



Cisco IOS Voice Commands:

A

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*.

aaa nas port voip

To send out the standard NAS-Port attribute (RADIUS IETF Attribute 5) on voice interfaces, use the **aaa nas port voip** command in global configuration mode. To disable the command, use the **no** form of the command.

aaa nas port voip

no aaa nas port voip

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco AS5300.

Usage Guidelines

This command brings back the original behavior of the AAA NAS-Port on Voice over IP (VoIP) interfaces. By default this feature should not be enabled.



Note

Some customers using the Cisco AS5300 voice gateway have had the Debit Card application stop working after upgrading from 12.1(5)T to 12.1(5.3)T.

Examples

The following example shows how to return to the original behavior of the AAA NAS-Port:

```
aaa nas port voip
```

Related Commands

Command	Description
aaa nas port extended	Replaces the NAS-port attribute with RADIUS IETF attribute 26 and displays extended field information.

aaa username

To determine the information with which to populate the username attribute for AAA billing records, use the **aaa username** command in SIP user agent configuration mode. To achieve default capabilities, use the **no** form of this command.

```
aaa username {calling-number | proxy-auth}
```

```
no aaa username
```

Syntax Description

calling-number	Uses the FROM: header in the SIP INVITE (default value). This keyword is used in most implementations.
proxy-auth	Parses the Proxy-Authorization header. Decodes the Microsoft Passport user ID (PUID) and password, and then populates the PUID into the username attribute and a "." into the password attribute. The username attribute is used for billing, and the "." is used for the password, because the user has already been authenticated before this point.

Defaults

calling-number

Command Modes

SIP user agent configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco AS5300, Cisco AS5350 and the Cisco AS5400.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(11)T	This command was integrated Cisco IOS Release 12.2(11)T and was implemented on the Cisco AS5850. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800 in this release.

Usage Guidelines

Parsing the Proxy-Authorization header, decoding the PUID and password, and populating the username attribute with the PUID must be enabled through this command. If this command is not issued, the Proxy-Authorization header is ignored.

The keyword **proxy-auth** is a nonstandard implementation, and Session Initiation Protocol (SIP) gateways do not normally receive or process the Proxy-Authorization header.

Examples

The following example enables the processing of the SIP username from the Proxy-Authorization header:

```
Router(config)# sip-ua  
Router(config-sip-ua)# aaa username proxy-auth
```

Related Commands

Command	Description
show call active voice	Shows active call information for voice calls or fax transmissions in progress.
show call history voice	Displays the voice call history table.

access-code (cm-fallback)

To configure trunk access codes for each type of line so that the Cisco IP phones can access the trunk lines only during Cisco CallManager fallback mode when Survivable Remote Site (SRS) Telephony feature is enabled, use the **access-code** command in call-manager-fallback configuration mode. To remove the telephone access code configuration from the Cisco IP phones, use the **no** form of this command.

access-code {fxo | e&m} *dial-string*

no access-code {fxo | e&m} *dial-string*

access-code {bri | pri} *dial-string* [**direct-inward-dial**]

no access-code {bri | pri} *dial-string* [**direct-inward-dial**]

Syntax	Description
fxo	Enables a foreign exchange office (FXO) interface.
e&m	Enables an analog ear and mouth (E&M) interface.
<i>dial-string</i>	Sets up dial access codes for each specified line type by creating dial peers.
bri	Enables a Basic Rate Interface (BRI).
pri	Enables a Primary Rate Interface (PRI).
direct-inward-dial	(Optional) Enables direct-inward-dial on an access code plain old telephone service (POTS) dial peer.

Defaults No default behavior or values

Command Modes Call-manager-fallback configuration

Command History	Release	Modification
	12.1(5)YD	This command was introduced on the Cisco 2600 series and Cisco 3600 series multiservice routers, and Cisco IAD2420 series IADs.
	12.2(2)XT	This command was implemented on Cisco 1750 and Cisco 1751.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 3725, Cisco 3745, and Cisco MC3810-V3.
	12.2(8)T1	This command was implemented on the Cisco 2600-XM and Cisco 2691.
	12.2(11)T	This command was implemented on the Cisco 1760.

Usage Guidelines

The **access-code** command configures trunk access codes for each type of line—BRI, E&M, FXO, and PRI—so that the Cisco IP phones can access the trunk lines in Cisco CallManager fallback mode when the SRS Telephony feature is enabled. This provides system-wide access.

**Note**

The **access-code** command creates temporary dial peers in Cisco CallManager fallback mode. In many cases, you may already have the local PSTN ports configured with appropriate access codes provided by dial peers (for example, dial 9 to select a FXO PSTN line), in which case this command is not needed.

The **access-code** command creates temporary POTS voice dial peers for all the selected types of voice-ports, during Cisco CallManager fallback mode. Use this command only if your normal network dial-plan configuration prevents you from configuring permanent POTS voice dial peers to provide trunk access for use in the fallback mode. When the **access-code** command is used, it is important to ensure that all ports covered by the command have valid trunk connections. Selection between ports for outgoing calls is random.

The dial string is used to set up temporary dial peers for each specified line type. If there are multiple lines of the same type, a dial peer is set up for each line. The dial peers are active only during Cisco CallManager fallback mode when the SRS Telephony feature is enabled. The result of this configuration is that all PSTN interfaces of the same type, for example BRI, are treated as equivalent, and any port may be selected to place the outgoing PSTN call. The **direct-inward-dial** keyword enables you to set direct-inward-dial access for PRI and BRI trunk lines.

Examples

The following example sets the **access-code** command for BRI 8:

```
Router(config)# call-manager-fallback
Router(config-cm-fallback)# access-code bri 8 direct-inward-dial
```

The following example sets the **access-code** command for E&M 8:

```
Router(config)# call-manager-fallback
Router(config-cm-fallback)# access-code e&m 8
```

The following example sets the **access-code** command for FXO 9:

```
Router(config)# call-manager-fallback
Router(config-cm-fallback)# access-code fxo 9
```

The following example sets the **access-code** command for PRI 9:

```
Router(config)# call-manager-fallback
Router(config-cm-fallback)# access-code pri 9 direct-inward-dial
```

Related Commands

Command	Description
call-manager-fallback	Enables SRS Telephony feature support and enters call-manager-fallback configuration mode.

access-list (voice source-group)

To assign an IOS access list to a voice source group, use the **access-list** command in voice source-group configuration mode. To delete the access list, use the **no** form of this command.

access-list *access-list-number*

no access-list *access-list-number*

Syntax Description

access-list-number Number of an access list. The range is from 1 to 99.

Note Other versions of this command permit access-list-numbers from 1300 to 1999.

Defaults

No default behavior or values

Command Modes

Voice source-group configuration

Command History

Release	Modification
12.2(11)T	This command was introduced in voice source group configuration mode.

Usage Guidelines

An access list defines a range of IP addresses for incoming calls that require additional scrutiny. Two related commands are used for voice source groups:

- Use the **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**] command in global configuration mode to define the contents of the access list.
- Use the **access-list** *access-list-number* command in voice source-group configuration mode to assign the defined access list to the voice source group.

The terminating gateway uses the source IP group to identify the source of the incoming VoIP call before selecting an inbound dial peer. If the source is found in the access list, then the call is accepted or rejected, depending on how the access list is defined.

The terminating gateway uses the access list to implement call blocking. If the call is rejected, the terminating gateway returns a disconnect cause to the source. Use the **disconnect-cause** command to specify a disconnect cause to use for rejected calls.

Use the **show access-lists** EXEC command to display the contents of all access lists.

Use the **show ip access-list** EXEC command to display the contents of one access list.

