This command is valid only at the ISDN interface level. The ISDN interface must use the NET5 switch type, which is set using the **isdn switch-type primary-net5** command. Protocol emulation must be set to user, which is the default for the **isdn protocol-emulate** command.

Examples

The following example shows the setting of the timer to a wait period of 5000 ms:

```
interface serial0:23
 isdn switch-type primary-net5
 ip address 10.10.10.0 255.255.255.0
 isdn suppserv mcid
 isdn t-activate 5000
```

Related Commands

Command	Description
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller for ISDN PRI, channel-associated signaling, or robbed-bit signaling.
isdn protocol-emulate	Configures the PRI interface to serve as either the primary (user) or the secondary (network).
isdn switch-type	Specifies the central office switch type on the ISDN interface.
isdn suppserv mcid	Configures an ISDN serial interface for MCID.

isdn tei-negotiation (interface)

To configure when Layer 2 becomes active and ISDN terminal endpoint identifier (TEI) negotiation occurs, use the **isdn tei-negotiation** command in interface configuration mode. To remove TEI negotiation from an interface, use the **no** form of this command.

isdn tei-negotiation {**first-call** | **powerup**} {**preserve** | **remove**}
no isdn tei-negotiation

Syntax Description

first-call	ISDN TEI negotiation occurs when the first ISDN call is placed or received.
powerup	ISDN TEI negotiation occurs when the router is powered up.
preserve	Preserves dynamic TEI negotiation when ISDN Layer 1 flaps, and when the **clear interface** or the **shutdown**and **no shutdown** EXEC commands are executed.
remove	Removes dynamic TEI negotiation when ISDN Layer 1 flaps, and when the **clear interface** or the **shutdown** and **no shutdown** EXEC commands are executed.

Command Default

The **powerup** state is the default condition. Depending on the ISDN switch type configured, the default action is to preserve or remove the TEI negotiation options.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3T	This command was introduced as an interface command.
12.2	The **preserve** and **remove** keywords were added.

Usage Guidelines

This command is for BRI configuration only.

The **first-call** and **powerup**, and **preserve** and **remove**command pairs are mutually exclusive, that is, you must choose only one command from either the **first-call** and **powerup** or **preserve** and **remove**command pairs, per command line.

The **no isdn tei-negotiation**command returns the configuration to default to the **powerup** state.

Use of the **preserve**keyword causes different behavior depending on the ISDN switch type configured, that is, the TEI negotiation configured will be preserved during ISDN Layer 1 flaps, and when the **clear interface** or the **shutdown** and **no shutdown** EXEC commands are executed, on the switch types listed in the table below.

Table 17: Switch Types with Preserved TEI Negotiation

Switch Type	Cisco IOS Keyword
French ISDN switch types	**vn2, vn3**
Lucent (AT&T) basic rate 5ESS switch	**basic-5ess**

Switch Type	Cisco IOS Keyword
Northern Telecom DMS-100 basic rate switch	**basic-dms100**
National ISDN basic rate switch	**basic-ni**
PINX (PBX) switches with QSIG signaling per Q.931	**basic-qsig**

For all other ISDN switch types, the TEI negotiation will be removed during ISDN Layer 1 flaps, and when the **clear interface** or the **shutdown** and **no shutdown** EXEC commands are executed. Use the **remove** keyword to specifically set one of the switches listed in the table above to the remove state.

The **first-call** keyword and its functionality are not supported on U.S. switch types (basic-ni, basic-5ess, basic-dms100, primary-ni, primary-4ess, primary-5ess, and primary-dms100), especially for service profile identifier (SPID) negotiations. The **first-call** keyword and its functionality are supported on European switch types (basic-net3 and primary-net5) to prevent Layer 2 activity when there are no Layer 3 calls.

Examples

The following example shows the ISDN TEI negotiation configuration with default settings. (Defaults settings do not appear in the router configuration.)

```
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 cdapi buffers regular 0
 cdapi buffers raw 0
 cdapi buffers large 0
```

The following example shows how to set TEI negotiation timing to the first call:

```
Router(config-if)# isdn tei-negotiation first-call
Router(config-if)# exit
Router(config)# exit
Router# show startup-config
.
.
.
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 isdn tei-negotiation first-call
 cdapi buffers regular 0
 cdapi buffers raw 0
 cdapi buffers large 0interface BRI0/0
```

The following example shows how to change TEI negotiation timing back to the default power-up state:

```
Router(config-if)# no isdn tei-negotiation
Router(config-if)# exit
Router(config)# exit
Router# show startup-config
.
.
.
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 cdapi buffers regular 0
```

```
 cdapi buffers raw 0
 cdapi buffers large 0
```

