

isdn bind-l3 through ixi transport http

- isdn bind-l3, on page 3
- isdn bind-l3 (Interface BRI), on page 4
- isdn bind-l3 ccm-manager, on page 6
- isdn bind-l3 iua-backhaul, on page 7
- isdn contiguous-bchan, on page 9
- isdn dpnss, on page 10
- isdn gateway-max-interworking, on page 12
- isdn global-disconnect, on page 13
- isdn gtd, on page 15
- isdn ie oli, on page 16
- isdn integrate calltype all, on page 17
- isdn network-failure-cause, on page 19
- isdn outgoing display-ie, on page 22
- isdn protocol-emulate, on page 24
- isdn rlm-group, on page 26
- isdn skipsend-idverify, on page 28
- isdn spoofing, on page 31
- isdn supp-service calldiversion, on page 32
- isdn supp-service mcid, on page 33
- isdn supp-service name calling, on page 34
- isdn supp-service tbct, on page 36
- isdn t-activate, on page 38
- isdn tei-negotiation (interface), on page 40
- iua, on page 43
- ivr asr-server, on page 45
- ivr autoload mode, on page 47
- ivr prompt memory, on page 49
- ivr autoload url, on page 51
- ivr contact-center, on page 53
- ivr language link, on page 56
- ivr prompt cutoff-threshold, on page 57
- ivr prompt streamed, on page 58
- ivr record cpu flash, on page 60

- ivr record jitter, on page 61
- ivr record memory session, on page 63
- ivr record memory system, on page 64
- ivr tts-server, on page 65
- ivr tts-voice-profile, on page 67
- ixi application cme, on page 68
- ixi application mib, on page 70
- ixi transport http, on page 72

isdn bind-l3

To configure an ISDN D-channel serial interface for signaling backhaul and associate it with a session set, use the **isdn bind-l3** command in interface configuration mode. To disable signaling backhaul on an ISDN D-channel serial interface, use the **no** form of this command.

isdn bind-l3 *set-name*
no isdn bind-l3

Syntax Description

set -name	Session set with which you are associating a D-channel interface.

Command Default

The ISDN D channel is not configured for signaling backhaul and is not associated with a session set

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco IAD2420 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Examples

The following example configures T1 signaling channel serial 0:23 for signaling backhaul and associate the D channel with the session set named "Set1":

```
Router(config)# interface s0:23
Router(config-if)# isdn bind-L3 set1
Router(config-if)# exit
```

The following example configures E1 signaling channel serial 0:15 for signaling backhaul and associates the D channel with the session set named "Set3":

```
Router(config)# interface s0:15
Router(config-if)# isdn bind-L3 set3
Router(config-if)# exit
```

isdn bind-l3 (Interface BRI)

To cause a Basic Rate Interface (BRI) port to bind ISDN Layer 3 protocol to either a regular gateway (GW) q931 stack or a Cisco CallManager Transmission Control Protocol (TCP) backhaul application and, if the latter, to operate in Media Gateway Control Protocol (MGCP) mode for backhaul, use the **isdn bind l3** command in interface configuration mode. To disable binding and reset the BRI to Session Application mode for backhaul, use the **no** form of this command.

isdn bind-l3 {**q931** | **ccm-manager service mgcp**}
no isdn bind-l3 {**q931** | **ccm-manager service mgcp**}

Syntax Description

q931	Regular GW q931 stack. This is the default.
ccm manager service mgcp	Cisco CallManager TCP backhaul application. You must also select MGCP service mode for backhaul.

Command Default

If the command is not used, the BRI port uses Session Application mode and binding is disabled. If the command is used with no keywords, q931 is assumed.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(15)ZJ	This command was integrated into Cisco IOS Release 12.2(15)ZJ on the Cisco 26xxXM, Cisco 2691, Cisco 3640, Cisco 3640A, Cisco 3660, and Cisco 37xx.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.

Usage Guidelines

This command reinitializes the BRI interface, including the two B-channel voice ports within the BRI, to support MGCP-backhaul call control. It also binds ISDN Q931 Layer 3 to the Cisco CallManager.