Examples

The following example assigns access list 1 to voice source-group alpha. Access list 1 was defined previously using another command. An incoming source IP group call is checked against the conditions defined for access list 1 and is processed based on the permit or deny conditions of the access list.

```
Router(config)# voice source-group alpha
Router(cfg-source-grp)# access-list 1
```

Related Commands	Command	Description
	carrier-id (dial-peer)	Specifies the carrier as the source of incoming VoIP calls (for carrier ID routing).
	disconnect-cause	Specifies a cause for blocked calls.
	h323zone-id (voice source group)	Associates a zone for an incoming H.323 call.
	show access-lists	Displays the contents of all access lists.
	show ip access-list	Displays the contents of one access list.
	translation-profile (source group)	Associates a translation profile with incoming source IP group calls.
	trunk-group-label (voice source group)	Specifies the trunk group as the source of incoming VoIP calls (for trunk group label routing).
	voice source-group	Initiates the source IP group profile definition.

access-policy

To require that a neighbor be explicitly configured in order for requests to be accepted, use the **access-policy** command in Annex G configuration mode. To reset the configuration to accept all requests, use the **no** form of this command.

access-policy [**neighbors-only**]

no access-policy

Syntax Description	neighbors-only (Optional) Requires that a neighbor be configured.						
Defaults	Border elements accept any and all requests if service relationships are not configured.						
Command Modes	Annex G Configuration						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(11)T</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(11)T	This command was introduced.		
Release	Modification						
12.2(11)T	This command was introduced.						
Usage Guidelines	Border elements accept any and all requests if service relationships are not configured. The access-policy command eliminates arbitrary requests from unknown border elements, and is a required prerequisite for configuring service relationships.						
Examples	<p>The following example shows how to enable the service relationship between border elements:</p> <pre>Router(config-annexg)# access-policy neighbors-only</pre>						
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>call-router</td> <td>Enables the Annex G border element configuration commands.</td> </tr> <tr> <td>domain-name</td> <td>Sets the domain name reported in service relationships.</td> </tr> </tbody> </table>	Command	Description	call-router	Enables the Annex G border element configuration commands.	domain-name	Sets the domain name reported in service relationships.
Command	Description						
call-router	Enables the Annex G border element configuration commands.						
domain-name	Sets the domain name reported in service relationships.						

accounting method

To set an accounting method at login for calls that come into a dial peer, use the **accounting method** command in voice class AAA configuration mode. To disable the accounting method set at login, use the **no** form of this command.

accounting method *MethListName* [out-bound]

no accounting method *MethListName* [out-bound]

Syntax Description

<i>MethListName</i>	Defines an accounting method list name.
out-bound	(Optional) Defines the outbound leg.

Defaults

When this command is not used to specify an accounting method, the system uses the **aaa accounting connection h323** command as the default. If the method list name is not specified, the outbound call leg uses the same method list name as the inbound call leg.

Command Modes

Voice class AAA configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

- This command sets the accounting method for dial peers in voice class AAA configuration mode. To initially define a method list, refer to the *Cisco IOS Security Configuration Guide*, Release 12.2.
- If the outbound option is specified, the outbound call leg on the dial peer uses the method list name specified in the command.
- If the method list name is not specified, by default, the outbound call leg uses the same method list name as the inbound call leg.

Examples

The following example sets the dp-out method for the outbound leg:

```
voice class aaa 1
  accounting method dp-out out-bound
```

Related Commands

Command	Description
voice class aaa	Enables dial-peer-based VoIP AAA configurations.
aaa accounting connection h323	Defines the accounting method list H.323 with RADIUS, using stop-only or start-stop accounting options.

accounting suppress

To disable accounting that is automatically generated by a service provider module for a specific dial peer, use the **accounting suppress** command in voice class AAA configuration mode. To allow accounting to be automatically generated, use the **no** form of this command.

accounting suppress [**in-bound** | **out-bound**]

no accounting suppress [**in-bound** | **out-bound**]

Syntax Description

in-bound	(Optional) Defines the call leg for incoming calls.
out-bound	(Optional) Defines the call leg for outbound calls.

Defaults

Accounting is automatically generated by the service provider module.

Command Modes

Voice class AAA configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

- If a call leg option is not specified by the command, accounting is disabled for both inbound and outbound calls.
- For accounting to be automatically generated in the service provider module, you must first configure **gw-accounting aaa** command in global configuration mode before configuring dial-peer-based accounting in voice class AAA configuration mode.

Examples

In the example below, accounting is suppressed for the incoming call leg.

```
voice class aaa 1
  accounting suppress in-bound
```

Related Commands

Command	Description
gw-accounting aaa	Enables VoIP gateway accounting.
suppress	Turns off accounting for a call leg on a POTS or VoIP dial peer. This command is used in gw-accounting aaa configuration mode.
voice class aaa	Enables dial-peer-based VoIP AAA configurations.

accounting template

To allow each dial peer to choose and send a customized accounting template to the RADIUS server, use the **accounting template** command in voice class AAA configuration mode. To disable the dial peer from choosing and sending a customized accounting template, use the **no** form of this command.

accounting template *acctTempName* [**out-bound**]

no accounting template *acctTempName* [**out-bound**]

Syntax Description

<i>acctTempName</i>	Defines an accounting template name.
out-bound	(Optional) Defines the outbound leg.

Defaults

The dial peer does not choose and send a customized accounting template to the RADIUS server.

Command Modes

Voice class AAA configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

- Use this command to search for new VSAs in the voice accounting record. Use the **show call accounting template master** command to get a complete list of VSAs.
- This command overrides the **acct-template** command in gateway accounting AAA configuration mode when a customized accounting template is used.
- If you use a Tool Command Language (TCL) script, the TCL verb **aaa accounting start [-t acctTempName]** takes precedence over the **accounting template** command in voice class AAA configuration mode.

Refer to the [RADIUS VSA Voice Implementation Guide](#) for more information about accounting templates.

Examples

The following example sets the template temp-dp for the outbound leg

```
voice class aaa 1
  accounting template temp-dp out-bound
```

Related Commands

Command	Description
acct-template	Sends a selected group of voice accounting VSAs.
show call accounting template master	Displays a list of all available VSAs in the voice accounting record.
voice class aaa	Enables dial-peer-based VoIP AAA configurations.

acc-qos

To define the acceptable quality of service (QoS) for any inbound and outbound call on a Voice over IP (VoIP) dial peer, use the **acc-qos** command in dial peer configuration mode. To restore the default QoS setting, use the **no** form of this command.

acc-qos { **best-effort** | **controlled-load** | **guaranteed-delay** }

no acc-qos

Syntax Description

best-effort	Indicates that Resource Reservation Protocol (RSVP) makes no bandwidth reservation. This is the default.
controlled-load	Indicates that RSVP guarantees a single level of preferential service, presumed to correlate to a delay boundary. The controlled load service uses admission (or capacity) control to ensure that preferential service is received even when the bandwidth is overloaded.
guaranteed-delay	Indicates that RSVP reserves bandwidth and guarantees a minimum bit rate and preferential queueing if the bandwidth reserved is not exceeded.

Defaults

best-effort

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series routers.
12.1(5)T	The description of the command was modified.

Usage Guidelines

This command is applicable only to VoIP dial peers.

When VoIP dial peers are used, the Cisco IOS software uses RSVP to reserve a certain amount of bandwidth so that the selected QoS can be provided by the network. Call setup is aborted if the RSVP resource reservation does not satisfy the acceptable QoS for both peers.

To select the most appropriate value for this command, you need to be familiar with the amount of traffic this connection supports and what kind of impact you are willing to have on it. The Cisco IOS software generates a trap message when the bandwidth required to provide the selected quality of service is not available.

Examples

The following example selects **guaranteed-delay** as the acceptable QoS for inbound and outbound calls on VoIP dial peer 10:

```
dial-peer voice 10 voip
  acc-qos guaranteed-delay
```

Related Commands	Command	Description
	req-qos	Requests a particular QoS using RSVP to be used in reaching a specified dial peer in VoIP.

acct-template

To send a selected group of voice accounting vendor-specific attributes (VSAs), use the **acct-template** command in gateway accounting AAA configuration mode. To disable sending that selected group of voice accounting VSAs, use the **no** form of this command.

```
acct-template { callhistory-detail | acctTemplateName }
```

```
no acct-template { callhistory-detail | acctTemplateName }
```

Syntax Description

<i>acctTemplateName</i>	Name of the custom accounting template created by deleting unwanted attributes.
callhistory-detail	Sends all voice attributes for accounting.

Defaults

No voice accounting VSAs are sent.

Command Modes

Gateway accounting AAA configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

- If you do not want to create a custom template, use the **callhistory-detail** keyword to send all voice VSAs to the accounting server. These voice VSAs consist of the VSAs introduced in Cisco IOS releases up to Cisco IOS Release 12.2(11)T. Refer to the *RADIUS Vendor-Specific Attributes Voice Implementation Guide* for the current list of attributes.
- Use the **acct-template** command with the name of the template to send only those voice VSAs that are defined in the accounting template. The accounting template is a text file that you can create by selecting specific VSAs that are applicable to your billing needs. You must first use the **call accounting-template voice** command to define your accounting template before using the **acct-template** command. refer to the *RADIUS Vendor-Specific Attributes Voice Implementation Guide* for the latest list of attributes.
- When you send only those VSAs defined in your accounting template, the default call-history records that are created by the service provider are automatically suppressed.