The following example shows how to remove TEI negotiation when ISDN Layer 1 flaps (the preserve state is the default for the National ISDN basic rate switch):

```
Router(config-if)# isdn tei-negotiation remove
Router(config-if)# exit
Router(config)# exit
Router# show startup-config
.
.
.
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 isdn tei-negotiation first-call
 isdn tei-negotiation remove
 cdapi buffers regular 0
 cdapi buffers raw 0
 cdapi buffers large 0
```

The following example shows how to return the National ISDN basic rate switch to its default preserve state:

```
Router(config-if)# no isdn tei-negotiation
Router(config-if)# exit
Router(config)# exit
Router# show startup-config
.
.
.
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 isdn tei-negotiation first-call
 cdapi buffers regular 0
 cdapi buffers raw 0
 cdapi buffers large 0
```

iua

To specify backhaul using Stream Control Transmission Protocol (SCTP) and to enter IDSN User Adaptation Layer (IUA) configuration mode, use the **iua** command in terminal configuration mode.

iua

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. 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 support was added for the Cisco AS5300 and Cisco AS5850.
12.2(15)T	This command was implemented on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series; and Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.

Usage Guidelines

You must first enter IUA configuration mode to access SCTP configuration mode. First enter IUA configuration mode by using the example below and then enter sctp at the Router(config-iua)#prompt to bring up SCTP configuration mode. See the sctp command.

Examples

The following example shows how to enter iua configuration mode:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# iua
Router(config-iua)#
```

The following example shows how to configure the failover-timer by setting the failover time (in milliseconds) to 1 second for a particular AS:

```
Router(config-iua)# as as5400-3 fail-over-timer 1000
```

The following example configure the number of SCTP streams for this AS to 57, which is the maximum value allowed:

```
Router(config-iua)# as as5400-3 sctp-streams 57
```

Related Commands

Command	Description
isdn bind -L3 iua-backhaul	Specifies ISDN backhaul using SCTP for an interface.
show iua as	Shows information about the current condition of an AS.
show iua asp	Shows information about the current condition of an ASP.

ivr asr-server

To specify the location of an external media server that provides automatic speech recognition (ASR) functionality to voice applications, use the **ivr asr-server** command in global configuration mode. To remove the server location, use the **no** form of this command.

ivr asr-server *url*
no ivr asr-server

Syntax Description

url	Location of the ASR resource on the media server, in uniform resource locator (URL) format.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 26.2.1	This command was modified to display warning message for insecure protocol usage.
12.4(15)T	The *url* argument was modified to accept a Media Resource Control Protocol version 2 (MRCP v2) server URL.
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

This command sets the server location globally for all voice applications on the gateway.

For Nuance media servers that use the default installation, specify the URL as follows:

ivr asr -server rtsp://*host***:***port]***/recognizer**

(*host* is the host name of the media server; **:***port* is optional.)

For media servers using MRCP v2, specify the URL as follows:

ivr asr -server sip:*server-name@host-name* | *ip-address*

You can specify the location of the media server within a VoiceXML document, overriding the Cisco gateway configuration. For more information, see the Cisco VoiceXML Programmer's Guide.

Warning Starting with Cisco IOS XE 26.2.1, a warning message is displayed when insecure protocols such as HTTP, FTP, or TFTP are used, as they do not provide encryption or authentication. Use secure alternatives such as HTTPS, SFTP, or SCP instead.

Examples

The following example shows the warning message being displayed for the usage of insecure RTSP protocol:

```
Device(config)#ivr asr-server rtsp://asr_serv/recognizer
SECURITY WARNING - Module: DEFAULT_VOICE_CONFIG, Command: ivr asr-server
rtsp://asr_serv/recognizer,
Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of
encryption and authentication,
Description: ivr asr-server configured with insecure RTSP URL, Remediation: Use secure
protocols instead of insecure RTSP
Device(config)#
```

Examples

The following example specifies that voice applications use the ASR server named "asr_serv":

```
Router(config)# ivr asr-server rtsp://asr_serv/recognizer
```

The following example specifies that voice applications use the MRCP v2 ASR server named "asr_mrcpv2serv":