This command is visible when the BRI voice interface card (VIC) is present. The BRI VIC provides narrowband digital-voice connectivity in the voice network module on the Cisco 2600 series and Cisco 3600 series.

Before you use this command to enable binding, disable any active calls on the BRI interface by using the **shutdown (voice port)** command. You need not shut down the interface if no active calls are present or to configure L3 binding.

The combined ccm-manager service mgcp keywords are available only for supported BRI interfaces.

The **q931** keyword is available only for supported BRI interfaces. This keyword is not available for ISDN PRI interfaces.

Examples

The following example sets binding for BRI interface slot 1, port 0:

```
Router (config-if)# isdn bind-l3 q931
```

Related Commands

Command	Description
ccm-manager config	Supplies the local MGCP voice gateway with the IP address or logical name of the TFTP server from which to download XML configuration files and enable the download of the configuration.
debug ccm-manager	Displays debugging information about the Cisco CallManager.
show ccm-manager	Displays a list of Cisco CallManager servers, their current status, and their availability.
show ccm-manager fallback-mgcp	Displays the status of the MGCP gateway fallback feature.
show mgcp	Displays values for MGCP parameters.
shutdown (voice-port)	Takes voice ports for a specific VIC offline.

isdn bind-l3 ccm-manager

To bind Layer 3 of the ISDN PRI interface of the Media Gateway Control Protocol (MGCP) voice gateway to the Cisco CallManager for PRI Q.931 signaling backhaul support, use the **isdn bind-l3 ccm-manager**command in interface configuration mode. To disable this binding, use the no form of this command.

isdn bind-l3 ccm-manager
no isdn bind-l3 ccm-manager

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(2)XN	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco Voice Gateway 200 (Cisco VG200).
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2, and implemented on the Cisco IAD2420.

Usage Guidelines

This command enables ISDN PRI backhaul on an MGCP-enabled voice gateway.

Note While the ISDN PRI is configured as MGCP, the Layer 3 binding cannot revert to Q.931.

Examples

The following example binds PRI Layer 3 to the Cisco CallManager:

```
isdn bind-l3 ccm-manager
```

isdn bind-l3 iua-backhaul

To specify ISDN backhaul using Stream Control Transmission Protocol (SCTP) for an interface and to bind Layer 3 to DUA for DPNSS backhaul, use the **isdn bind-l3 iua-backhaul**command in interface configuration mode. To disable the backhaul capability, use the **no** form of this command.

isdn bind-l3 iua-backhaul [*application-server-name*]
no isdn bind-l3 iua-backhaul

Syntax Description

application-server-name	(Optional) Name of the application server (AS) to use for backhauling the interface.

Command Default

No default behavior or values

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.2(4)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco IAD2420 series. The Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.2(15)ZJ	The capability to bind Layer 3 to DUA for DPNSS backhaul was added.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

DPNSS is not configured for backhaul and is not associated with a session set.

Examples

The following example configures DUA for DPNSS backhaul using an AS called "as1:"

```
Router(config-if)# isdn bind-l3 iua-backhaul as1
```

The following example configures T1 signaling channel serial 0:23 for signaling backhaul and associates the D channel with the session set named "set1":

```
Router(config)# interface s0:23
Router(config-if)# isdn bind-l3 set1
```

The following example configures E1 signaling channel serial 0:15 for signaling backhaul and associates the D channel with the session set named "set3":

```
Router(config)# interface s0:15
Router(config-if)# isdn bind-l3 set3
```

The following example shows IUA backhaul on the application server "as1":

```
interface Serial1/0:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 isdn bind-L3 iua-backhaul as1
```

Related Commands

Command	Description
as	Defines an AS for backhaul.
asp	Defines an ASP for backhaul.

isdn contiguous-bchan

To configure contiguous bearer channel handling on an E1 PRI interface, use the **isdn contiguous-bchan**command in interface configuration mode. To disable the contiguous B-channel handling, use the **no**form of this command.

isdn contiguous-bchan
no isdn contiguous-bchan

Syntax Description

This command has no arguments or keywords.