Examples

In the example below, the **acct-template** command is used to specify temp-glob, a custom template.

```
gw-accounting aaa

acct-template temp-glob
```

Related Commands	Command	Description
	call accounting-template voice	Defines and applies a customized template.
	gw-accounting aaa	Enables VoIP gateway accounting.
	show call accounting template master	Displays a list of all available VSAs in the voice accounting record.
	show call accounting-template voice	Displays VSAs sent through accounting templates.

address-family

To set the global address family to be used on all dial peers, use the **address-family** command in TGREP configuration mode. To change back to the default address family, use the **no** form of this command.

address family {**e164** | **decimal** | **penta-decimal**}

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

Syntax Description		
	e164	E.164 address family.
	decimal	Digital address family
	penta-decimal	Pentadecimal address family

Defaults E.164 address family

Command Modes TGREP configuration

Command History	Release	Modification
	12.3(1)	This command was introduced.

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

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

Examples The following example shows that the address family for ITAD 1234 is set for E.164 addresses:

```
Router(config)# tgrep local-itad 1234
Router(config-tgrep)# address family e164
```

Related Commands	Command	Description
	tgrep local-itad	Enters TGREP configuration mode and defines an ITAD.

admin-password (telephony-service)

To set a password for the local system administrator of the Cisco IOS Telephony Service router, use the **admin-password** command in telephony-service configuration mode. To disable the password, use the **no** form of this command.

admin-password *password*

no admin-password *password*

Syntax Description

password Password used by the administrator to prevent unauthorized access to the Cisco IOS Telephony Service router or Cisco IP phone configuration.

Defaults

No default behavior or values

Command Modes

Telephony-service configuration

Command History

Release	Modification
12.2(2)XT	This command was introduced on the Cisco 1750, Cisco 1751, Cisco 2600 series, Cisco 3600 series multiservice routers, and Cisco IAD2420 series IADs.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 3725, Cisco 3745, and Cisco MC3810-V3.
12.2(8)T1	This command was implemented on the Cisco 2600-XM and Cisco 2691.
12.2(11)T	This command was implemented on the Cisco 1760.

Usage Guidelines

The **admin-password** command sets a password for the local system administrator to prevent unauthorized access to the Cisco IOS Telephony Service router or Cisco IP phone configuration. The specific password for the local system administrator is associated with the username set with the **admin-username** command. The password and the username for the local system administrator, as a pair, are associated with a specific Cisco IP phone.



Note

The password and username are used from the graphical user interface (GUI) for the Cisco IOS Telephony Service administration.

Examples

The following example shows how to set the password U2021 for a local administrator:

```
Router(config)# telephony-service
Router(config-telephony-service)# admin-password U2021
```

■ **admin-password (telephony-service)**

Related Commands	Command	Description
	admin-username (telephony-service)	Sets the username for the local system administrator of the Cisco IOS Telephony Service router.
	telephony-service	Enables Cisco IOS Telephony Service and enters telephony-service configuration mode.
	username (ephone)	Assigns a phone user login account username and password to permit user login to the Cisco IOS Telephony Service router through a web browser.

admin-username (telephony-service)

To set the username for the local system administrator of the Cisco IOS Telephony Service router, use the **admin-username** command in telephony-service configuration mode. To disable the username, use the **no** form of this command.

admin-username *username*

no admin-username *username*

Syntax Description

<i>username</i>	Assigned username for the administrator to prevent unauthorized access to the Cisco IOS Telephony Service router or Cisco IP phone configuration. The default is Admin.
-----------------	---

Defaults

The default username is Admin

Command Modes

Telephony-service configuration

Command History

Release	Modification
12.2(2)XT	This command was introduced on the Cisco 1750, Cisco 1751, Cisco 2600 series, Cisco 3600 series multiservice routers, and Cisco IAD2420 series IADs.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 3725, Cisco 3745, and Cisco MC3810-V3.
12.2(8)T1	This command was implemented on the Cisco 2600-XM and Cisco 2691.
12.2(11)T	This command was implemented on the Cisco 1760.

Usage Guidelines

The **admin-username** command sets the username for the local system administrator of the Cisco IOS Telephony Service router to prevent unauthorized access to the router or Cisco IP phone configuration. The specific username of the local administrator is associated with the password set with the **admin-password** command. The username and password for the local system administrator, as a pair, are associated with a specific Cisco IP phone.



Note

The username and password are used from the graphical user interface (GUI) for the Cisco IOS Telephony Service administration.

Examples

The following example sets the username “ssmith” for a local administrator:

```
Router(config)# telephony-service
Router(config-telephony-service)# admin-username ssmith
```

■ **admin-username (telephony-service)**

Related Commands	Command	Description
	admin-password (telephony-service)	Sets a password for the local system administrator of the Cisco IOS Telephony Service.
	telephony-service	Enables Cisco IOS Telephony Service and enters telephony-service configuration mode.
	username (ephone)	Assigns a phone user login account username and password to permit user login to the Cisco IOS Telephony Service router through a web browser.

advertise (annex g)

To control the types of descriptors that the border element (BE) advertises to its neighbors, use the **advertise** command in Annex G configuration mode. To reset this command to the default value, use the **no** form of this command.

advertise [**static** | **dynamic** | **all**]

no advertise

Syntax Description	static	(Optional) Only the descriptors provisioned on this BE is advertised. This is the default.
	dynamic	(Optional) Only dynamically learned descriptors is advertised.
	all	(Optional) Both static and dynamic descriptors is advertised.

Defaults Static

Command Modes Annex G configuration

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

Examples The following example configures a BE that advertises both static and dynamic descriptors to its neighbors:

```
Router(config)# call-router h323-annexg be20
Router(config-annexg)# advertise all
```

Related Commands	Command	Description
	call-router	Enables the Annex G border element configuration commands.
	show call history	Displays the routes stored in cache for the BE.
	show call-router status	Displays the Annex G BE status.

advertise (tgrep)

To turn on reporting for a specified address family, use the **advertise** command in TGREP configuration mode. To turn off reporting for a specified address family, use the **no** form of this command.

```
advertise {e164 | decimal | penta-decimal }[csr][ac][tc][trunk-group | carrier]
```

```
advertise {trunk-group | carrier}[csr][ac][tc]
```

```
no advertise {e164 | decimal | penta-decimal | trunk-group | carrier}
```

Syntax Description

e164	E.164 address family.
decimal	Decimal address family
penta-decimal	Penta-decimal address family (what is this?)
trunk-group	Trunk group address family
carrier	Carrier code address family
csr	Call success rate
ac	Available circuits
tc	Total circuits

Defaults

No attributes for address families are advertised.

Command Modes

TGREP configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

If you specify **e164**, **decimal** or **penta-decimal** for the address family, you can stipulate whether the related **carrier** or **trunk-group** parameters are advertised. If you stipulate **carrier** or **trunk-group** for the address family, you can stipulate that the related address family prefix is advertised. If you stipulate **carrier** or **trunk-group** for the address family, you cannot stipulate **carrier** or **trunk-group** attributes for advertising.

When the **no** version of this command is used, it turns off the advertisement of that particular address family altogether.

Examples

The following example shows that the E.164 address family with call success rate, available circuits, total circuits, and trunk group attributes is being advertised for ITAD 1234:

```
Router(config)# tgrep local-itad 1234
Router(config-tgrep)# advertise e164 csr ac tc trunk-group
```

Related Commands

Command	Description
tgrep local-itad	Enters TGREP configuration mode and defines an ITAD.

alarm-trigger

To configure a T1 or E1 controller to send an alarm to the public switched telephone network (PSTN) or switch if specified T1 or E1 DS0 groups are out of service, use the **alarm-trigger** command in controller configuration mode. To configure a T1 or E1 controller not to send an alarm, use the **no** form of this command.

alarm-trigger blue *ds0-group-list*

no alarm-trigger

Syntax Description	blue	Specifies the alarm type to be sent is “blue,” also known as an Alarm Indication Signal (AIS).
	<i>ds0-group-list</i>	Specifies the DS0 group or groups to be monitored for permanent trunk connection status or busyout status.

Defaults No alarm is sent

Command Modes Controller configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600, Cisco 3600, and Cisco MC3810.

Usage Guidelines Any monitored time slot can be used for either permanent trunk connections or switched connections. Permanent virtual circuits (PVCs) and switched virtual circuits (SVCs) can be combined on a T1 or E1 controller and monitored for alarm conditioning.

An alarm is sent only if all of the time slots configured for alarm conditioning on a T1 or E1 controller are out of service. If one monitored time slot remains in service or returns to service, no alarm is sent.

