



## Cisco IOS Voice Commands: E

---

This chapter contains commands to configure and maintain Cisco IOS voice applications. The commands are presented in alphabetical order. Some commands required for configuring voice may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice Configuration Guide*.

# e911

To enable E911 system services for SIP on the VoIP dial peer, use the **e911** command in voice service VoIP configuration mode. To disable SIP E911 functionality, use the **no** form of this command.

**e911**

**no e911**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Disabled

**Command Modes** Voice service VoIP (dial peer) configuration mode.

Release	Modification
12.4(9)T	This command was introduced.

**Usage Guidelines** The **no** form of the command disables E911 functionality from a global perspective. Output from the **show running-config** command shows whether E911 is configured. See also the **voice-class sip e911** and **debug csm neat** commands.

**Examples** The following example enables E911 services in voice service VoIP SIP configuration mode:

```
Router# configure terminal
Router(config-term)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# e911
```

The following example disables E911 functionality:

```
Router(conf-serv-sip)# no e911
```

Command	Description
<b>debug csm neat</b>	Turns on debugging for all Call Switching Module (CSM) Voice over IP (VoIP) calls.
<b>show running-config</b>	Displays the current configuration information.
<b>voice-class sip e911</b>	Configures e911 services on the voice dial peer.

# echo-cancel comfort-noise

To specify that background noise be generated, use the **echo-cancel comfort-noise** command in controller configuration mode. To disable this feature, use the **no** form of this command.

**echo-cancel comfort-noise**

**no echo-cancel comfort-noise**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values

**Command Modes** Controller configuration

Command History	Release	Modification
	12.1(2)T	This command was introduced.

**Usage Guidelines** Use the **echo-cancel comfort-noise** command to generate background noise to fill silent gaps during calls if voice activated dialing (VAD) is activated. If comfort noise is not enabled and VAD is enabled at the remote end of the connection, the user hears nothing or silence when the remote party is not speaking.

The configuration of comfort noise affects only the silence generated at the local interface; it does not affect the use of VAD on either end of the connection or the silence generated at the remote end of the connection.

For the OC-3/STM-1 ATM Circuit Emulation Service network module, echo cancellation must be enabled.

**Examples** The following example enables comfort noise on a T1 controller:

```
controller T1 0/0
echo-cancel enable
echo-cancel comfort-noise
```

Related Commands	Command	Description
	<b>echo-cancel enable (controller)</b>	Enables echo cancellation on a voice port.
	<b>voice port</b>	Specifies which port is used for voice traffic.

# echo-cancel compensation

To set attenuation for loud signals, use the **echo-cancel compensation** command in controller configuration mode. To disable this feature, use the **no** form of this command.

**echo-cancel compensation**

**no echo-cancel compensation**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values

**Command Modes** Controller configuration

Command History	Release	Modification
	12.1(2)T	This command was introduced.

**Usage Guidelines** Use the **echo-cancel compensation** command to add attenuation control to the T1 or E1 controller. When this command is enabled, 6 decibels of attenuation are inserted if the signal level from the receive direction is loud. When loud signals are not received, the attenuation is removed.

For the OC-3/STM-1 ATM Circuit Emulation Service network module, echo cancellation must be enabled.

**Examples** The following example enables attenuation control on a T1 controller:

```
controller T1 0/0
 echo-cancel enable
 echo-cancel compensation
```

Related Commands	Command	Description
	<b>echo-cancel enable (controller)</b>	Enables echo cancellation on a voice port.
	<b>voice port</b>	Specifies which port is used for voice traffic.

## echo-cancel coverage

To adjust the size of the echo canceller (EC) and to select the extended EC when the Cisco default EC is present, use the **echo-cancel coverage** command in voice-port configuration mode. To reset this command to the default value (64 ms), use the **no** form of this command.

**echo-cancel coverage { 8 | 16 | 24 | 32 | 48 | 64 }**

**no echo-cancel coverage**

Syntax Description	8	EC size of 8 ms.
	<b>16</b>	EC size of 16 ms.
	<b>24</b>	EC size of 24 ms.
	<b>32</b>	EC size of 32 ms.
	<b>48</b>	EC size of 48 ms.
	<b>64</b>	EC size of 64 ms. This is the default.

**Command Default** 64 ms

**Command Modes** Voice-port configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced on the Cisco 3600 series.
	11.3(1)MA	This command was implemented on the Cisco MC3810.
	12.0(5)XK	The command was modified to add the 8-ms option.
	12.0(5)XE	The command was implemented on the Cisco 7200 series.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
	12.2(13)T	This command was modified to provide a new set of size options when the extended EC is configured. This command is supported on all T1 Digital Signal Processor (DSP) platforms.
	12.3(11)T	This command was modified for use on NextPort platforms for use with the dual-filter G.168 echo canceller.

**Usage Guidelines** Use the **echo-cancel coverage** command to adjust the coverage size of the EC. This command enables cancellation of voice that is sent out the interface and received on the same interface within the configured amount of time. If the local loop (the distance from the interface to the connected equipment that is producing the echo) is greater than this amount of time, the configured value of this command should be increased.

If you configure a greater value for this command, the EC takes longer to converge. In this case, you might hear a slight echo when the connection is initially set up. If the configured value for this command is too short, you might hear some echo for the duration of the call because the EC is not canceling the longer delay echoes.

There is no echo or echo cancellation on the network side (for example, the non-POTS side) of the connection.

**Note**

This command is valid only if the echo cancellation feature has been enabled. For more information, see the **echo-cancel enable** command.

The NextPort dual-filter G.168 echo canceller feature supports echo tails from 8 to 64 ms in 8-ms increments. Use the **echo-cancel coverage** command to limit the echo canceller coverage to 64 ms on NextPort platforms. Tail length values greater than 64 ms are not accepted with the NextPort dual-filter G.168 echo canceller feature. For more information about the NextPort dual0filter G.168 echo canceller, see [NextPort Voice Tuning and Background Noise Statistics with NextPort Dual-Filter G.168 Echo Cancellation](#).

**Examples**

The following example enables the extended echo cancellation feature and adjusts the size of the echo canceller to 16 milliseconds:

```
Router (config-voiceport)# echo-cancel coverage 16
```

**Related Commands**


Command	Description
<b>echo-cancel enable (controller)</b>	Enables echo cancellation on a controller.
<b>echo-cancel enable</b>	Enables echo cancellation on a voice port.

# echo-cancel enable

To enable the cancellation of voice that is sent out the interface and received back on the same interface, use the **echo-cancel enable** command in voice-port configuration mode or global configuration mode. To disable echo cancellation, use the **no** form of this command.

**echo-cancel enable type [hardware | software]**

**no echo-cancel enable**

<b>Syntax Description</b>	<b>hardware</b>	(Optional) Specifies that echo cancellation is enabled via the hardware on the network module.
	<b>software</b>	(Optional) Specifies that echo cancellation is enabled via command-line interface entries.
	<b>Note</b>	The <b>hardware</b> and <b>software</b> keywords are available only when the optional hardware echo cancellation module is installed on the multiflex VWIC.

