

H

- h225 alt-ep hunt, on page 3
- h225 connect-passthru, on page 8
- h225 display-ie, on page 10
- h225 h245-address, on page 12
- h225 h245-address on-connect (H.323 voice-class), on page 14
- h225 h245-address on-connect (H.323 voice-service), on page 16
- h225 h245-address setup, on page 18
- h225 id-passthru, on page 20
- h225 plus-digit passthru, on page 21
- h225 signal overlap, on page 23
- h225 start-h245, on page 24
- h225 timeout call-proceeding, on page 25
- h225 timeout keepalive, on page 27
- h225 timeout setup, on page 28
- h225 timeout t302, on page 29
- h225 timeout t304, on page 30
- h225 timeout tcp call-idle (H.323 voice service), on page 31
- h225 timeout tcp establish, on page 32
- h225 timeut ntf, on page 33
- h245 address-check, on page 35
- h245 passthru, on page 36
- h245 timeout, on page 37
- h323, on page 39
- h323 asr, on page 40
- h323 call start, on page 41
- h323 gatekeeper, on page 43
- h323 h323-id, on page 44
- h323 interface, on page 45
- h323 qos, on page 46
- h323 t120, on page 47
- h323-annexg, on page 48
- h323-gateway voip bind srcaddr, on page 50
- h323-gateway voip h323-id, on page 51

- h323-gateway voip id, on page 52
- h323-gateway voip interface, on page 54
- h323-gateway voip tech-prefix, on page 55
- h323zone-id (voice source group), on page 57
- h450 h450-3 timeout, on page 58
- handle-replaces, on page 59
- hangup-last-active-call, on page 61
- header-passing, on page 63
- history-info, on page 65
- history session event-log save-exception-only, on page 66
- history session max-records, on page 67
- history session retain-timer, on page 68
- hold-resume, on page 69
- hopcount, on page 70
- host (SIP URI), on page 71
- host-registrar, on page 73
- http client cache memory, on page 75
- http client cache query, on page 77
- http client cache refresh, on page 78
- http client connection idle timeout, on page 80
- http client connection persistent, on page 81
- http client connection timeout, on page 82
- http client cookie, on page 83
- http client post-multipart, on page 84
- http client response timeout, on page 85
- http client secure-ciphersuite, on page 86
- http client secure-trustpoint, on page 90
- hunt-scheme least-idle, on page 91
- hunt-scheme least-used, on page 93
- hunt-scheme longest-idle, on page 95
- hunt-scheme random, on page 97
- hunt-scheme round-robin, on page 98
- hunt-scheme sequential, on page 100
- huntstop, on page 102

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 1: 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.