Examples The following example configures T1 0 to send a blue (AIS) alarm if DS0 groups 0 and 1 are out of service:

```
controller t1 0
alarm-trigger blue 0,1
exit
```

Related Commands	Command	Description
	busyout monitor	Configures a voice port to monitor an interface for events that would trigger a voice-port busyout.
	connection trunk	Creates a permanent trunk connection (private line or tie-line) between a voice port and a PBX.
	voice class permanent	Creates a voice class for a Cisco or FRF-11 permanent trunk.

alias (cm-fallback)

To provide a mechanism for rerouting calls to telephone numbers that are unavailable during Cisco CallManager fallback, use the **alias** command in call-manager-fallback configuration mode. To disable rerouting of unmatched call destination calls, use the **no** form of this command.

alias *tag number-pattern to alternate-number*

no alias *tag number-pattern to alternate-number*

Syntax Description

<i>tag</i>	Identifier for alias rule range. The range is from 1 to 10.
<i>number-pattern</i>	Pattern to match the incoming telephone number. This pattern may include wildcards.
to	Connects the tag number pattern to the alternate number.
<i>alternate-number</i>	Alternate telephone number to route incoming calls to match the number pattern.

Defaults

No default behavior or values

Command Modes

Call-manager-fallback configuration

Command History

Release	Modification
12.2(2)XT	This command was introduced on the Cisco 1750, Cisco 1751, Cisco 2600 series, Cisco 3600 series, and Cisco IAD2420 series IADs.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 3725, Cisco 3745, and Cisco MC3810-V3.
12.2(8)T1	This command was implemented on the Cisco 2600-XM and Cisco 2691.
12.2(11)T	This command was implemented on the Cisco 1760.

Usage Guidelines

The **alias** command provides a mechanism for servicing calls placed to telephone numbers that are unavailable during CallManager fallback. Individual alias rules are activated only when a phone registers that has an extension number equal to the alternate number.

When a phone with the alternate number registers, calls that match the number pattern are rerouted to the alternate number. The alternate number can be a specific phone number or can contain wildcard digits such as "50.." (where ".." represents any two digits 01 to 99) to enable rerouting of a range of numbers. When an IP phone registers with an alternate number, an additional plain old telephone service (POTS) dial peer is created using the number pattern as the dial peer destination pattern. The POTS dial peer voice port is set to match the voice port associated with the alternate number.

If other IP phones register that have specific phone numbers that fall within the range of the alternate number, the call routes to the IP phone in preference to being rerouted to the alternate number (according to normal dial-peer longest-match, preference, and huntstop rules).

Examples

The following example sets the **alias** command:

```
Router(config)# call-manager-fallback  
Router(config-cm-fallback)# alias 1 50.. to 5001
```

Calls to numbers in the 5000 to 5099 range that are not otherwise explicitly resolved to a specific extension number are routed to the phone with extension 5001. This supports configurations in which only a subset of phones are supported in the Cisco CallManager fallback mode. Phone calls intended for phones that are not given fallback service can then be redirected to the specified extension number.

Related Commands

Command	Description
call-manager-fallback	Enables SRS Telephony feature support and enters call-manager-fallback configuration mode.
default-destination	Assigns a default destination number for incoming telephone calls on the SRS Telephony router.

alias static

To create a static entry in the local alias table, use the **alias static** command in gatekeeper configuration mode. To remove a static entry, use the **no** form of this command.

alias static *ip-signaling-addr* [*port*] **gkid** *gatekeeper-name* [**ras** *ip-ras-addr* *port*] [**terminal** | **mcu** | **gateway** {**h320** | **h323-proxy** | **voip**}] [**e164** *e164-address*] [**h323id** *h323-id*]

no alias static *ip-signaling-addr* [*port*] **gkid** *gatekeeper-name* [**ras** *ip-ras-addr* *port*] [**terminal** | **mcu** | **gateway** {**h320** | **h323-proxy** | **voip**}] [**e164** *e164-address*] [**h323id** *h323-id*]

Syntax Description

<i>ip-signaling-addr</i>	IP address of the H.323 node, used as the address to signal when establishing a call.
<i>port</i>	(Optional) Port number other than the endpoint Call Signaling well-known port number (1720).
gkid <i>gatekeeper-name</i>	Name of the local gatekeeper of whose zone this node is a member.
ras <i>ip-ras-addr</i>	(Optional) Node remote access server (RAS) signaling address. If omitted, the <i>ip-signaling-addr</i> parameter is used in conjunction with the RAS well-known port.
<i>port</i>	(Optional) Port number other than the RAS well-known port number (1719).
terminal	(Optional) Indicates that the alias refers to a terminal.
mcu	(Optional) Indicates that the alias refers to a multiple control unit (MCU).
gateway	(Optional) Indicates that the alias refers to a gateway.
h320	(Optional) Indicates that the alias refers to an H.320 node.
h323-proxy	(Optional) Indicates that the alias refers to an H.323 proxy.
voip	(Optional) Indicates that the alias refers to VoIP.
e164 <i>e164-address</i>	(Optional) Specifies the node E.164 address. This keyword and argument can be used more than once to specify as many E.164 addresses as needed. Note that there is a maximum number of 128 characters that can be entered for this address. To avoid exceeding this limit, you can enter multiple alias static commands with the same call signaling address and different aliases.
h323id <i>h323-id</i>	(Optional) Specifies the node H.323 alias. This keyword and argument can be used more than once to specify as many H.323 identification (ID) aliases as needed. Note that there is a maximum number of 256 characters that can be entered for this address. To avoid exceeding this limit, you can enter multiple alias static commands with the same call signaling address and different aliases.

Defaults

No static aliases exist.

Command Modes

Gatekeeper configuration

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

The local alias table can be used to load static entries by performing as many of the commands as necessary. Aliases for the same IP address can be added in different commands, if required.

Typically, static aliases are needed to access endpoints that do not belong to a zone (that is, they are not registered with any gatekeeper) or whose gatekeeper is inaccessible for some reason.

Examples

The following example creates a static terminal alias in the local zone:

```
zone local gk.zone1.com zone1.com
alias static 191.7.8.5 gkid gk.zone1.com terminal e164 14085551212 h323id bobs_terminal
```

allow-connections

To allow connections between specific types of end points in a Cisco Multiservice IP-to-IP Gateway, use the **allow-connections** command in voice service configuration mode. To refuse specific types of connections, use the **no** form of this command.

allow-connections *from-type* **to** *to-type*

no allow-connections *from-type* **to** *to-type*

Syntax Description

<i>from-type</i>	Type of connection. Valid type is h323.
<i>to-type</i>	Type of connection. Valid type is h323.

Defaults

H.323 to H.323 connections are allowed. Connections to or from POTS end points are not allowed.

Command Modes

Voice service configuration

Command History

Release	Modification
12.2(13)T3	This command was introduced.

Examples

The following example specifies that connections between H.323 end points are allowed:

```
voice service voip
no allow-connections any to pots
no allow-connections pots to any
allow-connections h323 to h323
```

Usage Guidelines

Only H.323 to H.323 connections are supported.

alt-dial

To configure an alternate dial-out string for dial peers on the Cisco MC3810 multiservice concentrator, use the **alt-dial** command in dial peer configuration mode. To delete the alternate dial-out string, use the **no** form of this command.

alt-dial *string*

no alt-dial *string*

Syntax Description

<i>string</i>	The alternate dial-out string.
---------------	--------------------------------

Defaults

No alternate dial-out string is configured

Command Modes

Dial peer configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.

Usage Guidelines

This command applies to Cisco MC3810 multiservice concentrator plain old telephone service (POTS), Voice over Frame Relay (VoFR), and Voice over ATM (VoATM) dial peers.

The **alt-dial** command is used for the on-net-to-off-net alternative dialing function. The string replaces the destination-pattern string for dialing out.

Examples

The following example configures an alternate dial-out string of 9,5559871:

```
alt-dial 9,5559871
```

ani mapping

To preprogram the Numbering Plan Area (NPA), or area code, into a single Multi Frequency (MF) digit, use the **ani mapping** command in voice-port configuration mode. To disable Automatic Number Identification (ANI) mapping, use the **no** form of this command.

ani mapping *npd-value npa-number*

no ani mapping

Syntax Description

<i>npd-value</i>	Value of the Numbering Plan Digit (NPD). Range is 0 to 3. There is no default.
<i>npa-number</i>	Number (area code) of the NPA. Range is 100 to 999. There is no default value.

Defaults

No default behavior or values

Command Modes

Voice port

Command History

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

Usage Guidelines

The **ani mapping** command table translates the NPA into a single MF digit. The number of NPDs programmed is determined by local policy as well as by the number of NPAs that the public service answering point (PSAP) serves. Repeat this command until all NPDs are configured or until the NPD maximum range is reached.