**Command Default** The Cisco-proprietary G.168 echo canceller (EC) is enabled with the echo suppressor turned off.

**Command Modes** Voice-port configuration  
Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.3(1)T	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. This command is supported on all TI Digital Signal Processor (DSP) platforms.
	12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T and the optional <b>hardware</b> and <b>software</b> keywords were added.

**Usage Guidelines** The **echo-cancel enable** command enables cancellation of voice that is sent out the interface and received back on the same interface; sound that is received back in this manner is perceived by the listener as an echo. Disabling echo cancellation might cause the remote side of a connection to hear an echo. Because echo cancellation is an invasive process that can minimally degrade voice quality, this command should be disabled if it is not needed.

Typically a hybrid circuit can provide greater than 6 decibels (dB) echo return loss (ERL), so the extended EC is configured to handle 6 dB worst case by default. However, if a measurement shows that a circuit can provide only 6 dB ERL or less, the extended EC can be configured to use this lower rate.

The Cisco G.168 EC is enabled by default with the echo suppressor turned off. The echo suppressor can be turned on only when the default Cisco G.168 EC is used. The **echo-cancel suppressor** command used with the Cisco default EC is still visible when the extended EC is selected, but it does not do anything.

The **echo-cancel enable** command does not affect the echo heard by the user on the analog side of the connection.

There is no echo path for a 4-wire receive and transmit interface (also called ear and mouth and abbreviated as E&M). The echo canceller should be disabled for that interface type.

**Note**


---

This command is valid only when the **echo-cancel coverage** command has been configured.

---

**Examples**

The following example enables the extended echo cancellation feature in voice-port configuration mode:

```
Router (config-voiceport)# echo-cancel enable
```

The following example enables the extended echo cancellation feature on the Cisco 1700 series or Cisco ICS7750 in global configuration mode:

```
Router (config)# echo-cancel enable
```

**Related Commands**

Command	Description
<b>echo-cancel coverage</b>	Specifies the amount of coverage for echo cancellation.
<b>echo-cancel enable (controller)</b>	Enables echo cancellation on a controller.
<b>echo-cancel suppressor</b>	Enables echo suppression to reduce initial echo before the echo canceller converges.
<b>non-linear</b>	Enables nonlinear processing in the echo canceler.

## echo-cancel enable (controller)

To enable the echo cancel feature, use the **echo-cancel enable** command in controller configuration mode. To disable this feature, use the **no** form of this command.

**echo-cancel enable**

**no echo-cancel enable**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Enabled for all interface types

**Command Modes** Controller configuration

Command History	Release	Modification
	12.1(2)T	This command was introduced.

**Usage Guidelines** The **echo-cancel enable** command enables cancellation of voice that is sent out of the interface and received back on the same interface. Disabling echo cancellation might cause the remote side of a connection to hear an echo. Because echo cancellation is an invasive process that can minimally degrade voice quality, this command should be disabled if it is not needed.

The **echo-cancel enable** command does not affect the echo heard by the user on the analog side of the connection.



**Note** This command is valid only if the **echo-cancel coverage** command has been configured.

The following example enables the echo cancel feature on a T1 controller:

```
controller T1 0/0
 echo-cancel enable
 echo-cancel coverage 32
```

Related Commands	Command	Description
	<b>echo-cancel coverage</b>	Specifies the amount of coverage for echo cancellation.
	<b>echo-cancel enable</b>	Enables echo cancellation on a voice port.
	<b>non-linear</b>	Enables nonlinear processing in the echo canceler.
	<b>voice port</b>	Configures the voice port.

# echo-cancel erl worst-case

To determine worst-case Echo Return Loss (ERL) in decibels (dB), use the **echo-cancel erl worst-case** command in voice-port configuration mode. To disable the command, use the **no** form.

**echo-cancel erl worst-case {6 | 3 | 0}**

**no echo-cancel erl worst-case {6 | 3 | 0}**

<b>Syntax Description</b>	<b>6   3   0</b>	Values of 6, 3, or 0 dB ERL in the extended echo canceller (EC). The default is 6.
---------------------------	------------------	--

<b>Command Default</b>	Enabled at 6 dB when the extended G.168 EC is used
------------------------	--

<b>Command Modes</b>	Voice-port configuration
----------------------	--------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(13)T	This command was introduced.

<b>Usage Guidelines</b>	This command is used only when the extended EC is present and is not supported with the Cisco proprietary-G.165 EC. This command predicts the worst-case ERL that the EC might encounter.
-------------------------	---

<b>Examples</b>	The following example shows a worst-case ERL of 3:
-----------------	--

```
Router(config-voiceport)# echo-cancel erl worst-case 3
```

To check the configuration, enter the **show voice port** command in privileged EXEC mode:

```
Router# show voice port
.
.
Echo Cancel worst case ERL is set to 6 dB
Playout-delay Mode is set to adaptive
.
.
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
		<b>echo-cancel enable</b>

# echo-cancel loopback

To place the echo cancellation processor in loopback mode, use the **echo-cancel loopback** command in controller configuration mode. To disable loopback of the echo cancellation processor, use the **no** form of this command.

**echo-cancel loopback**

**no echo-cancel loopback**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values

**Command Modes** Controller configuration

Release	Modification
12.1(2)T	This command was introduced.

**Usage Guidelines** Use an **echo-cancel loopback** test on lines to detect and distinguish equipment malfunctions caused by either the line or the interface. If correct echo cancellation is not possible when an interface is in loopback mode, the interface is the source of the problem.

**Examples** The following example sets up echo cancellation loopback diagnostics:

```
controller T1 0/0
echo-cancel enable
echo-cancel coverage 32
echo-cancel loopback
```

Command	Description
<b>echo-cancel enable (controller)</b>	Enables echo cancellation on a controller.

# echo-cancel mode

To enable echo cancel mode on the extended G.168 echo canceller, use the **echo-cancel mode** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

**echo-cancel mode { 1 | 2 }**

**no echo-cancel mode**

Syntax Description	1	2
	Enables fast convergence for multiple echo reflectors and applies 0 dB Sin gain and 0 dB Sout gain.	Enables fast convergence for multiple echo reflectors and improves double-talk detection by applying 6 dB Sin gain and -6 dB Sout gain.

**Command Default** Disabled

**Command Modes** Voice-port configuration

Command History	Release	Modification
	12.3(7)	This command was introduced.

**Usage Guidelines** This command enables an operation mode to improve echo canceller (EC) performance in systems that have multiple echo reflectors and double-talk caused by low volume. When this command is enabled, the extended EC cancels the echo better in multiple echo reflector scenarios, which occur most often in analog interfaces.



**Note**

- This command is available only if the extended G.168 echo canceller is enabled for the voice port.
- If you select mode **2**, set the **echo-cancel erl worst-case** command to 0.

**Examples**

The following example sets the extended G.168 EC mode to 1 on a Cisco 1700 series router:

```
Router(config)# voice-port 1/0/1
Router(config-voiceport)# echo-cancel mode 1
```

Related Commands	Command	Description
	<b>echo-cancel coverage</b>	Adjusts the size of the echo canceller.
	<b>echo-cancel enable</b>	Enables echo cancellation for voice that is sent and received on the same interface.
	<b>echo-cancel erl worst-case</b>	Determines worst-case Echo Return Loss (ERL).

# echo-cancel suppressor

To enable echo suppression to reduce initial echo before the echo canceller converges, use the **echo-cancel suppressor** command in voice-port configuration mode. To disable echo suppression, use the **no** form of this command.

**echo-cancel s uppressor** *seconds*

**no echo-cancel suppressor**

<b>Syntax Description</b>	<i>seconds</i>	Suppressor coverage, in seconds. Range is from 1 to 10. Default is 7.				
<b>Command Default</b>	Disabled					
<b>Command Modes</b>	Voice-port configuration					
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(13)T</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(13)T	This command was introduced.	
Release	Modification					
12.2(13)T	This command was introduced.					
<b>Usage Guidelines</b>	This command is used only when the echo canceller is enabled. In case of double-talk in the first number of seconds, the code automatically disables the suppressor.					
<b>Examples</b>	<p>The following example shows echo suppression configured for a suppression coverage of 9 seconds:</p> <pre>Router(config-voiceport)# <b>echo-cancel suppressor 9</b></pre>					
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>echo-cancel enable</b></td> <td>Enables the cancellation of voice that is sent out and received on the same interface.</td> </tr> </tbody> </table>	Command	Description	<b>echo-cancel enable</b>	Enables the cancellation of voice that is sent out and received on the same interface.	
Command	Description					
<b>echo-cancel enable</b>	Enables the cancellation of voice that is sent out and received on the same interface.					

# element

To define component elements of local or remote clusters, use the **element** command in gatekeeper configuration mode. To disable component elements of local or remote clusters, use the **no** form of this command.

**element** *gatekeeper-name ip-address [port]*

**no element** *gatekeeper-name ip-address [port]*

## Syntax Description

<i>gatekeeper-name</i>	Name of the gatekeeper component to be added to the local or remote cluster.
<i>ip-address</i>	IP address of the gatekeeper to be added to the local or remote cluster.
<i>port</i>	(Optional) Registration, Admission, and Status (RAS) signaling port number for the remote zone. Range is from 1 to 65535. Default is the well-known RAS port number 1719.

## Command Default

No default behavior or values

## Command Modes

Gatekeeper configuration

## Command History

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

## Examples

The following example places the GenevaGK gatekeeper into the specified local or remote cluster:

```
element GenevaGK 172.16.204.158 1719
```

## Related Commands

Command	Description
<b>zone cluster local</b>	Defines a local grouping of gatekeepers, including the gatekeeper that you are configuring.
<b>zone cluster remote</b>	Defines a remote grouping of gatekeepers, including the gatekeeper that you are configuring.

# emptycapability

To eliminate the need for identical codec capabilities for all dial peers in the rotary group, use the **emptycapability** command in h.323 voice-service configuration mode. To return to the default configuration, use the **no** form of this command.

**emptycapability**

**no emptycapability**

**Syntax Description** There are no keywords or arguments for this command.

**Command Default** Identical codec capabilities are required on all dial peers.

**Command Modes** H.323 voice-service configuration mode

Command History	Release	Modification
	12.3(11)T	This command was introduced.

**Usage Guidelines** The default dial-peer configuration requires that all members of a hunt group must have the same codec configured to complete calls. Configuring **emptycapability** on the IP-to-IP gateway (IPIPGW) eliminates the need for identical codec capabilities for all dial peers in the rotary group, and allows the IPIPGW to restart the codec negotiation end-to-end.



**Note**

If extended caps (DTMF or T.38) are configured on the outgoing gateway or the trunking gateway, extended caps must be configured in both places.

**Examples** The following example shows emptycapability being configured to allow the IPIPGW to restart codec negotiation from end-to-end regardless of codec configured on each endpoint:

```
Router(conf-serv-h323)# emptycapability
```

Related Commands	Command	Description
	<b>h323</b>	Enters H.323 voice service configuration mode.

# emulate cisco h323 bandwidth

To instruct the H.323 gateway to use H.323 version 2 behavior for bandwidth management, use the **emulate cisco h323 bandwidth** command in gateway configuration mode. To instruct the gateway to use H.323 version 3 behavior for bandwidth management, use the **no** form of the command.

**emulate cisco h323 bandwidth**

**no emulate cisco h323 bandwidth**

**Syntax Description** This command has no keywords or arguments.

**Command Default** No default behaviors or values

**Command Modes** Gateway configuration

## Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

## Usage Guidelines

Prior to Cisco IOS Release 12.2(2)XA, gateway calls were always reported to require a bandwidth of 64 kbps, the unidirectional bandwidth for a Cisco G.711 codec. If the endpoints in the call chose to use a more efficient codec, this was not reported to the Cisco gatekeeper.

In the version of the Cisco H.323 gateway in Cisco IOS Release 12.2(2)XA or later (which conforms with H.323 version 3), the reported bandwidth is bidirectional. Initially, 128 kbps is reserved. If the endpoints in the call select a more efficient codec, the Cisco gatekeeper is notified of the bandwidth change.

For backward compatibility, the **emulate cisco h323 bandwidth** command allows devices running Cisco IOS Release 12.2(2)XA and later to conform to the H.323 version 2 bandwidth reporting implementation.

## Examples

The following example shows that the router emulates the behavior of a Cisco H.323 Version 2 gateway.

```
Router(config-gateway)# emulate cisco h323 bandwidth
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>bandwidth</b>	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.
<b>bandwidth remote</b>	Specifies the total bandwidth for H.323 traffic between this gatekeeper and any other gatekeeper.
<b>gateway</b>	Enables gateway configuration commands.

# encapsulation atm-ces

To enable circuit emulation service (CES) ATM encapsulation, use the **encapsulation atm-ces** command in interface configuration mode. To disable CES ATM encapsulation, use the **no** form of this command.

**encapsulation atm-ces**

**no encapsulation atm-ces**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values

**Command Modes** Interface configuration

Command History	Release	Modification
	11.3(1)MA	This command was introduced on the Cisco MC3810.
	12.0	This command was integrated into Cisco IOS Release 12.0.

**Usage Guidelines** This command is supported only on serial ports 0 and 1.

**Examples** The following example enables CES ATM encapsulation on serial port 0:

```
interface serial 0
 encapsulation atm-ces
```

Related Commands	Command	Description
	<b>ces cell-loss-integration-period</b>	Sets the CES cell-loss integration period.
	<b>ces clockmode synchronous</b>	Configures the ATM CES synchronous clock mode.
	<b>ces connect</b>	Maps the CES service to an ATM PVC.
	<b>ces initial-delay</b>	Configures the size of the receive buffer of a CES circuit.
	<b>ces max-buf-size</b>	Configures the send buffer of a CES circuit.
	<b>ces partial-fill</b>	Configures the number of user octets per cell for the ATM CES.
	<b>ces service</b>	Configures the ATM CES type.