Command Default

Contiguous B channel handling is disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(7)XK	This command was introduced on the following platforms: Cisco 2500 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use this command to specify contiguous bearer channel handling so that B channels 1 to 30, skipping 16, map to time slots 1 to 31. This is available for E1 PRI interfaces only, when the **primary-qsig** or **primary-dms100** switch type option is configured by using the **isdn switch-type** command.

Examples

The following example shows the configuration on the E1 interface of a Cisco 3660 router E1 interface:

```
interface Serial5/0:15
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-qsig
 isdn overlap-receiving
 isdn incoming-voice voice
 isdn contiguous-bchan
```

Related Commands

Command	Description
isdn switch -type	Configures the **primary-qsig**or **primary-dms100**switch type for PRI support.

isdn dpnss

To indicate whether ISDN DPNSS is to act as PBX A or PBX B, or revert to Layer 2, use the **isdn dpnss** command in interface configuration mode. To reset to the default, use the **no** form of this command.

isdn dpnss [**pbxA** | **layer 2** [**retry max-count** *range*] [**timers** [**Tretry** *timer-value*] [**Ttest** *timer-value*]] [**test frame**]]
no isdn dpnss [**pbxA** | **layer 2** [**retry max-count** *range*] [**timers** [**Tretry** *timer-value*] [**Ttest** *timer-value*]] [**test frame**]]

Syntax Description

pbxA	(Optional) Enables DPNSS to act as PBX A.
layer 2	(Optional) Reverts to Layer 2.
retry max-count *range*	(Optional) Selects the number of times a frame will be retried if unacknowledged. The max-count value can be any number from 0 to 64. Default is 4
timers	(Optional) Selects DPNSS timers, which can be **Tretry** or **Ttest**.
Tretry *timer-value*	(Optional) Sets the Tretry timer in ms and seconds. Valid retry time values range from 5 ms to 10 seconds. Default is 500 ms.
Ttest *timer-value*	(Optional) Sets the Ttest timer in minutes. When the Ttest timer expires, frames are sent on all the DLCs. Valid test time values range from 1 to 60. Default is 5.
test frame	(Optional) Allows test frames to be sent periodically.

Command Default

PBX B

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Before you try to implement the **isdn dpnss layer2 test frame** command, make sure the ISDN switch type is configured (using the **isdn switch-type (PRI)** command) as PRIMARY-DPNSS. If you enter the **isdn dpnss layer2 test frame** command for a switch type that is not DPNSS, the router is forced into a reload.

Examples

The following example sets ISDN DPNSS to act as PBX A:

```
Router(config-if)# isdn dpnss pbxA
```

The following example sets the Tretry and Ttest timers:

```
Router(config-if)# isdn dpnss layer2 timers Tretry 500 Ttest 5
```

The following example selects the number of times a frame will be retried if unacknowledged:

```
Router(config-if)# isdn dpnss layer2 retry max-count 4
```

The following example allows test frames to be sent periodically:

```
Router(config-if)# isdn dpnss layer2 test frame
```

Related Commands

Command	Description
isdn bind-l3 iua-backhaul	Binds Layer 3 for DPNSS to DUA.
isdn switch-type (PRI)	Specifies the central office switch type on the ISDN interface.

isdn gateway-max-interworking

To prevent an H.323 gateway from checking for ISDN protocol compatibility and dropping information elements (IEs) in call messages, use the **isdn gateway-max-interworking**commandglobal configuration mode. To reset to the default, use the **no** form of this command.

isdn gateway-max-interworking
no isdn gateway-max-interworking

Syntax Description

This command has no arguments or keywords.

Command Default

The gateway checks for protocol compatibility.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)XI	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)XA	This command was implemented on the Cisco AS5400 and Cisco AS5350.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

If this command is enabled on an originating H.323 gateway, the information elements (IEs) in call messages to the terminating gateway are not checked for end-to-end protocol compatibility. If this command is enabled on a terminating gateway, IEs are not checked in the reverse direction. If this command is not enabled, and the ISDN protocols are not compatible on the originating and terminating gateways, the gateway drops all IEs, including the progress indicator. The gateway then inserts a progress indicator of 1 into all Progress messages.