Examples

The following example shows the voice port preprogramming the NPA into a single MF digit:

```
voice-port 1/1/0
 timing digit 100
 timing inter-digit 100
 ani mapping 1 408
 signal cama KP-NPD-NXX-XXXX-ST
!
voice-port 1/1/1
 timing digit 100
 timing inter-digit 100
 ani mapping 1 408
 signal cama KP-NPD-NXX-XXXX-ST
```

Related Commands	Command	Description
	signal	Specifies the type of signaling for a CAMA port.
	voice-port	Enters voice-port configuration mode.

answer-address

To specify the full E.164 telephone number to be used to identify the dial peer of an incoming call, use the **answer-address** command in dial peer configuration mode. To disable the configured telephone number, use the **no** form of this command.

answer-address [+]*string*[**T**]

no answer-address

Syntax Description

+	(Optional) Character that indicates an E.164 standard number.
<i>string</i>	Series of digits that specify the E.164 or private dial plan telephone number. Valid entries are as follows: <ul style="list-style-type: none"> • Digits 0 through 9, letters A through D, pound sign (#), and asterisk (*), which represent specific characters that can be entered. • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit.
T	(Optional) Control character that indicates that the answer-address value is a variable-length dial string.

Defaults

The default value is enabled with a null string

Command Modes

Dial peer configuration

Command History

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

Usage Guidelines

Use the **answer-address** command to identify the origin (or dial peer) of incoming calls from the IP network. Cisco IOS software identifies the dial peers of a call in one of two ways: by identifying either the interface through which the call is received or the telephone number configured with the **answer-address** command. In the absence of a configured telephone number, the peer associated with the interface is associated with the incoming call.

For calls that come in from a plain old telephone service (POTS) interface, the **answer-address** command is not used to select an incoming dial peer. The incoming POTS dial peer is selected on the basis of the port configured for that dial peer.

There are certain areas in the world (for example, certain European countries) where valid telephone numbers can vary in length. Use the optional control character **T** to indicate that a particular **answer-address** value is a variable-length dial string. In this case, the system does not match the dialed numbers until the interdigit timeout value has expired.

**Note**

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

Examples

The following example shows the E.164 telephone number 555-9626 as the dial peer of an incoming call being configured:

```
dial-peer voice 10 pots
answer-address +5559626
```

Related Commands

Command	Description
destination-pattern	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer.
port (dial peer)	Associates a dial peer with a specific port.
prefix	Specifies the prefix of the dialed digits for a dial peer.

application

To enable a specific application on a dial peer, use the **application** command in dial-peer configuration mode. To remove the application from the dial peer, use the **no** form of this command.

application *application-name* [**out-bound**]

no application [**out-bound**]

Syntax Description

<i>application-name</i>	Name of the predefined application that you wish to enable on the dial peer. See the “Usage Guidelines” section for valid application names.
out-bound	(Optional) Outbound calls are handed off to the named application. This keyword is used for store-and-forward fax applications and VoiceXML applications.

Defaults

No default behavior or values

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the Cisco 2500 series, Cisco 3600 series, and Cisco AS5300.
12.0(5)T	The SGCPAPP application was supported initially on the Cisco AS5300 in a private release that was not generally available.
12.0(7)XK	Support for the SGCPAPP application was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	The SGCPAPP application was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	The MGCPAPP application was implemented on the Cisco AS5300.
12.1(3)XI	The out-bound keyword was added for store-and-forward fax on the Cisco AS5300.
12.1(5)T	The out-bound keyword was integrated into Cisco IOS Release 12.1(5)T, and the command was implemented on the Cisco AS5800.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(2)XN	Support for enhanced MGCP voice gateway interoperability was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(4)XM	This command was implemented on the Cisco 1751.

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: The Cisco 3725 and Cisco 3745. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was integrated into Cisco CallManager Version 3.2 and implemented on the Cisco 1760 and Cisco IAD2420 series routers. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.
12.2(13)T	The <i>application-name</i> argument was removed from the no form of this command.
12.2(15)T	Malicious Caller Identification (MCID) was added as a valid <i>application-name</i> argument.

Usage Guidelines

Use this command when configuring interactive voice response (IVR) or any of the IVR-related features to associate a predefined session application with an incoming POTS dial peer and an outgoing Multimedia Mail over IP (MMoIP) dial peer. Calls that use the incoming POTS dial peer and the outgoing MMoIP dial peer are handed off to the specified predefined session application.

For Media Gateway Control Protocol (MGCP) and Simple Gateway Control Protocol (SGCP) networks, enter the application name in uppercase characters. For example, for MGCP networks, you would enter MGCPAPP for the *application-name* argument. The application can be applied only to POTS dial peers. Note that SGCP dial peers do not use dial-peer hunting.



Note

In Cisco IOS Release 12.2, you cannot mix SGCP and non-SGCP endpoints in the same T1 controller, nor can you mix SGCP and non-SGCP endpoints in the same DS0 group.



Note

MGCP scripting is not supported on the Cisco 1750 router or on Cisco 7200 series routers.

For H.323 networks, the application is defined by a Tool Command Language/interactive voice response (TCL/IVR) filename and location. Incoming calls that use POTS dial peers and outgoing calls that use MMoIP dial peers are handed off to this application.

For Session Initiation Protocol (SIP) networks, use this command to associate a predefined session application. The default TCL application (from the Cisco IOS image) for SIP is session and can be applied to both VoIP and POTS dial peers.

Examples

The following example defines an application and applies it to an outbound MMoIP dial peer for the fax on-ramp operation:

```
call application voice fax_on_vfc_onramp http://santa/username/clid_4digits_npw_3.tcl
dial-peer voice 3 mmoip
 application fax_on_vfc_onramp out-bound
 destination-pattern 57108..
 session target mailto:$d@mail-server.cisco.com
```

The following example applies the MGCP application to a dial peer:

```
dial-peer voice 1 pots
 application MGCPAPP
```

The following example applies a predefined application to an incoming POTS dial peer:

```
dial-peer voice 100 pots
 application c4
```

The following example applies a predefined application to an outbound MMoIP dial peer for the on-ramp operation:

```
dial-peer voice 3 mmoip
 application fax_on_vfc_onramp_ap out-bound
 destination-pattern 57108..
 session target mailto:$d$@mail-server.cisco.com
```

The following example applies the predefined SIP application to a dial peer:

```
dial-peer voice 10 pots
 application session
```

For Cisco IOS Release 12.2(15)T, MCID was added as a valid *application-name* argument. The following is a sample configuration using the MCID application name:

```
call application voice mcid http://santa/username/app_mcid_dtmf.2.0.0.28.tcl
dial-peer voice 3 pots
 application mcid
 incoming called-number 222....
 direct-inward-dial
 port 1:D
```

Related Commands

Command	Description
call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
mgcp	Starts the MGCP daemon.
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.

application (ephone-dn)

To select a session-level application on a per Cisco IP phone directory number basis, use the **application** command in ephone-dn configuration mode. To disable this feature, use the **no** form of this command.

application *application-name*

no application *application-name*

Syntax Description

<i>application-name</i>	Interactive voice response (IVR) application name.
-------------------------	--

Defaults

No default behavior or values

Command Modes

Ephone-dn configuration

Command History

Release	Modification
12.2(2)XT	This command was introduced on the Cisco 1750, Cisco 1751, Cisco 2600 series, Cisco 3600 series, and Cisco IAD2420 series IADs.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 3725, Cisco 3745, and Cisco MC3810-V3.
12.2(8)T1	This command was implemented on the Cisco 2600-XM and Cisco 2691.
12.2(11)T	This command was implemented on the Cisco 1760.

Usage Guidelines

The **application** command selects a session-level application on a per Cisco IP phone directory number basis. Use this command to assign a Tool Command Language (TCL) IVR application to the Cisco IP phone directory number (ephone-dn).