# encoding h450 call-identity

To set the Abstract Syntax Notation (ASN) Packed Encoding Rules (PER) format used for encoding and decoding the H.450 protocol data units (PDUs), use the **encoding h450 call-identity** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

```
encoding h450 call-identity{ cisco | itu }
```

```
no encoding h450 call-identity
```

Syntax Description	Parameter	Description
	<b>cisco</b>	Gateway uses a PER encoding format that is not compliant with ITU X.691 for encoding or decoding the H.450.2 callIdentity field.
	<b>itu</b>	Gateway uses a PER encoding format that is compliant with ITU X.691 for encoding or decoding the H.450.2 callIdentity field.

**Command Default** Cisco encoding is enabled at the global (voice-service configuration) level.

**Command Modes** Voice-class configuration

Command History	Release	Modification
	12.3(11)T	This command was introduced.
	12.3(7)T3	This command was integrated into Cisco IOS release 12.3(7)T3.

**Usage Guidelines** Use this command to set the encoding format in the voice-class assigned to individual dial peers. By default, Cisco encoding is enabled globally. However, Cisco encoding for the H.450.2 callIdentity field is not compliant with ITU X.691 and can cause interoperability problems with third-party devices during H.450.2 call transfer with consultation. Use the **itu** keyword to configure ITU X.691 encoding in the dial peer.



**Note** This command takes precedence over the **encoding h450 call-identity itu** command in voice-service configuration mode.

**Examples** The following example enables X.691-compliant encoding for the H.450-2 PDUs for calls on dial-peer 4:

```
voice class h323 1
  encoding h450 call-identity itu

dial-peer voice 4 voip
  voice-class h323 1
```

The following example enables Cisco encoding, which is not compliant with ITU X.691, on dial-peer 5:

```
voice class h323 1
  encoding h450 call-identity cisco

dial-peer voice 5 voip
  voice-class h323 1
```

By entering the **no encoding h450 call-identity** command under the voice-class configuration mode, the following example sets the encoding for calls only on dial-peer 7 to reset to the global configuration. However, the **no encoding h450 call-identity** configuration is not displayed in the running configuration:

```
voice class h323 1
  no encoding h450 call-identity

dial-peer voice 7 voip
  voice-class h323 1
```

The following example illustrates a typical use case when the ITU encoding is configured for all the dial peers except dial-peer 4; dial-peer 4 uses Cisco encoding:

```
voice service voip
  h323
  encoding h450 call-identity itu

voice class h323 1
  encoding h450 call-identity cisco

dial-peer voice 1 voip
  destination-pattern 1..

dial-peer voice 2 voip
  destination-pattern 2..

dial-peer voice 3 voip
  destination-pattern 3..

dial-peer voice 4 voip
  destination-pattern 4..
  voice-class h323 1
```

#### Related Commands

Command	Description
<b>encoding h450 call-identity itu</b>	Sets the Abstract Syntax Notation (ASN) Packed Encoding Rules (PER) format used for encoding and decoding the H.450 protocol data units (PDUs).
<b>voice class h323</b>	Enters voice-class configuration mode and creates a voice class for H.323 attributes.

# encoding h450 call-identity itu

To set the Abstract Syntax Notation (ASN) Packed Encoding Rules (PER) format used for encoding and decoding the H.450 protocol data units (PDUs), use the **encoding h450 call-identity itu** command in voice-service configuration mode. To reset to the default, use the **no** form of this command.

**encoding h450 call-identity itu**

**no encoding h450 call-identity**

**Syntax Description** This command has no argument or keywords.

**Command Default** Cisco encoding enabled globally

**Command Modes** Voice-service configuration

Command History	Release	Modification
	12.3(11)T	This command was introduced on Cisco voice gateways.
	12.3(7)T3	This command was integrated into Cisco IOS release 12.3(7)T3.

**Usage Guidelines** Use this command to set ITU X.691 encoding globally on the Cisco voice gateway. By default, Cisco encoding is enabled. However, Cisco encoding for the H.450.2 callIdentity field is not compliant with ITU X.691 and could cause interoperability problems with third-party devices during H.450.2 call transfer with consultation.



**Note** The **encoding h450 call-identity** command in voice-class configuration mode takes precedence over this command.

**Examples** The following example globally configures all dial-peers with the ITU X.691:

```
voice service voip
  h323
  encoding h450 call-identity itu
```

Related Commands	Command	Description
	<b>encoding h45 call-identity</b>	Sets the Abstract Syntax Notation (ASN) Packed Encoding Rules (PER) format used for encoding and decoding the H.450 protocol data units (PDUs).
	<b>voice service voip</b>	Enters voice-service configuration mode.

# encryption

To set the algorithm to be negotiated with the provider, use the **encryption** command in settlement configuration mode. To reset to the default encryption method, use the **no** form of this command.

```
encryption { des-cbc-sha | des40-cbc-sha | dh-des-cbc-sha | dh-des40-cbc-sha | null-md5 |
null-sha | all }
```

```
no encryption { des-cbc-sha | des40-cbc-sha | dh-des-cbc-sha | dh-des40-cbc-sha | null-md5 |
null-sha | all }
```

## Syntax Description

<b>des-cbc-sha</b>	Encryption type ssl_rsa_with_des_cbc_sha cipher suite.
<b>des40-cbc-sha</b>	Encryption type ssl_rsa_export_with_des40_cbc_sha cipher suite.
<b>dh-des-cbc-sha</b>	Encryption type ssl_dh_rsa_with_des_cbc_sha cipher suite.
<b>dh-des40-cbc-sha</b>	Encryption type ssl_dh_rsa_export_with_des40_cbc_sha cipher suite.
<b>null-md5</b>	Encryption type ssl_rsa_with_null_md5 cipher suite.
<b>null-sha</b>	Encryption type ssl_rsa_with_null_sha cipher suite.
<b>all</b>	All encryption methods are used in the Secure Socket Layer (SSL).

## Command Default

The default encryption method is **all**. If none of the encryption methods is configured, the system uses all of the encryption methods in the SSL session negotiation.

## Command Modes

Settlement configuration

## Command History

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

## Usage Guidelines

For Cisco IOS Release 12.0(4)XH1, only one encryption method is allowed for each provider.

## Examples

The following example sets the algorithm to be negotiated with the provider, using the **encryption** command:

```
settlement 0
  encryption des-cbc-sha
```

## Related Commands

Command	Description
<b>connection-timeout</b>	Sets the connection timeout.
<b>customer-id</b>	Sets the customer identification.

Command	Description
<b>device-id</b>	Sets the device identification.
<b>max-connection</b>	Sets the maximum number of simultaneous connections.
<b>response-timeout</b>	Sets the response timeout.
<b>retry-delay</b>	Sets the retry delay.
<b>retry-limit</b>	Sets the connection retry limit.
<b>session-timeout</b>	Sets the session timeout.
<b>settlement</b>	Enters settlement configuration mode.
<b>show settlement</b>	Displays the configuration for all settlement server transactions.
<b>shutdown</b>	Disables the settlement provider.
<b>type</b>	Specifies the provider type.
<b>url</b>	Specifies the ISP address.

# endpoint alt-ep collect

To configure the collection of alternate routes to endpoints, use the **endpoint alt-ep collect** command in gatekeeper configuration mode. To disable alternate route collection, use the **no** form of this command.