```
Router(config)# ivr asr-server sip:asr_mrcpv2serv@mediaserver.com
```

Related Commands

Command	Description
ivr tts -server	Specifies the location of a media server that provides TTS functionality to voice applications.
ivr tts -voice-profile	Specifies the location of the voice profile that is used by the TTS server.

ivr autoload mode

To load files from TFTP to memory using either verbose or silent mode, use the **ivr autoload mode** command in global configuration mode. To disable this function, use the **no** form of this command.

ivr autoload mode { **verbose** | **silent** } { **url** *location* | [**retry** *number*] }
no ivr autoload

Syntax Description

verbose	Displays the file transfer activity to the console. This mode is recommended while debugging.
silent	Performs the file transfer in silent mode, meaning that no file transfer activity is displayed to the console.
url *location*	URL that is used to locate the index file that contains a list of all available audio files.
retry *number*	(Optional) Number of times that the system tries to transfer a file when there are errors. This parameter applies to each file transfer. Range is from 1 to 5. Default is 3.

Command Default

Silent

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 26.2.1	This command was modified to display warning message for insecure protocol usage.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.0(7)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.

Usage Guidelines

The index file contains a list of audio files (URL) that can be downloaded from the TFTP server. Use the **ivr autoload mode** command to download audio files from TFTP to memory. The command only starts up a background process. The background process (loader) does the actual downloading of the files.

The background process first reads the index file from either Flash or TFTP. It parses the files line by line looking for the URL. It ignores lines that start with # as comment lines. Once it has a correct URL, it tries to read that.au file into memory and creates a media object. If there are any errors during the reading of the file, it retries the configured number of times. If the mode is set to **verbose**, the loader logs the transaction to console. Once parsing has reached the end of the index file, the background process exits memory.

Perform the following checks before initiating the background process. If one of the checks fails, it indicates the background process is not started, and instead you see an error response to the command.

- Check if any prompt is being actively used (IVR is actively playing some prompts). If there are active prompts, the command fails, displaying the following error message (.au files are also referred to as prompts): "Command is not allowed when prompts are active".

- Check if there is already a background process in progress. If there is a process, the command fails, displaying the following error: "Previous autoload command is still in progress".
- If the **ivr autoload url** command has already been configured, the user sees the following response when the command is issued: "Previous command is being replaced".
- When the **no ivr autoload url** command is issued, while there was already an **ivr autoload url** command in progress, the original command is aborted.

The audio files (prompts) loaded using the **ivr autoload url** command are not dynamically swapped out of memory. They are considered to be autoloaded prompts, as opposed to dynamic prompts. (See the **ivr prompt memory** command for details on dynamic prompts.)



Warning Starting with Cisco IOS XE 26.2.1, a warning message is displayed when insecure protocols such as HTTP, FTP, or TFTP are used, as they do not provide encryption or authentication. Use secure alternatives such as HTTPS, SFTP, or SCP instead.

Examples

The following example shows the warning message being displayed for the usage of insecure TFTP protocol:

```
Device(config)#ivr autoload mode silent url tftp://blue/orange/tclware/index4
SECURITY WARNING - Module: IVR, Command: ivr autoload mode silent url
tftp://blue/orange/tclware/index4,
Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of
encryption and authentication,
Description: IVR autoload mode configured with insecure TFTP protocol - vulnerable to content
 tampering,
Remediation: Use secure protocols such as HTTPS, SFTP, or SCP instead of insecure HTTP,
FTP, or TFTP
```

The following example configures verbose mode:

```
ivr autoload mode verbose url tftp://blue/orange/tclware/index4 retry 3
```

The following example shows the resulting index file:

```
more index4
tftp://blue/orange/tclware/au/en/en_one.au
tftp://blue/orange/tclware/au/ch/ch_one.au
tftp://blue/orange/tclware/au/ch/ch_one.au
```

The following example shows an index file on Flash memory:

flash:index

Related Commands

Command	Description
ivr prompt memory	Configures the maximum amount of memory that the dynamic audio files occupy in memory.

ivr prompt memory

To configure the maximum amount of memory that the dynamic audio files (prompts) occupy in memory, use the **ivr prompt memory** command in global configuration mode. To disable the maximum memory size, use the **no** form of this command.

ivr prompt memory *size* **files** *number*
no ivr prompt memory

Syntax Description

size	Maximum memory to be used by the free dynamic prompts, in kilobytes. Range is 128 to 16384. The default is 128.
files *number*	Number of files that can stay in memory. Range is 50 to 1000. The default is 200.

Command Default

Memory size: 128 KB Number of files: 200

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

When both the *number* and *size* parameters are specified, the minimum memory out of the two is used for memory calculations.

All the prompts that are not autoloaded or fixed are considered dynamic. Dynamic prompts are loaded in to memory from TFTP or Flash, as and when they are needed. When they are actively used for playing prompts, they are considered to be in "active" state. However, once the prompt playing is complete, these prompts are no longer active and are considered to be in a free state.

The free prompts either stay in memory or are removed from memory depending on the availability of space in memory for these free prompts. This command essentially specifies a maximum memory to be used for these free prompts.

The free prompts are saved in memory and are queued in a wait queue. When the wait queueis full (either because the totally memory occupied by the free prompts exceeds the maximum configured value or the number of files in the wait queue exceeds maximum configured), oldest free prompts are removed from memory.

Examples

The following example sets memory size to 2048 KB and number of files to 500:

```
ivr prompt memory 2048 files 500
```

Related Commands

Command	Description
ivr autoload	Loads files from a particular TFTP server.
show call prompt -mem-usage	Displays the memory site use by prompts.
ivr prompt streamed	Streams audio prompts from particular media types during playback.

ivr autoload url

To load files from a particular TFTP server (as indicated by a defined URL), use the **ivr autoload** command in global configuration mode. To disable this function, use the **no** form of this command.

ivr autoload url *location*
no ivr autoload url *location*

Syntax Description

url *location*	URL that is to be used to locate the index file that contains a list of all available audio files.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 26.2.1	This command was modified to display warning message for insecure protocol usage.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.0(7)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.

Usage Guidelines

The index file contains a list of audio files URLs that can be downloaded from the TFTP server. Use the **ivr autoload url** command to download audio files from TFTP to memory. The command starts a background process (loader) that does the actual downloading of the files.

The background process first reads the index file from either Flash memory or TFTP. It parses the files line by line, looking for the URL. It ignores lines that start with # as comment lines. Once it has a correct URL, it tries to read that .au file into memory and creates a media object. If there are any errors during the reading of the file, it retries the configured number of times. If the *mode* is set to "verbose," in the **ivr autoload mode** command the loader logs the transaction to console. Once parsing has reached the end of the index file, the background process exits memory.

Perform the following checks before initiating the background process. If one of the checks fails, it indicates that the background process is not started, and instead you see an error response to the command.

- Check to see if any prompt is being actively used (IVR is actively playing some prompts). If there are active prompts, the command fails, displaying the following error message (.au files are also referred to as prompts): "Command is not allowed when prompts are active"
- Check to see if there is already a background process in progress. If there is a process, the command fails, displaying the following error: "Previous autoload command is still in progress"
- Check to see if an earlier **ivr autoload url** command has already been configured. If configured, the user sees the following response when the command is issued again: "previous command is being replaced"

- When the **no ivr autoload url** command is issued, if there is already an **ivr autoload url** command in progress, it is aborted.

The audio files (prompts) loaded using the **ivr autoload** command are not dynamically swapped out of memory. They are considered as autoloaded prompts as opposed to "dynamic" prompts. See the **ivr prompt memory** command for details on dynamic prompts.

Warning Starting with Cisco IOS XE 26.2.1, a warning message is displayed when insecure protocols such as HTTP, FTP, or TFTP are used, as they do not provide encryption or authentication. Use secure alternatives such as HTTPS, SFTP, or SCP instead.

Examples

The following example shows the warning message being displayed for the usage of insecure TFTP protocol:

```
Device(config)#ivr autoload url tftp://blue/orange/tclware/index4
 previous autoload command will be replaced

SECURITY WARNING - Module: DEFAULT_VOICE_CONFIG, Command: ivr autoload url
tftp://blue/orange/tclware/index4 ,
Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of
encryption and authentication,
Description: ivr autoload url voice configured with insecure FTP/HTTP/TFTP URL protocol,
Remediation: Use secure protocols such as HTTPS, SFTP, or SCP instead of insecure HTTP,
FTP, or TFTP
Device(config)#
```

Examples

The following example loads audio files from the TFTP server (located at //jurai/mgindi/tclware/index4):

```
ivr autoload url tftp://jurai/mgindi/tclware/index4
```

The following example shows the resulting index file:

```
more index4
tftp://jurai/mgindi/tclware/au/en/en_one.au
tftp://jurai/mgindi/tclware/au/ch/ch_one.au
tftp://jurai/mgindi/tclware/au/ch/ch_one.au
```

The following example shows an index file on Flash:

```
flash:index
```

Related Commands

Command	Description
ivr prompt memory	Configures the maximum amount of memory that the dynamic audio files (prompts) occupy in memory.

ivr contact-center

To enable a specific set of debug commands on a Cisco router that is being used in a contact center, use the **ivr command-cente**r command in global configuration mode. To stop automatically enabling these debug commands after the router is reloaded, use the **no** form of this command.

ivr command-center
no ivr command-center

Syntax Description

This command has no arguments or keywords.

Command Default

Specific individual debug commands must be manually enabled each time the router is reloaded.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T2	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(15)T4	The ccapi, cch323, and ccsip error debugs were included in the output display.
12.4(20)YA	This command was integrated into Cisco IOS Release 12.4(20)YA.

Usage Guidelines

To troubleshoot a Cisco router that is being used in a contact center, it is often necessary to enable specific debug commands to display error messages. Typically, you must manually enable the individual debug commands each time the router is reloaded. Use the **ivr contact-center** command to enable the following debug commands and to automatically re-enable these commands each time the router is reloaded:

- **debug ccsip error**
- **debug cch323 error**
- **debug http client error**
- **debug mrcp error**
- **debug rtsp error**
- **debug voip application error**
- **debug voip application vxml error**
- **debug voice ccapi error**

While this command is configured, the listed debug commands cannot be disabled. Attempts to disable any of these debug commands while the **ivr contact-center** command is configured will display a warning message and the debug command will not be disabled.

Configuring the **no ivr contact-center** command does not disable the listed debug commands. To disable these debug commands after configuring the **no ivr contact-center** command, you must either manually

disable each individual debug command or reload the router, after which these debug commands are not re-enabled.

You can verify that the listed debug commands are enabled after you configure the **ivr contact-center** command by using the **show debug**command.

Examples

The following partial output from the **show running-config** command shows that the **ivr contact-center** command is enabled:

```
Router# show running-confi
Building configuration...
Current configuration : 20256 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname c5400-02
!
! ***** snipped *****
!
ivr contact-center
ivr prompt memory 16384 files 1000
ivr asr-server rtsp://CVPASR/media/speechrecognizer
ivr tts-server rtsp://CVPTTS/media/speechsynthesizer
!
! ***** snipped *****
```

The following output from the **show debug**command displays current debugging information that includes the error debug messages automatically enabled by the **ivr contact-center**command:

To display current debugging information that includes the error debug messages automatically enabled by "ivr contact-center", use the show debug command in privileged EXEC mode.

```
c3825-01(config)#ivr contact-center
c3825-01(config)#end
Router# show debug
CCH323 SPI: Error debug is enabled
CCAPI:
  debug voip ccapi error call is ON (filter is OFF)
  debug voip ccapi error software is ON
CCSIP SPI: SIP error debug tracing is enabled   (filter is OFF)
HTTP Client:
  HTTP Client Error debugging is on
APPLICATION:
  debug voip application error is ON
RTSP:
  RTSP client Protocol Error debugging is on
MRCP:
  MRCP client error debugging is on
VXML:
  debug voip application vxml error software is ON
  debug voip application vxml error call is ON (filter is OFF)
c3825-01#
```

Related Commands

Command	Description
debug http client error	Displays error messages for the HTTP client.
debug mrcp error	Displays error messages for Media Resource Control Protocol (MRCP) operations.
debug rtsp error	Displays debug information about the Real-Time Streaming Protocol (RTSP) client.
debug voip application error	Displays error messages for all voice applications.
debug voip application vxml error	Displays error messages for a VoiceXML application.
debug voice ccapi error	Displays error messages for the call control application programming interface (CCAPI) contents.
debug ccsip error	Displays Session Initiation Protocol (SIP)-related error messages.
debug cch323 error	Displays error messages for components within the H.323 subsystem.
show debug	Displays current debugging information automatically enabled by **ivr contact-center** command.

ivr language link

To link configured language packages, use the **ivr language link** command in global configuration mode. To delink the configured language packages, use the **no** form of this command.

ivr language link {**all** | **on-demand**}
no ivr language link

Syntax Description

all	Links all the configured language packages.
on-demand	Links the language packages when asked for.

Command Modes

Global configuration (config)

Command Default

The language packages are not linked.

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 Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to link all the configured language packages:

```
Router# configure terminal
Router(config)# ivr language link all
```

Related Commands

Command	Description
ivr asr-server	Specifies the location of an external media server that provides ASR functionality to voice applications.

ivr prompt cutoff-threshold

To configure the maximum delay time for audio prompts, use the **ivr prompt cut-off threshold** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ivr prompt cutoff-threshold *time*
no ivr prompt cutoff-threshold

Syntax Description

time	Maximum delay time, in milliseconds (ms). The range is from 120 to 1000.

Command Default

The maximum delay time 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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to configure the maximum delay time for audio prompts:

```
Router# configure terminal
Router(config)# ivr prompt cutoff-threshold 129
```

Related Commands

Command	Description
ivr prompt streamed	Streams audio prompts from particular media types during playback.

ivr prompt streamed

To stream audio prompts from particular media types during playback, use the **ivr prompt streamed** command in global configuration mode. To reset to the default, use the **no** form of this command.

ivr prompt streamed { **all** | **flash** | **http** | **none** }
no ivr prompt streamed { **all** | **flash** | **http** | **none** }

Syntax Description

all	All audio prompts, from all URL types (Flash memory, HTTP).
flash	Audio prompts from Flash memory.
http	Audio prompts from an HTTP URL. This is the default value.
none	No audio prompts from any media type.

Command Default

Audio prompts from HTTP URLs and other media types are not streamed during playback.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 26.2.1	This command was modified to display warning message for insecure protocol usage.
12.4(20)T	The **tftp** keyword was removed.
12.4(15)T	The command default was changed from streaming for audio prompts during playback to no streaming.
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

To enable streaming for multiple media types, either enter this command for each URL type or enter the ivr prompt streamed all command. If you do not enter this command, audio prompts from HTTP servers and Flash servers are not streamed during playback.

Note Prompts from a Real Time Streaming Protocol (RTSP) server are not controlled by this command and are always streamed during playback.

Warning Starting with Cisco IOS XE 26.2.1, a warning message is displayed when insecure protocols such as HTTP, FTP, or TFTP are used, as they do not provide encryption or authentication. Use secure alternatives such as HTTPS, SFTP, or SCP instead.

Examples

The following example indicates that audio prompts from Flash memory are streamed when they are played back:

```
ivr prompt streamed flash
```

The following example shows the warning message being displayed for the usage of insecure HTTP protocol:

```
Device(config)#ivr prompt streamed http
SECURITY WARNING - Module: IVR, Command: ivr prompt streamed http,
Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of
encryption and authentication,
Description: IVR prompt streaming configured with insecure HTTP protocol - vulnerable to
content tampering,
Remediation: Use secure protocols such as HTTPS, SFTP, or SCP instead of insecure HTTP,
FTP, or TFTP
```

Related Commands

Command	Description
ivr prompt memory	Sets the maximum amount of memory that dynamic audio prompts can occupy in memory.

ivr record cpu flash

To configure the maximum percentage allowed for the flash write process in CPU, use the **ivr record cpu flash**command in global configuration mode. To disable this configuration, use the **no** form of this command.

ivr record cpu flash *number*
no ivr record cpu flash

Syntax Description

number	Numeric label that specifies the maximum percentage allowed for the flash write process in the CPU. The range is from 1 to 99. The default is 99.

Command Default

The maximum percentage is configured to 99.

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 that the flash recording allowed is set to 50 percent:

```
Router# configure terminal
Router(config)# ivr record cpu flash 50
```

Related Commands

Command	Description
ivr prompt streamed	Streams audio prompts from particular media types during playback.

ivr record jitter

To set the maximum amount of jitter memory that can be used to record voice messages during a single call session, use the **ivr record jitter** command in global configuration mode. To free up the allocated jitter memory, use **no** form of this command.

ivr record jitter *WORD kilobytes*
no ivr record jitter *WORD*

Syntax Description

WORD	Specifies string containing url scheme.
tftp: | http:	Specifies the protocol.
kilobytes	Memory size in kilobytes. Range is from 1024 to 32,000.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 26.2.1	This command was modified to display warning message for insecure protocol usage.
IOS XE Fuji Release 16.8.1	This command was introduced.

Usage Guidelines

Use this command to limit the maximum jitter memory allowed for audio recordings during a single call session on a VoiceXML-enabled gateway.

Warning Starting with Cisco IOS XE 26.2.1, a warning message is displayed when insecure protocols such as HTTP, FTP, or TFTP are used, as they do not provide encryption or authentication. Use secure alternatives such as HTTPS, SFTP, or SCP instead.

Examples

The following example shows the warning message being displayed for the usage of insecure HTTP protocol:

```
Device(config)#ivr record jitter http://10.10.10.70//tftpboot/COLT-DE-CUCM.cfg 1024
SECURITY WARNING - Module: IVR, Command: ivr record jitter
http://10.10.10.70//tftpboot/COLT-DE-CUCM.cfg 1024 ,
Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of
encryption and authentication,
Description: IVR record jitter configured with insecure URL protocol - vulnerable to data
interception,
Remediation: Use secure protocols such as HTTPS, SFTP, or SCP instead of insecure HTTP,
FTP, or TFTP
```

Related Commands

Command	Description
ivr record memory session	Sets the maximum amount of memory that can be used to record voice message during a single call session.
ivr record memory system	Sets the maximum amount of memory that can be used to store all voice recordings on the VoiceXML-enabled gateway.

ivr record memory session

To set the maximum amount of memory that can be used to record voice messages during a single call session, use the **ivr record memory session** command in global configuration mode. To reset to the default, use the **no** form of this command.

ivr record memory session *kilobytes*
no ivr record memory session

Syntax Description

kilobytes	Memory size, in kilobytes. Range is 0 to 256000. The default is 256.

Command Default

256 KB

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300.
12.2(11)T	This command was implemented on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

Use this command to limit the maximum memory allowed for audio recordings during a single call session on a VoiceXML-enabled gateway.

Note This command configures memory limits only for voice messages recorded to local memory on the gateway. Memory limits are not configurable on the gateway for HTTP, Real Time Streaming Protocol (RTSP), or Simple Mail Transfer Protocol (SMTP) recordings.

Examples

The following example sets the maximum memory limit to 512 KB for a single call session:

```
ivr record memory session 512
```

Related Commands

Command	Description
ivr record memory system	Sets the maximum amount of memory that can be used to store all voice recordings on the VoiceXML-enabled gateway.

ivr record memory system

To set the maximum amount of memory that can be used to store all voice recordings on the gateway, use the **ivr record memory system** command in global configuration mode. To reset to the default, use the **no** form of this command.

ivr record memory system *kilobytes*
no ivr record memory system

Syntax Description

kilobytes	Memory limit, in kilobytes. Range is 0 to 256000. If 0 is configured, the RAM recording function is disabled on the gateway. The default for Cisco 3640 and Cisco AS5300 is 10000. The default for Cisco 3660, Cisco AS5350, and Cisco AS5400 is 20000.

Command Default

Cisco 3640 and Cisco AS5300: 10,000 KB Cisco 3660, Cisco AS5350, and Cisco AS5400: 20,000 KB

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300.
12.2(11)T	This command was implemented on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

Use this command to limit the maximum amount of gateway memory that is used for storing all voice recordings.

Note This command configures memory limits only for voice messages recorded to local memory on the gateway. Memory limits are not configurable on the gateway for HTTP, Real Time Streaming Protocol (RTSP), or Simple Mail Transfer Protocol (SMTP) recordings.

Examples

The following example sets the total memory limit for all recordings to 8000 KB:

```
ivr record memory system 8000
```

Related Commands

Command	Description
ivr record memory session	Sets the maximum amount of memory that can be used to record voice messages during a single call session.

ivr tts-server

To specify the location of an external media server that provides text-to-speech (TTS) functionality to voice applications, use the **ivr tts-server** command in global configuration mode. To remove the server location, use the **no** form of this command.

ivr tts-server *url*
no ivr tts-server

Syntax Description

url	Location of the TTS resource on the media server, in uniform resource locator (URL) format.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 26.2.1	This command was modified to display warning message for insecure protocol usage.
12.4(15)T	The *url* argument was modified to accept a Media Resource Control Protocol version 2 (MRCP v2) server URL.
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

This command sets the server location globally for all voice applications on the gateway.

For Nuance media servers that use the default installation, specify the URL as follows:

ivr tts-server rtsp:// *host* **:** *port* **/synthesizer**

(*host* is the host name of the media server; **:***port* is optional.)

For media servers using MRCP v2, specify the URL as follows:

ivr tts -server sip:*server-name@host-name* | *ip-address*

You can specify the location of the media server within a VoiceXML document, overriding the Cisco gateway configuration. For more information, see the Cisco VoiceXML Programmer's Guide.

To specify the voice profile that the TTS server uses for voice synthesis operations, use the **ivr tts-voice-profile** command.

Warning Starting with Cisco IOS XE 26.2.1, a warning message is displayed when insecure protocols such as HTTP, FTP, or TFTP are used, as they do not provide encryption or authentication. Use secure alternatives such as HTTPS, SFTP, or SCP instead.

Examples

The following example shows the warning message being displayed for the usage of insecure RSTP protocol:

```
Device(config)#ivr tts-server rtsp://tts_serv/synthesizer
SECURITY WARNING - Module: DEFAULT_VOICE_CONFIG, Command: ivr tts-server
rtsp://tts_serv/synthesizer,
Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of
encryption and authentication,
Description: ivr tts-server configured with insecure RTSP URL, Remediation: Use secure
protocols instead of insecure RTSP
Device(config)#
```

Examples

The following example specifies that voice applications use the TTS server named "tts_serv":

```
Router(config)# ivr tts-server rtsp://tts_serv/synthesizer
```

The following example specifies that voice applications use the MRCP v2 TTS server named "tts_mrcpv2serv":

```
Router(config)# ivr tts-server sip:tts_mrcpv2serv@mediaserver.com
```

Related Commands

Command	Description
ivr asr -server	Specifies the location of a media server that provides ASR functionality to IVR applications.
ivr tts -voice-profile	Specifies the location of the voice profile that is used by the TTS server.

ivr tts-voice-profile

To specify the location of the voice profile that is used by text-to-speech (TTS) servers, use the **ivr tts-voice-profile** command in global configuration mode. To remove the voice profile, use the **no** form of this command.

ivr tts-voice-profile *url*
no ivr tts-voice-profile

Syntax Description

url	Location of the TTS voice profile file, in URL format.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

This command specifies the voice profile that a TTS server uses for voice synthesis operations. The voice profile is a W3C Simple Markup Language (SML) file that specifies voice parameters like gender, speed, and so forth. The TTS server uses this voice profile unless the markup file that it is translating has overriding values.

The TTS voice profile can be stored on an HTTP server or on RTSP, TFTP, or FTP servers if the media sever supports these locations.

The TTS voice profile location can also be specified in the VoiceXML document by using the Cisco proprietary property com.cisco.tts-voice-profile. The VoiceXML property in the document overrides the value that is configured by using this command.

To specify the location of the external media server that is providing TTS functionality, use the **ivr tts-server** command.

Examples

The following example tells the TTS server to use the voice profile file named "vprofil2", which is located on an HTTP server:

```
ivr tts-voice-profile http://ttserver/vprofil2.sml
```

Related Commands

Command	Description
ivr asr -server	Specifies the location of a media server that provides ASR functionality to IVR applications.
ivr tts -server	Specifies the media server that provides TTS functionality to IVR applications.

ixi application cme

To enter XML application configuration mode for the Cisco Unified CallManager Express (Cisco Unified CME) application, use the **ixi application cme**command in global configuration mode.

ixi application cme

Syntax Description

This command has no arguments or keywords.

Command Default

XML parameters are not set for the Cisco Unified CME application.

Command Modes

Global configuration (config)

Command History

Cisco IOS Release	Modification
12.4(4)XC	This command was introduced.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

In Cisco Unified CME 4.0 and later versions, an XML interface is provided through the Cisco IOS XML Infrastructure (IXI), in which the parser and transport layers are separated from the application itself.

When you are using the Cisco IOS XML Infrastructure, the same HTTP transport layer can be used by multiple applications. The **ixi application cme** command enters XML application configuration mode to allow you to set Cisco IOS XML Infrastructure parameters for the Cisco Unified CME application. In this configuration mode, you can set the response timeout parameter using the **response timeout**command and enable communication with the application using the **no shutdown** command.

The **ixi transport** command allows you to set parameters for the Cisco IOS XML Infrastructure transport layer.

Note The **no** form of the **ixi application cme** command is not supported.

Examples

The following example shows how to configure the Cisco Unified CME application to overwrite the Cisco IOS XML Infrastructure transport-level timeout with a 30-second response timeout and enable XML communication with the application.

```
Router(config)# ixi application cme
Router(conf-xml-app)# response timeout 30
Router(conf-xml-app)# no shutdown
```

Related Commands

Command	Description
ixi transport	Enters XML transport configuration mode.

Command	Description
no shutdown	Enables XML communication with the application.
response (XML application)	Sets a timeout for responding to the XML application and overwrites the IXI transport-level timeout.

ixi application mib

To enter XML application configuration mode, use the **ixi application**command in global configuration mode.

ixi application mib

Syntax Description

mib	XML application for which parameters will be configured. Valid value: **mib**.

Command Default

No XML applications are configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The Cisco IOS XML Infrastructure (IXI) simplifies the implementation and deployment of XML-based applicatiosn in Cisco IOS software. IXI applications can be clients and or servers where the parser and transport layers are separated from the application itself. This modularity provides scalability and enables future XML supports to be developed.

An eXtensible Markup Language (XML) application programming interface (API) supports Cisco IOS commands allowing you to specify certain parameters associated with the XML API.

Once you are in XML application configuration mode, you can use the following commands:

- **default** --XML application configuration parameters defaults.
- **exit** --Apply changes and exit from XML application configuration mode.
- **help** --Display of the interactive help system.
- **no** --Negate a command or set its defaults.
- **response** --Response parameters.
- **shutdown** --Stop the application.

Examples

The following example shows how to enter XML application configuration mode, set the XML application timeout period to 30 seconds, format the response parameters to in human readable XML, and exit XML application configuration mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ixi application mib
Router(conf-xml-app)# response timeout 30
Router(conf-xml-app)# response formatted
Router(conf-xml-app)# exit
```

Related Commands

Command	Description
ixi transport http	Sets XML transport parameters.
response (XML application)	Sets XML application mode response parameters.

ixi transport http

To enter XML transport configuration mode, use the **ixi transport**command in global configuration mode.

ixi transport http

Syntax Description

http	Specifies the http transport protocol.

Command Default

No XML transport is configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The Cisco IOS XML Infrastructure (IXI) simplifies the implementation and deployment of XML-based applications in Cisco IOS software. IXI applications can be clients and or servers where the parser and transport layers are separated from the application itself. This modularity provides scalability and enables future XML supports to be developed. IXI allows applications to be written in a transport independent manner. The **ixi transport** command enters XML transport configuration mode where you can set transport configuration parameters.

Once you are in XML transport configuration mode, you can access the following commands:

- **default** *option* --XML transport configuration command defaults.
- **exit** --Apply changes and exit from XML application configuration mode.
- **help** --Display the interactive help system.
- **no** --Negate a command or set its defaults.
- **request** --Request handling parameters.
- **response size** --Response transport fragment size.
- **shutdown** --Stop the transport.

Examples

The following example shows how to enter XML transport configuration mode, set the XML transport fragment size to 32 Kbytes, and exit XML transport configuration mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ixi transport http
Router(conf-xml-trans)# response size 32

Router(conf-xml-trans)# exit
```

Related Commands

Command	Description
ixi application mib	Sets XML application parameters.
request (XML transport)	Sets XML transport request handling parameters.
response size (XML transport)	Set the XML transport fragment size.