Examples

The following example sets the IVR application for directory number 1:

```
Router(config)# ephone-dn 1
Router(config-ephone-dn) application TCL IVR
```

Related Commands

Command	Description
ephone-dn	Enters ephone-dn configuration mode.

application (telephony-service)

To select the session-level application for all Cisco IP phone lines served by the Cisco IOS Telephony Service (ITS) router, use the **application** command in telephony-service configuration mode. To disable this application, use the **no** form of this command.

application *application-name*

no application *application-name*

Syntax Description	<i>application-name</i>	Selected interactive voice response (IVR) application name.
--------------------	-------------------------	---

Defaults	DEFAULT session application
----------	-----------------------------

Command Modes	Telephony-service configuration
---------------	---------------------------------

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 to assign a tool command language (TCL) IVR application to all IP phones served by the ITS router.
------------------	---

Examples	The following example selects a TCL IVR application named app-xfer for all IP phones served by the ITS router:
----------	--

```
Router(config)# telephony-service
Router(config-telephony-service) application app-xfer
```

Related Commands	Command	Description
	telephony-service	Enables Cisco ITS and enters telephony-service configuration mode.

arq hopoff zone

To configure a list of hopoff zones to which to send location request (LRQ) messages, use the **arq hopoff zone** command in gatekeeper configuration mode. To disable this feature, use the **no** form of this command.

```
arq hopoff zone zone-name [zone zone-name]
```

```
no arq hopoff zone
```

Syntax Description

<i>zone-name</i>	Defines a valid remote zone or cluster.
zone <i>zone-name</i>	Defines a zone and a valid remote zone or cluster.

Defaults

No default behavior or values.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

This command is an admission request (ARQ) message forwarding enhancement that modifies the ARQ handling logic on the access GK. This enhancement forces the access GK to send LRQ messages to remote zones or clusters to resolve the called number, even though the routing information for the called number is already known.

If more than one zone (cluster) names are configured as hopoffs, an LRQ is sent to each of the zones in the list. The LRQ sending order is determined by the cost and priority associated with the corresponding remote zone (cluster). LRQs are sent in sequential mode.

GKTMP request are sent before an override is applied. In this case the following applies:

- If a Gatekeeper Transaction Message Protocol (GKTMP) server is configured and gives a RspACF message with a call signaling address, the override has no effect.
- If a GKTMP server is configured and gives an override remote zone list, that list takes precedence over the configured list. You can either use the CLI to override or GKTMP override. Authentication, authorization, and accounting (AAA) is completed before the override is applied.

If a border element (BE) is configured and active, an LRQ is sent to the BE as well as to any zones on the override list. The LRQ sending order is decided by cost and priority on respective remote zones.

All the called numbers, irrespective of the prefix to which they belong, are overridden. This includes following cases:

- Called number resolves to an endpoint on the local zone of the GK
- Called number resolves to a set of remote prefixes (configured on GK)
- Called number resolves to a local prefix (configured on GK)

If carrier-based routing is used, the remote zone list obtained by processing the carrier information is used.

With this feature, an LRQ is sent for any ARQ, irrespective of the DNIS or prefix.

Examples

The following example configures a list of hopoff zones to which LRQ messages are sent. In this example, zonename1 and zonename2 have been configured as remote zones or clusters.

```
Router (gk-config) # arq hopoff zone zonename1 zone zonename2
```

Related Commands

Command	Description
arq reject-unknown-prefix	Enables the gatekeeper to reject ARQs for zone prefixes that are not configured.
gw-type-prefix	Configures a technology prefix in the gatekeeper.
lrq forward-queries	Enables a gatekeeper to forward LRQ messages that contain E.164 addresses that match zone prefixes controlled by remote gatekeepers.
lrq reject-unknown-prefix	Enables the gatekeeper to reject all LRQ messages for zone prefixes that are not configured.
zone local	Specifies a zone controlled by a gatekeeper.
zone remote	Statically specifies a remote zone if DNS is unavailable or undesirable.

arq reject-resource-low

To configure the gatekeeper to send an Admission Reject (ARJ) message to the requesting gateway if destination resources are low, use the **arq reject-resource-low** command in gatekeeper configuration mode. To disable the gatekeeper from checking resources, use the **no** form of this command.

arq reject-resource-low

no arq reject-resource-low

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Gatekeeper configuration

Command History	Release	Modification
	12.3(1)	This command was introduced.

Examples The following example shows that the gatekeeper is configured to send an ARJ message to the requesting gateway if destination resources are low:

```
gatekeeper
 arq reject-resource-low
```

Related Commands	Command	Description
	lrq reject-resource-low	Configures a gatekeeper to notify a sending gatekeeper on receipt of an LRQ message that no terminating endpoints are available.

arq reject-unknown-prefix

To enable the gatekeeper to reject admission requests (ARQs) for zone prefixes that are not configured, use the **arq reject-unknown-prefix** command in gatekeeper configuration mode. To reenable the gatekeeper to accept and process all incoming ARQs, use the **no** form of this command.

arq reject-unknown-prefix

no arq reject-unknown-prefix

Syntax Description This command has no arguments or keywords

Defaults The gatekeeper accepts and processes all incoming ARQs.

Command Modes Gatekeeper configuration

Command History	Release	Modification
	11.3(6)Q, 11.3(7)NA	This command was introduced.
	12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines Use the **arq reject-unknown-prefix** command to configure the gatekeeper to reject any incoming ARQs for a destination E.164 address that does not match any of the configured zone prefixes.

When an endpoint or gateway initiates an H.323 call, it sends an ARQ to its gatekeeper. The gatekeeper uses the configured list of zone prefixes to determine where to direct the call. If the called address does not match any of the known zone prefixes, the gatekeeper attempts to *hairpin* the call out through a local gateway. If you do not want your gateway to do this, then use the **arq reject-unknown-prefix** command. (The term *hairpin* is used in telephony. It means to send a call back in the direction from which it came. For example, if a call cannot be routed over IP to a gateway that is closer to the target phone, the call is typically sent back out through the local zone, back the way it came.)

This command is typically used to either restrict local gateway calls to a known set of prefixes or deliberately fail such calls so that an alternate choice on a gateway's rotary dial peer is selected.

Examples Consider a gatekeeper configured as follows:

```
zone local gk408 cisco.com
zone remote gk415 cisco.com 172.21.139.91
zone prefix gk408 1408.....
zone prefix gk415 1415.....
```

In this example configuration, the gatekeeper manages a zone containing gateways to the 408 area code, and it knows about a peer gatekeeper that has gateways to the 415 area code. Using the **zone prefix** command, the gatekeeper is then configured with the appropriate prefixes so that calls to those area codes hop off in the optimal zone.

If the **arq request-unknown-prefix** command is not configured, the gatekeeper handles calls in the following way:

- A call to the 408 area code is routed out through a local gateway.
- A call to the 415 area code is routed to the gk415 zone, where it hops off on a local gateway.
- A call to the 212 area code is routed to a local gateway in the gk408 zone.

If the **arq reject-unknown-prefix** command is configured, the gatekeeper handles calls in the following way:

- A call to the 408 area code is routed out through a local gateway.
- A call to the 415 area code is routed to the gk415 zone, where it hops off on a local gateway.
- A call to the 212 area code is rejected because the destination address does not match any configured prefix.

as

To define an application server for backhaul, use the **as** command in IUA configuration mode. To disable, use the **no** form of this command.


Note

All of the ASPs in an AS must be removed before an AS can be unconfigured.

```
as as-name {localip1 [localip2]} [local-sctp-port] [fail-over-timer] [sctp-startup-rtx]
[sctp-streams] [sctp-t1init]
```

```
no as name
```

Syntax Description

<i>as-name</i>	Defines the protocol name (only ISDN is supported).
<i>localip1</i>	Defines the local IP address(es) for all the ASPs in a particular AS.
<i>localip2</i>	(Optional) Defines the local IP address(es) for all the ASPs in a particular AS.
local-sctp-port	(Optional) Defines a specific local Simple Control Transmission Protocol (SCTP) port rather than an ISDN Q.921 User Adaptation Layer (IUA) well-known port.
fail-over-timer	(Optional) Configures the failover timer for a particular AS.
sctp-startup-rtx	(Optional) Configures the SCTP maximum startup retransmission timer.
sctp-streams	(Optional) Configures the number of SCTP streams for a particular AS.
sctp-t1init	(Optional) Configures the SCTP T1 initiation timer.

Defaults

No AS is defined.

Command Modes

IUA configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300 platform.
12.2(13)T1	This command was implemented on the Cisco AS5850.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T and implemented on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series; Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.

Usage Guidelines

A maximum of two local IP addresses can be specified. (Note that SCTP has built-in support for multihomed machines.)

The default value of the SCTP streams is determined by the hardware that you have installed. The value of the failover timer is found in the **show iua as all** command output.

The number of streams to assign to a given association is implementation dependent. During the initialization of the IUA association, you need to specify the total number of streams that can be used. Each D channel is associated with a specific stream within the association. With multiple trunk group support, every interface can potentially be a separate D channel.