**endpoint alt-ep collect** *value* [**distribute**]

**no endpoint alt-ep collect**

Syntax Description	<i>value</i>	Number of alternate routes to endpoints for the gatekeeper to collect before ending the collection process and sending the Location Confirmation (LCF) message to the requesting endpoint. Range for the <i>value</i> argument is from 1 to 20. The default is 0, which indicates that alternate route collection is not enabled.
	<b>distribute</b>	(Optional) Causes the gatekeeper to include alternate routes from as many LCF messages as possible in the consolidated list. Use of this keyword allows the gatekeeper to give fairness to the information of alternate routes present in various LCF messages.
	<b>Note</b>	Identical alternate endpoints are removed from the list. That is, if an alternate endpoint received in an LCF message has an identical IP address or trunk group label or carrier ID as any alternate endpoints received in previous LCF messages, the previous duplicate alternate endpoints are removed from the consolidated list.

**Command Default** The default value for the *value* argument is 0, which indicates that alternate route collection is not enabled.

**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.
	12.2(8)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
	12.2(11)T	Duplicate alternate endpoints received in an LCF message were removed from the consolidated list of endpoints. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

**Usage Guidelines** Use this command to force the gatekeeper to collect a specified number of alternate routes to endpoints and to create a consolidated list of those alternate routes to report back to the requesting endpoint.

---

**Examples**

The following example shows that 15 alternate routes to endpoints should be collected:

```
Router(config-gk)# endpoint alt-ep collect 15
```

---

**Related Commands**

Command	Description
<b>endpoint alt-ep h323id</b>	Configures an alternate endpoint on a gatekeeper, including endpoint ID, IP address, port, and trunk group label or carrier-ID information.
<b>show gatekeeper endpoints alternates</b>	Displays information about alternate endpoints.

---

# endpoint alt-ep h323id

To configure alternate endpoints, use the **endpoint alt-ep h323id** command in gatekeeper configuration mode. To disable alternate endpoints, use the **no** form of this command.

**endpoint alt-ep h323id** *h323-id ip-address* [*port-number*] [**carrier-id** *carrier-name*]

**no endpoint alt-ep h323id**

Syntax Description		
<i>h323-id</i>		H.323 name (ID) of the endpoint for which an alternate address is being supplied. This ID is used by a gateway when the gateway communicates with the gatekeeper. Usually, this H.323 ID is the name given to the gateway, with the gatekeeper domain name appended to the end.
<i>ip-address</i>		IP address of an alternate for this endpoint.
<i>port-number</i>		(Optional) Port number associated with the address of the alternate. Default is 1720.
<b>carrier-id</b> <i>carrier-name</i>		(Optional) Trunk group label or carrier ID of the alternate endpoint. It may be added in addition to the IP address of the alternate endpoint. The <i>carrier-name</i> argument is the name of the trunk group label or circuit ID.

**Command Default** The default port number is 1720.

**Command Modes** Gatekeeper configuration

Command History	Release	Modification
	12.1(5)XM	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
	12.2(2)XB1	This command was implemented on the Cisco AS5850.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and the <b>carrier-id</b> keyword and <i>carrier-name</i> argument were added.

**Usage Guidelines** This command defines the IP address for an alternate endpoint for the primary endpoint identified by its H.323 ID. The IP address is returned in the alternate endpoint field whenever the primary endpoint is returned in an Admission Confirmation (ACF) or Location Confirmation (LCF) message. The alternate endpoint provides an alternate address to which a call can be placed if a call to the primary endpoint fails.

This command provides a failover mechanism if a gateway becomes disabled for a period of time before the gatekeeper becomes aware of the problem. After receiving an ACF message from the gatekeeper with an alternate endpoint list, the Cisco gateway may attempt to use an alternate address if a SETUP message results in no reply from the destination. This command causes the alternate endpoints specified in the *h323-id* argument to be sent in all subsequent ACF and LCF messages. Gatekeepers that support the **endpoint alt-ep h323id** command can also send alternate endpoint information in Registration, Admissions, and Status (RAS) messages. The gatekeeper accepts IP, port call signal address, and trunk

group ID and carrier ID information in endpoint Registration Request (RRQ) messages. The gatekeeper list of alternates for a given endpoint includes the configured alternates and the alternates received in RRQ messages from that endpoint and any alternate endpoints received in incoming RAS LCF messages.

---

**Examples**

The following example shows that the endpoint at 172.16.53.15 1719 has been configured as an alternate for “GW10”. There are no carrier IDs:

```
endpoint alt-ep h323id GW10 172.16.53.15 1719
```

The following example shows that an alternate endpoint list with different carrier IDs (CARRIER\_ABC, CARRIER\_DEF, and CARRIER\_GHI) has been configured for “gwid”:

```
endpoint alt-ep h323id gwid 1.1.1.1 carrier-id CARRIER_ABC
endpoint alt-ep h323id gwid 2.2.2.2 carrier-id CARRIER_DEF
endpoint alt-ep h323id gwid 1.1.1.1 carrier-id CARRIER_GHI
```

---

**Related Commands**

Command	Description
<b>show gatekeeper endpoints</b>	Displays information about alternate endpoints.

## endpoint circuit-id h323id

To associate a circuit with a non-Cisco endpoint or on using a Cisco IOS Release older than that on the gatekeeper, use the **endpoint circuit-id h323id** command in gatekeeper configuration mode. To delete the association, use the **no** form of this command.

**endpoint circuit-id h323id** *endpoint-h323id circuit-id* [**max-calls** *number*]

**no endpoint circuit-id h323id** *endpoint-h323id descriptor* [**max-calls** *number*]

Syntax Description	Parameter	Description
	<i>endpoint-h323id</i>	ID of the H.323 endpoint.
	<i>circuit-id</i>	Circuit assigned to the H.323 endpoint.
	<b>max-calls</b> <i>number</i>	(Optional) Maximum number of calls that this endpoint can handle. Range is from 1 to 10000. There is no default.

**Command Default** No default behavior or values

**Command Modes** Gatekeeper configuration

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

**Usage Guidelines** The **endpoint circuit-id h323id** command allows the gatekeeper and GKTMP server application to work with Cisco gateways that are running non-Cisco gateways or Cisco IOS versions that cannot identify incoming circuits. This command permits only one circuit to be associated with the endpoint.

**Examples** The following example associates a non-Cisco endpoint **first** with a circuit **westcoast**, and assigns a maximum of 2750 calls to the endpoint:

```
Router(config)# gatekeeper
Router(config-gk)# endpoint circuit-id h323-id first westcoast maxcalls 2750
```

Related Commands	Command	Description
	<b>show gatekeeper endpoint circuits</b>	Displays information about all registered endpoints for a gatekeeper.

# endpoint max-calls h323id

To set the maximum number of calls that are allowed for an endpoint, use the **endpoint max-calls h323id** command in gatekeeper configuration mode. To disable the number of calls that are set, use the **no** form of the command.

**endpoint max-calls h323id** *endpoint-h323id maximum-number-of-calls*

**no endpoint max-calls h323id**

Syntax Description		
	<i>endpoint-h323id</i>	H.323 ID of the endpoint.
	<i>maximum-number-of-calls</i>	Maximum number of calls that the endpoint can handle. The value is a number from 1 through 100000.

**Command Default** No default behavior or values

**Command Modes** Gatekeeper configuration

Command History	Release	Modifications
	12.3(1)	This command was introduced.
	12.3(10)	This command was modified to reject the limit set by the endpoints.
	12.3(14)T	This command was modified to reject the limit set by the endpoints.

**Usage Guidelines** You must configure the **endpoint resource-threshold** command and the **arj reject-resource-low** command to start resource monitoring on a gatekeeper before you can configure the **endpoint max-calls h323id** command. The **endpoint resource-threshold** command sets the call capacity threshold of a gateway in the gatekeeper. The **arj reject-resource-low** command allows the endpoint to reject the limit of automatic repeat request message-packet (ARQs) when the endpoint reaches its configured maximum number of calls.

**Examples** The following example shows that the maximum number of calls that GW-1 can handle is 1000.

```
gatekeeper
 endpoint max-calls h323id GW-1 1000
```

Related Commands	Command	Description
	<b>arj reject-resource-low</b>	Enables the gatekeeper to send an admission reject message-packet (ARJ) to the requesting gateway if destination resources are low.
	<b>endpoint resource-threshold</b>	Sets the call capacity threshold of a gateway in the gatekeeper.

# endpoint naming

To customize the T3 endpoint naming convention on a per-MGCP-profile basis, use the **endpoint naming** command in MGCP profile configuration mode. To disable endpoint naming, use the **no** form of this command.

**endpoint naming {t1 | t3}**

**no endpoint naming**

Syntax Description	t1	Flat-T3-endpoint naming convention.
	t3	Hierarchical-T3-endpoint naming convention.

Command Default t1

Command Modes MGCP profile configuration

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

**Usage Guidelines** The option to select between a flat-endpoint naming convention and a hierarchical-T3-endpoint naming convention gives call agents flexibility without enforcing one naming convention. Signaling, backhauling, and trunks using SS7 are supported. T3 naming conventions on XCC signaling types, SS7, and ISDN are not supported.

**Examples** The following example shows the T3 endpoint naming convention on an MGCP profile:

```
Router# configure terminal
Router(config)# mgcp profile default
Router(config-mgcp-profile)# endpoint naming t3
Router(config-mgcp-profile)# end
```

Related Commands	Command	Description
	<b>show mgcp</b>	Displays MGCP configuration information.

# endpoint resource-threshold

To set a gateway's call capacity thresholds in the gatekeeper, use the **endpoint resource threshold** command in gatekeeper configuration mode. To delete the thresholds, use the **no** form of this command.

**endpoint resource-threshold** [**onset** *high-water-mark* | **abatement** *low-water-mark*]

**no endpoint resource-threshold** [**onset** *high-water-mark*] [**abatement** *low-water-mark*]

Syntax Description	onset <i>high-water-mark</i>	(Optional) Maximum call volume usage for the gateway, as a percent. Range is from 1 to 99. The default is 90.
	<b>abatement</b> <i>low-water-mark</i>	(Optional) Minimum call volume usage for the gateway, as a percent. Range is from 1 to 99. The default is 70.

Command Default	High-water-mark: 90 percent Low-water-mark: 70 percent
-----------------	---

Command Modes	Gatekeeper configuration
---------------	--------------------------

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

**Usage Guidelines**

The gatekeeper monitors the call volume in each of its gateways. If the call capacity usage in a particular gateway exceeds the high-water-mark threshold, the gatekeeper stops sending calls to that gateway. When the gateway's active call volume falls below the low-water-mark threshold, the gatekeeper resumes sending new calls to the gateway. These thresholds are global values and affect all gateways registered with a given gatekeeper.

If neither threshold is set, the gatekeeper uses the default values.

**Examples**

The following example sets the high and low call-volume thresholds for all of its gateways:

```
Router(config)# gatekeeper
Router(config-gk)# endpoint resource-threshold onset 85 abatement 65
```

Related Commands	Command	Description
	<b>show gatekeeper endpoint circuits</b>	Displays the information of all registered endpoints for a gatekeeper.

# endpoint ttl

To enable the gatekeeper to assign a time-to-live (TTL) value to the endpoint when it registers with the gatekeeper, use the **endpoint ttl** *command* in gatekeeper configuration mode. To disable the TTL value, use the **no** form of this command.

**endpoint ttl** *time-to-live*

**no endpoint ttl** *time-to-live*

<b>Syntax Description</b>	<i>time-to-live</i>	TTL value, in seconds. Range is from 60 to 3600. The default is 1800.
---------------------------	---------------------	---

<b>Command Default</b>	1800 seconds
------------------------	--------------

<b>Command Modes</b>	Gatekeeper configuration
----------------------	--------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.	
12.2(2)XB1	This command was implemented on the Cisco AS5850.	

<b>Usage Guidelines</b>	This command specifies endpoint registration. Use this command to set the interval that the gatekeeper requires of an endpoint that does not supply its own value. Use a lower value to make the gatekeeper clear the registration of an unresponsive endpoint more quickly.
-------------------------	--

When an endpoint registers with the gatekeeper and does not provide a TTL value, the gatekeeper assigns this value as the time to live. When the TTL expires, the endpoint becomes subject to removal. However, the endpoint is queried a few times in an attempt to communicate with the device. If the device appears active, the registration does not expire. If the device is unresponsive after a few communication attempts, the endpoint is removed.

<b>Examples</b>	The following example enables a time to live value of 60 seconds:
-----------------	---

```
endpoint ttl 60
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>timer cluster-element announce</b>	Specifies the announcement period.
	<b>timer lrq seq delay</b>	Specifies the timer for sequential LRQs.
	<b>timer lrq window</b>	Specifies the window timer for LRQs.

# erase vfc

To erase the Flash memory of a specified voice feature card (VFC), use the **erase vfc** command in privileged EXEC mode.

**erase vfc** *slot*

<b>Syntax Description</b>	<i>slot</i>	Slot on the Cisco AS5300 in which the specified VFC resides. Range is from 0 to 2. There is no default.
<b>Command Default</b>	No default behavior or values	
<b>Command Modes</b>	Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.3(1)MA	This command was introduced on the Cisco AS5300.
<b>Usage Guidelines</b>	Use the <b>erase vfc</b> command to erase the contents of Flash memory for a specified VFC (thereby freeing space in VFC Flash memory) including the default file list and the capability file list.	
<b>Examples</b>	The following example erases the Flash memory on the VFC located in slot 0: Router# <b>erase vfc 0</b>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>delete vfc</b>	Deletes a file from VFC Flash memory.

## error-category

To specify Q.850 cause code mapping, use the **error-category** command in voice cause-code configuration mode. To disable Q.850 cause code mapping, use the **no** form of this command.

**error-category** *number* **q850-cause** *number*

**no error-category** *number* **q850-cause** *number*

Syntax Description	<i>number</i>	Specifies error category value to be mapped to a configured Q850 cause code value. Values range from 128 to 278.
	<b>q850-cause</b> <i>number</i>	Specifies the default Q.850 cause code value. Values range from 1 to 127.

**Command Default** The IEC mechanism defaults to the assigned Q.850 cause codes.

**Command Modes** Voice cause-code configuration

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

**Usage Guidelines** Only the Session Initiation Protocol (SIP) and H.323 subsystems use the category and Q.850 mapping tables to determine the disconnect cause code when releasing a call due to an internal error.

To disable all mappings, use the **no voice cause-code** command. To disable a single mapping, use the **voice cause-code** command, followed by the **no error-category** *number* command.

**Examples** The following example sets error category 128 to map to Q.850 cause code 27:

```
Router(config)# voice cause code
Router(conf-voice-cause)# error-category 128 q850-cause 27
```

The following example defines two mappings for categories 128 and 129:

```
Router(config)# voice cause-code
Router(conf-voice-cause)# error-category 128 q850-cause 27
Router(conf-voice-cause)# error-category 129 q850-cause 38
Router(conf-voice-cause)# exit
```

The following example removes the mapping for category 128 only, leaving 129 defined:

```
Router(config)# voice cause-code
Router(conf-voice-cause)# no error-category 128
Router(conf-voice-cause)# exit
```

The following example removes all configured mappings:

```
Router(config)# no voice cause-code
```

Related Commands	Command	Description
	<b>show voice cause-code</b>	Displays internal error category to q.850 cause code mapping.
	<b>voice cause-code</b>	Enables voice cause-code configuration mode.

## error-correction

To set error correction for the Signaling System 7 (SS7) signaling link when the SS7 Message Transfer Part Layer 2 (MTP2) variant is Bellcore or ITU-white, use the error-correction command in ITU configuration mode. To disable error correction, use the **no** form of this command.

**error-correction** [**basic** / **pcr** [**forced-retransmission** *parameters*]]

**no error-correction**

Syntax Description	
<b>basic</b>	(Optional) Sets SS7 signaling link error correction to basic mode for configurations in which one-way propagation delay is less than 40 ms.
<b>pcr</b>	(Optional) Sets intercontinental SS7 signaling link error correction to Preventive Cyclic Retransmission (PCR) mode for configurations that are transmitted over satellite connections and for configurations in which one-way propagation delay is greater than 40 ms.
<b>forced-retransmission</b>	(Optional) Enables forced retransmission when the <b>pcr</b> keyword is selected. To disable forced retransmission, use the <b>no</b> form of the command.
<i>parameters</i>	(Optional) Sets the error-correction method for an SS7 signaling link. The following types of error correction are configurable: <ul style="list-style-type: none"> <li>• <b>pcr-enabled</b>—Tracks the error-correction method on the SS7 signaling channel. The error-correction method can be either PCR or basic. PCR is disabled by default.</li> <li>• <b>forced-retransmission-enabled</b>—Tracks forced retransmission on the SS7 signaling channel.</li> </ul> <p><b>Note</b> Forced retransmission is enabled only if PCR is enabled.</p> <ul style="list-style-type: none"> <li>• <b>n2 octets</b>—The maximum number of N2 octets that can be queued in the RTB for an SS7 signaling channel before forced retransmission procedures are initiated. The number of octets can range from 200 to 4000. The default is 450.</li> </ul> <p><b>Note</b> This parameter is ignored if forced retransmission is not enabled.</p>

**Command Default** Error correction is set to basic.

**Command Modes** ITU configuration

Command History	Release	Modification
	12.3(2)T	This command was introduced on the Cisco 2600 series, Cisco AS5350, and Cisco AS5400 Cisco signaling link terminals (SLTs).

---

**Usage Guidelines**

The maximum supported signaling link loop (round trip) delay is 670 ms (the time between the sending of a message signal unit [MSU] and the reception of the acknowledgment for this MSU in undisturbed operation).

---

**Examples**

The following example sets the error-correction method to PCR and enables forced retransmission with the N2 parameter set and 1000 octets selected:

```
Router(config-ITU)# error-correction pcr forced-retransmission n2 1000
```

---

**Related Commands**

Command	Description
<b>ss7 mtp2-variant</b>	Configures an SS7 signaling link.

# event-log

To enable event logging for applications, use the **event-log** command in application configuration monitor mode. To disable, use the **no** form of this command.

**event-log**

**no event-log**

**Syntax Description** This command has no arguments or keywords.

**Command Default** By default, event logging is not enabled.

**Command Modes** Application configuration monitor

Command History	Release	Modification
	12.3(14)T	This command was introduced to replace the <b>call application event-log</b> command.

**Usage Guidelines** This command enables event logging globally for all voice applications. To enable or disable event logging for a specific application, use one of the following commands:

**param event-log** (application parameter configuration mode)

**paramspace appcommon event-log** (service configuration mode)



**Note**

To prevent event logging from adversely impacting system resources for production traffic, the gateway uses a throttling mechanism. When free processor memory drops below 20%, the gateway automatically disables all event logging. It resumes event logging when free memory rises above 30%. While throttling is occurring, the gateway does not capture any new event logs even if event logging is enabled. You should monitor free memory and enable event logging only when necessary for isolating faults.

**Examples** The following example shows event logging enabled:

```
application
monitor
event-log
```

Related Commands	Command	Description
	<b>call application event-log</b>	Enables event logging for all voice application instances.
	<b>event-log dump ftp</b>	Enables the gateway to write the contents of the application event log buffer to an external file.
	<b>event-log error-only</b>	Restricts event logging to error events only for application instances.
	<b>event-log max-buffer-size</b>	Sets the maximum size of the event log buffer for each application instance
	<b>param event-log</b>	Enables or disables event logging for a package.
	<b>paramspace appcommon event-log</b>	Enables or disables event logging for a service (application).

## event-log dump ftp

To enable the gateway to write the contents of the application event log buffer to an external file, use the **event-log dump ftp** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

```
event-log dump ftp server[:port]/file username password [encryption-type] password
```

```
no event-log dump ftp
```

### Syntax Description

<i>server</i>	Name or IP address of FTP server where file is located.
<i>port</i>	(Optional) Specific port number on server.
<i>file</i>	Name and path of file.
<i>username</i>	Username required to access file.
<i>encryption-type</i>	(Optional) The Cisco proprietary algorithm used to encrypt the password. Values are 0 or 7. To disable encryption enter 0; to enable encryption enter 7. If you specify 7, you must enter an encrypted password (a password already encrypted by a Cisco router).
<i>password</i>	Password required to access file.

### Command Default

By default, this feature is not enabled on the gateway.

### Command Modes

Application configuration monitor

### Command History

Release	Modification
12.3(14)T	This command was introduced to replace the <b>call application event-log dump ftp</b> command.

### Usage Guidelines

This command enables the gateway to automatically write the event log buffer to the named file either after an active application instance terminates or when the event log buffer becomes full. The default buffer size is 4 KB. To modify the size of the buffer, use the **event-log max-buffer-size** command in application configuration monitor mode.

Enabling the gateway to write event logs to FTP could adversely impact gateway memory resources in some scenarios, for example, when:

- The gateway is consuming high processor resources and FTP does not have enough processor resources to flush the logged buffers to the FTP server.
- The designated FTP server is not powerful enough to perform FTP transfers quickly
- Bandwidth on the link between the gateway and the FTP server is not large enough
- The gateway is receiving a high volume of short-duration calls or calls that are failing

You should enable FTP dumping only when necessary and not enable it in situations where it might adversely impact system performance.

**Examples**

The following example enables the gateway to write application event logs to an external file named `app_elogs.log` on a server named `ftp-server`:

```
application
monitor
 event-log dump ftp ftp-server/elems/app-elems.log username myname password 0 mypass
```

The following example specifies that application event logs are written to an external file named `app_elogs.log` on a server with the IP address of `10.10.10.101`:

```
application
monitor
 event-log dump ftp 10.10.10.101/elems/app-elems.log username myname password 0 mypass
```

**Related Commands**

Command	Description
<b>call application event-log dump ftp</b>	Enables the gateway to write the contents of the application event log buffer to an external file.
<b>event-log</b>	Enables event logging for applications.
<b>event-log error-only</b>	Restricts event logging to error events only for application instances.
<b>event-log max-buffer-size</b>	Sets the maximum size of the event log buffer for each application instance.

# event-log error-only

To restrict event logging to error events only for application instances, use the **event-log error-only** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

**event-log error-only**

**no event-log error-only**

**Syntax Description** This command has no arguments or keywords.

**Command Default** If logging is enabled, all application events are logged.

**Command Modes** Application configuration monitor

## Command History

Release	Modification
12.3(14)T	This command was introduced to replace the <b>call application event-log error-only</b> command.

## Usage Guidelines

- This command limits new event logging to error events only; it does not enable logging.

You must use this command with either the **event-log** command, which enables event logging for all voice applications, or enable event logging for a specific application using the **param event-log** command (package appcommon configuration mode) or the **paramspace appcommon event-log** command (service configuration mode).

- Any events logged before this command is issued are not affected.

## Examples

The following example enables event logging for error events only:

```
application
monitor
  event-log
  event-log error-only
```

## Related Commands

Command	Description
<b>call application event-log error-only</b>	Restricts event logging to error events only for application instances.
<b>event-log</b>	Enables event logging for applications.

Command	Description
<b>event-log dump ftp</b>	Enables the gateway to write the contents of the application event log buffer to an external file.
<b>event-log max-buffer-size</b>	Sets the maximum size of the event log buffer for each application instance

# event-log max-buffer-size

To set the maximum size of the event log buffer for each application instance, use the **event-log max-buffer-size** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

**event-log max-buffer-size** *kbytes*

**no event-log max-buffer-size**

<b>Syntax Description</b>	<i>kbytes</i>	Maximum buffer size, in kilobytes. Range is 1 to 50. Default is 4 KB.
---------------------------	---------------	---

<b>Command Default</b>	By default, the maximum size is set to 4 KB.
------------------------	--

<b>Command Modes</b>	Application configuration monitor
----------------------	-----------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(14)T	This command was introduced to replace the <b>call application event-log max-buffer-size</b> command.

**Usage Guidelines**

If the event log buffer reaches the limit set by this command, the gateway allocates a second buffer of equal size. The contents of both buffers is displayed when you use the **show call application session-level** command. When the first event log buffer becomes full, the gateway automatically appends its contents to an external FTP location if the **event-log dump ftp** command is used.

A maximum of two buffers are allocated for an event log. If both buffers are filled, the first buffer is deleted and another buffer is allocated for new events (buffer wraps around). If the **event-log dump ftp** command is configured and the second buffer becomes full before the first buffer is dumped, event messages are dropped and are not recorded in the buffer.



**Note**

- Do not set the maximum buffer size to more than you need for a typical application session. After an active session terminates, the amount of memory used by the buffer is allocated to the history table and is maintained for the length of time set by the **history session retain-timer** command. Also consider that most fatal errors are captured at the end of an event log.
- To conserve memory resources, write the event log buffer to FTP by using the **event-log dump ftp** command.

**Examples**

The following example sets the application event log buffer to 8 KB:

```
application
monitor
event-log max-buffer-size 8
```

Related Commands	Command	Description
	<b>event-log</b>	Enables event logging for applications.
	<b>event-log dump ftp</b>	Enables the gateway to write the contents of the application event log buffer to an external file.
	<b>call application event-log max-buffer-size</b>	Maximums size of the event log buffer for each application instance.

# expect-factor

To set the expect-factor value for voice quality, which affects the threshold calculated planning impairment factor (ICPIF) loss/delay busyout value, use the **expect-factor** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

**expect-factor** *value*

**no expect-factor** *value*

<b>Syntax Description</b>	<i>value</i>	Integers that represent quality of voice as described in ITU G.107. Range: 0 to 20, with 0 representing toll quality. Default: 10.
---------------------------	--------------	--

<b>Command Default</b>	10
------------------------	----

<b>Command Modes</b>	Dial peer configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.3(1)T	This command was introduced on the Cisco 3600 series.
12.2(8)T	The <i>value</i> default changed from 10 to 0.	
12.3(3)T	The <i>value</i> default changed from 0 to 10.	

**Usage Guidelines** The expect factor impacts the calculated value of ICPIF. This value is used in conjunction with Simple Network Management Protocol (SNMP) to generate a trap when voice quality falls below a configured value. It also impacts the value of ICPIF reported in call-account records as well as in call-history values on the gateway.

Use this and related commands together on a dial peer as follows:

- Use this command to set the expect-factor value.
- Use the **icpif** command to set a threshold ICPIF value (the ICPIF calculation uses the expect-factor value as well as values for loss and delay).
- Use the **snmp enable peer-trap poor-qov** command to generate notifications in the form of SNMP traps to the network manager for calls whose ICPIF value exceeds the threshold.



**Note** For more information on ICPIF, see *IP SLAs—Analyzing VoIP Service Levels Using the VoIP Jitter Operation* at [http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsla\\_c/hsvoipl.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsla_c/hsvoipl.htm)

**Examples** The following example sets the expect factor for a dial peer:

```
dial-peer voice 10 voip
  expect-factor 0
```

Related Commands	Command	Description
	<b>icpif</b>	Specifies the ICPIF threshold for calls sent by a dial peer.
	<b>snmp enable peer-trap poor-qov</b>	Generates poor-quality-of-voice notifications for applicable calls associated with a VoIP dial peer.

# extsig mgcp

To configure external signaling control by Media Gateway Control Protocol (MGCP) for a T1 or E1 trunk controller card, use the **extsig mgcp** command in controller configuration mode. To discontinue MGCP control for this controller, use the **no** form of this command.

**extsig mgcp**

**no extsig mgcp**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values

**Command Modes** Controller configuration

## Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

**Usage Guidelines** For T3 lines, each logical T1 trunk controller card must be configured using the **extsig mgcp** command.

## Examples

The following example shows MGCP signaling control being configured for T1 controller 7/0:

```
controller T1 7/0
 framing esf
 extsig mgcp
 guard-timer 10 on-expiry reject
 linecode b8zs
 ds0-group 1 timeslots 1-24 type none service mgcp
```

## Related Commands

Command	Description
<b>dialer extsig</b>	Configures an interface to initiate and terminate calls using an external signaling protocol.