At startup, the IUA code checks for all the possible T1, E1, or T3 interfaces and sets the total number of inbound and outbound streams supported accordingly. In most cases, there is only a need for one association between the gateway (GW) and the Media Gateway Controller (MGC). For the rare case that you are configuring multiple AS associations to various MGCs, the overhead from the unused streams would have minimal impact. The NFAS D channels are configured for one or more interfaces, where each interface is assigned a unique stream ID.

The total number of streams for the association needs to include an additional stream for the SCTP management messages. So during startup, the IUA code adds one to the total number of interfaces (streams) found.

You have the option to manually configure the number of streams per association. In the backhaul scenario, if the number of D channel links is limited to one, allowing the number of streams to be configurable avoids the unnecessary allocation of streams in an association that will never be used. For multiple associations between a GW and multiple MGCs, the configuration utility is useful in providing only the necessary number of streams per association. The overhead from the streams allocated but not used in the association is negligible.

If the number of streams is manually configured through the CLI, the IUA code cannot distinguish between a startup event, which automatically sets the streams to the number of interfaces, or if the value is set manually during runtime. If you are configuring the number of SCTP streams manually, you must add one plus the number of interfaces using the **sctp-streams** keyword. Otherwise, IUA needs to always add one for the management stream, and the total number of streams increments by one after every reload.

When you set the SCTP stream with the CLI, you cannot change the inbound and outbound stream support once the association is established with SCTP. The value takes effect when you first remove the IUA AS configuration and then configure it back as the same AS or a new one. The other option is to reload the router.

Examples

An AS and the application server process (ASP) should be configured first to allow a National ISDN-2 with Cisco extensions (NI2+) to be bound to this transport layer protocol. The AS is a logical representation of the SCTP local endpoint. The local endpoint can have more than one IP address but must use the same port number.

The following is an example of an AS configuration on a gateway. The configuration shows that an AS named as5400-3 is configured to use two local IP addresses and a port number of 2577:

```
Router(config-iua)# as as5400-3 10.1.2.34 10.1.2.35 2577
```

The following output shows that the AS (as1) is defined for backhaul:

```
AS as1 10.21.0.2 9900
```

Related Commands

Command	Description
asp	Defines an ASP for backhaul.

asp

To define an application server process (ASP) for backhaul, use the **asp** command in IUA configuration mode. To disable the ASP, use the **no** form of this command.


Note

All of the ASPs in an application server (AS) must be removed before an AS can be unconfigured.

```
asp asp-name as as-name {remoteip1 [remoteip2]} [remote-sctp-port] [ip-precedence]
[sctp-keepalives] [sctp-max-associations] [sctp-path-retransmissions] [sctp-t3-timeout]
```

```
no asp asp-name
```

Syntax Description

<i>asp-name</i>	Names the current ASP.
as	The application server to which the ASP belongs.
<i>as-name</i>	Name of the application server to which the ASP belongs.
<i>remoteip1</i>	Designates the remote IP address for this Simple Control Transmission Protocol (SCTP) association.
<i>remoteip2</i>	Designates the remote IP address for this SCTP association.
remote-sctp-port	Connects to a remote SCTP port rather than the IUA well-known port.
ip-precedence	(Optional) Sets IP Precedence bits for protocol data units (PDUs). <ul style="list-style-type: none"> IP precedence is expressed in the type of service (ToS) field of the show ip sctp association parameters output. The default type of service (ToS) value is 0. Valid precedence values range from 0 to 7. You can also use the default IP precedence value for this address by choosing the default option.
sctp-keepalives	(Optional) Modifies the keepalive behavior of an IP address in a particular ASP. <ul style="list-style-type: none"> Valid keepalive interval values range from 1000 to 60000. The default value is 500 ms (see the show ip sctp association parameters output under heartbeats).
sctp-max-associations	(Optional) Sets the SCTP maximum association retransmissions for a particular ASP. Valid values range from 2 to 20. The default is 3.
sctp-path-retransmissions	(Optional) Sets the SCTP path retransmissions for a particular ASP. Valid values range from 2 to 10. The default is 10.
sctp-t3-timeout	(Optional) Sets the SCTP T3 retransmission timeout for a particular ASP. The default value is 900 ms. Valid timeout values range from 300 to 60000. Default is 60000.

Defaults

No ASP is defined.

Command Modes

IUA configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and support was added for the Cisco AS5300.
12.2(11)T1	This command was implemented on the Cisco AS5850.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T and implemented on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series; and Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.

Usage Guidelines

This command establishes SCTP associations. There can be only a maximum of three ASPs configured per AS. IP precedence is expressed in the ToS field of **show ip sctp association parameters** output. The default ToS value is 0.

You can configure the precedence value in IUA in the range of 0 to 7 for a given IP address. Within IUA, the upper three bits representing the IP precedence in the ToS byte (used in the IP header) is set based on the user input before passing down the value to SCTP. In turn, SCTP passes the ToS byte value to IP. The default value is 0 for “normal” IP precedence handling.

The *asp-name* argument specifies the name of this ASP. The **ip-precedence** keyword sets the precedence and ToS field. The *remote-ip-address* argument specifies the IP address of the remote end-point (the address of MGC, for example). The *number* argument can be any IP precedence bits in the range 1 to 255.

The **no** form of the command results in precedence bits not being explicitly set by SCTP.

In the case of a hot-standby Cisco PGW2200 pair, from the gateway (GW) perspective there is usually one ASP active and another in the INACTIVE state. The ASP_UP message is used to bring the ASP state on the GW to the INACTIVE state, followed by the ASPTM message, ASP_ACTIVE to ready the IUA link for data exchange. (Eventually the QPTM Establish Request message actually initiates the start of the D channel for the given interface.) In the event that the GW detects a failure on the active ASP, it can send a NTFY message to the standby ASP to request that it become active.

Examples

An ASP can be viewed as a local representation of an SCTP association because it specifies a remote endpoint that will be in communication with an AS local endpoint. An ASP is defined for a given AS. For example, the following configuration defines a remote signaling controller *asp-name* at two IP addresses for AS as1. The remote SCTP port number is 2577:

```
as as1 10.4.8.69, 10.4.9.69 2477
asp asp1 as as1 10.4.8.68 10.4.9.68 2577
```

Multiple ASPs can be defined for a single AS for the purpose of redundancy, but only one ASP can be active. The ASPs are inactive and only become active after fail-over.

In the Cisco Media Gateway Controller (MGC) solution, a signaling controller is always the client that initiates the association with a gateway. During the initiation phase, you can request outbound and inbound stream numbers, but the gateway only allows a number that is at least one digit higher than the number of interfaces (T1/E1) allowed for the platform.

The following example specifies the IP precedence level on the specified IP address. This example uses IP precedence level 7, which is the maximum level allowed:

```
Router(config-ia) # asp asp1 ip-precedence 10.1.2.345 7
```

The following example specifies the IP address to enable and disable keepalives:

```
Router(config-ia) # asp asp1 sctp-keepalive 10.1.2.34
```

The following example specifies the keepalive interval in milliseconds. In this example, the maximum value of 60000 ms is used:

```
Router(config-ia) # asp asp1 sctp-keepalive 10.10.10.10 60000
```

The following example specifies the IP address for the SCTP maximum association and the maximum association value. In this example, a maximum value of 20 is used:

```
Router(config-ia) # asp asp1 sctp-max-association 10.10.10.10 20
```

The following example specifies the IP address for the SCTP path retransmission and the maximum path retransmission value. In this example, a maximum value of 20 is used:

```
Router(config-ia) # asp asp1 sctp-path-retransmissions 10.10.10.10 10
```

The following example specifies the IP address for SCTP T3 timeout and specifies the T3 timeout value in milliseconds. In this example, the maximum value of 60000 is used:

```
Router(config-ia) # asp asp1 sctp-t3-timeout 10.10.10.10 60000
```

Related Commands

Command	Description
as	Defines an application server (AS) for backhaul.

atm scramble-enable

To enable scrambling on E1 links, use the **atm scramble-enable** command in interface configuration mode. To disable scrambling, use the **no** form of this command.

atm scramble-enable

no atm scramble-enable

Syntax Description This command has no arguments or keywords.

Defaults By default, payload scrambling is set off

Command Modes Interface configuration

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

Usage Guidelines Enable scrambling on E1 links only. On T1 links, the default B8ZS line encoding normally ensures sufficient reliability. Scrambling improves data reliability on E1 links by randomizing the ATM cell payload frames to avoid continuous nonvariable bit patterns and to improve the efficiency of the ATM cell delineation algorithms.

The scrambling setting must match that of the far end.

Examples On a Cisco MC3810, the following example shows how to set the ATM0 E1 link to scramble payload:

```
interface atm0
 atm scramble-enable
```

atm video aesa

To set the unique ATM end-station address (AESA) for an ATM video interface that is using switched virtual circuit (SVC) mode, use the **atm video aesa** command in ATM interface configuration mode. To remove any configured address for the interface, use the **no** form of this command.

atm video aesa [**default** | *esi-address*]

no atm video aesa

Syntax Description

default	(Optional) Automatically creates a network service access point (NSAP) address for the interface, based on a prefix from the ATM switch (26 hexadecimal characters), the MAC address (12 hexadecimal characters) as the end station identifier (ESI), and a selector byte (two hexadecimal characters).
<i>esi-address</i>	(Optional) Defines the 12 hexadecimal characters used as the ESI. The ATM switch provides the prefix (26 hexadecimal characters), and the video selector byte provides the remaining two hexadecimal characters.

Defaults

default

Command Modes

ATM Interface configuration

Command History

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

Usage Guidelines

You cannot specify the ATM interface NSAP address in its entirety. The system creates either all of the address or part of it, depending on how you use this command.

Examples

On a Cisco MC3810 multiservice concentrator, the following example shows the ATM interface NSAP address set automatically:

```
interface atm0
  atm video aesa default
```

On a Cisco MC3810 multiservice concentrator, the following example shows the ATM interface NSAP address set to a specific ESI value:

```
interface atm0/1
  atm video aesa 444444444444
```

Related Commands	Command	Description
	show atm video-voice address	Displays the NSAP address for the ATM interface.

attribute acct-session-id overloaded

To overload the acct-session-id attribute with voice vendor-specific attributes (VSAs), use the **attribute acct-session-id overloaded** command in gateway accounting AAA configuration mode. To disable overloading the acct-session-id attribute with voice VSAs, use the **no** form of this command.

attribute acct-session-id overloaded

no attribute acct-session-id overloaded

Syntax Description

This command has no arguments or keywords.

Defaults

The acct-session-id attribute is not overloaded with voice VSAs.

Command Modes

Gateway accounting AAA configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

- The **attribute acct-session-id overloaded** command replaces the **gw-accounting h323 vsa** command.
- The acct-session-id attribute is RADIUS attribute 44. For more information on this attribute, Refer to the document *RADIUS Attribute 44 (Accounting Session ID) in Access Requests*.
- Attributes that cannot be mapped to standard RADIUS attributes are packed into the acct-session-id attribute field as ASCII strings separated by the forward slash (“/”) character.
- The Accounting Session ID (acct-session-id) attribute contains the RADIUS account session ID, which is a unique identifier that links accounting records associated with the same login session for a user. This unique identifier makes it easy to match start and stop records in a log file.
- Accounting Session ID numbers restart at 1 each time the router is power-cycled or the software is reloaded.

Examples

The following example, shows the acct-session-id attribute being overloaded with voice vendor-specific attributes (VSAs):

```
gw-accounting aaa
 attribute acct-session-id overloaded
```

Related Commands	Command	Description
	gw-accounting aaa	Enables VoIP gateway accounting.
	call accounting-template voice	Defines and loads the template file at the location defined by the URL.

attribute h323-remote-id resolved

To resolve the h323-remote-id attribute, use the **attribute h323-remote-id resolved** command in gateway-accounting AAA configuration mode. To keep the h323-remote-id attribute unresolved, use the **no** form of this command.

attribute h323-remote-id resolved

no attribute h323-remote-id resolved

Syntax Description This command has no arguments or keywords.

Defaults The h323-remote-id attribute is not resolved.

Command Modes gw-accounting aaa configuration

Command History	Release	Modification
	12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

- In Cisco IOS Release 12.2(11)T, the **attribute h323-remote-id resolved** command replaces the **gw-accounting h323 resolve** command, and the h323-remote-id attribute has been added as a Cisco vendor-specific attribute (VSA). This attribute is a string that indicates the Domain Name System (DNS) name or locally defined host name of the remote gateway.
- You can obtain the value of the h323-remote-id attribute by doing a DNS lookup of the h323-remote-address attribute. The h323-remote-address attribute indicates the IP address of the remote gateway.

Examples The following example sets the h323-remote-id attribute to resolved:

```
gw-accounting aaa
 attribute h323-remote-id resolved
```

Related Commands	Command	Description
	gw-accounting aaa	Enables VoIP gateway accounting.

audio-prompt load

To initiate loading the selected audio file (.au), which contains the announcement prompt for the caller, from Flash memory into RAM, use the **audio-prompt load** command in privileged EXEC mode. This command does not have a **no** form.

audio-prompt load *name*

Syntax Description

<i>name</i>	Location of the audio file that you want to have loaded from memory, Flash memory, or an FTP server.
-------------	--

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(6)NA2	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.1(5)T	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751. Support for other Cisco platforms is not included in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.

Usage Guidelines

The first time the interactive voice response (IVR) application plays a prompt, it reads it from the URL (or the specified location for the .au file, such as Flash or FTP) into RAM. Then it plays the script from RAM. An example of the sequence of events follows:

- When the first caller is asked to enter the account and personal identification numbers (PINs), the `enter_account.au` and `enter_pin.au` files are loaded into RAM from Flash memory.
- When the next call comes in, these prompts are played from the RAM copy.
- If all callers enter valid account numbers and PINs, the `auth_failed.au` file is not loaded from Flash memory into RAM.

The router loads the audio file only when the script initially plays that prompt after the router restarts. If the audio file is changed, you must run this EXEC command to reread the file. This generates an error message if the file is not accessible or if there is a format error.

**Note**

With Cisco IOS Release 11.3(6)NA2, the URL pointer refers to the directory where Flash memory is stored.

Examples

The following example shows how to load the enter_pin.au audio file from Flash memory into RAM:

```
audio-prompt load flash:enter_pin.au
```

authentication method

To set an authentication method at login for calls that come into a dial peer, use the **authentication method** command in voice class AAA configuration mode. To disable the authentication method set at login, use the **no** form of this command.

authentication method *MethListName*

no authentication method *MethListName*

Syntax Description

<i>MethListName</i>	Defines an authentication method list name.
---------------------	---

Defaults

When this command is not used to specify a login authentication method, the system uses the **aaa authentication login h323** command as the default.

Command Modes

Voice class AAA configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

- This command is used to direct authentication requests to a RADIUS server based on dialed number information service (DNIS) or trunk grouping.
- This command is used for directing dial-peer-based authentication requests. The method list must be defined during initial authentication setup.

Examples

In the example below, “dp” is the method list name used for authentication. The method list name is defined during initial authentication setup.

```
voice class aaa 1
 authentication method dp
```

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.
voice class aaa	Enables dial-peer-based VoIP AAA configurations.

authorization method

To set an authorization method at login for calls that are into a dial peer, use the **authorization method** command in voice class AAA configuration mode. To disable the authorization method set at login, use the **no** form of this command.

authorization method *MethListName*

no authorization method *MethListName*

Syntax Description

<i>MethListName</i>	Defines an authorization method list name.
---------------------	--

Defaults

When this command is not used to specify a login authorization method, the system uses the **aaa authorization exec h323** command as the default.

Command Modes

Voice class AAA configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

This command is used to direct authentication requests to a RADIUS server based on dialed number information service (DNIS) or trunk grouping.

This command is used for directing dial-peer-based authentication requests. The method list must be defined during initial authentication setup.

Examples

The following example set an authorization method of “dp”.

```
voice class aaa 1
  authorization method dp
```

Related Commands

Command	Description
aaa authorization exec	Runs authorization to determine if the user is allowed to run an EXEC shell.
voice class aaa	Enables dial-peer-based VoIP AAA configurations.

auto-cut-through

To enable call completion when a PBX does not provide an M-lead response, use the **auto-cut-through** command in voice-port configuration mode. To disable the auto-cut-through operation, use the **no** form of this command.

auto-cut-through

no auto-cut-through

Syntax Description

This command has no arguments or keywords.

Defaults

Auto-cut-through is enabled

Command Modes

Voice-port configuration

Command History

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

Usage Guidelines

The **auto-cut-through** command applies to ear and mouth (E&M) voice ports only.

Examples

The following example shows enabling of call completion on a Cisco MC3810 when a PBX does not provide an M-lead response:

```
voice-port 1/1
 auto-cut-through
```

The following example shows enabling of call completion on a Cisco 2600 or 3600 router when a PBX does not provide an M-lead response:

```
voice-port 1/0/0
 auto-cut-through
```

Related Commands

Command	Description
show voice port	Displays voice port configuration information.

■ auto-cut-through