Examples

The following example enables maximum interworking:

```
isdn gateway-max-interworking
```

isdn global-disconnect

To allow passage of RELEASE and RELEASE COMPLETE messages over a voice network, use the **isdn global-disconnect** command in interface configuration mode. To disallow passage of RELEASE and RELEASE COMPLETE messages, use the **no** form of this command.

isdn global-disconnect
no isdn global-disconnect

Syntax Description

This command has no arguments or keywords.

Command Default

RELEASE and RELEASE COMPLETE messages terminate locally; they are not passed over the voice network.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.
12.4(15)XY	Support was added for SIP voice networks.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **isdn global-disconnect** command works with ISDN interfaces configured for Q-signaling (QSIG) tunneling using the bri-qsig or pri-qsig ISDN switch type (in either primary or secondary mode). This command must be enabled on both IP to time-division multiplexing (IP-TDM) gateways in a toll-bypass scenario where RELEASE and RELEASE COMPLETE messages need to be transparently passed end-to-end and in both directions.

Enabling the **isdn global-disconnect** command allows passage of the RELEASE and RELEASE COMPLETE messages (including information element (IE) content) end-to-end across a voice network between PBXs. Use the **no** form of this command to prevent RELEASE and RELEASE COMPLETE messages from being passed across the network.

Examples

The following example shows the configuration on the T1 PRI interface of a Cisco 3660 router:

```
interface Serial5/0:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-qsig
 isdn global-disconnect
 isdn overlap-receiving
 isdn incoming-voice voice
```

Related Commands

Command	Description
isdn protocol -emulate	Configures the interface to serve as either the QSIG secondary or the QSIG primary (must be the opposite setting as that set on the PBX.)
isdn switch-type (BRI)	Specifies the central office switch type on an ISDN BRI.
isdn switch-type (PRI)	Specifies the central office switch type or enables support of QSIG or Q.931 signaling on an ISDN PRI.
signaling forward	Specifies tunneling for QSIG, Q.931, H.225, and ISUP messages globally for a SIP or H.323 gateway.
signaling forward (dial-peer)	Specifies tunneling for QSIG, Q.931, H.225, and ISUP messages for a specific dial peer on a SIP or H.323 gateway.

isdn gtd

To enable generic transparency descriptor (GTD) mapping for information elements (IEs) sent in ISDN Setup messages, use the isdn gtd command in interface configuration mode. To disable GTD mapping, use the **no** form of this command.

isdn gtd
no isdn gtd

Syntax Description

This command has no arguments or keywords.

Command Default

GTD mapping is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the isdn gtd command to enable parameter mapping for the following ISDN IEs to corresponding GTD parameters:

- Originating Line Information--OLI
- Bearer Capability--USI and TMR
- Called Party Number--CPN
- Calling Party Number--CGN
- Redirecting Number--RGN, OCN and RNI

The following GTD parameters, which have no corresponding ISDN IEs, are also supported:

- Calling Party Category--CPC
- Forward Call Indicators--FCI
- Protocol Name--PRN

Examples

The following example enables GTD parameter mapping:

```
isdn gtd
```

isdn ie oli

To configure the value of the Originating Line Information (OLI) information element (IE) identifier when the gateway receives ISDN signaling from an MCI switch, use the isdn ie oli command in interface configuration mode. To disable the OLI IE identifier, use the **no** form of this command.

isdn ie oli *value*
no isdn ie oli *value*

Syntax Description

value	Hexadecimal number specifying the value that indicates OLI information from the MCI switch. Range is 00-7F.

Command Default

This command is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the isdn ie oli command to configure gateway support for the MCI ISDN variant by specifying the IE value that indicates OLI information.

Examples

The following example configures the OLI IE value to a hex value of 7A:

```
isdn ie oli 7A
```

Related Commands

Command	Description
isdn gtd	Enables GTD parameter mapping for ISDN IEs.

isdn integrate calltype all

To enable integrated mode on an ISDN PRI interface, use the **isdn integrate calltype all** command in interface configuration mode. To disable integrated mode, use the **no** form of this command.

isdn integrate calltype all
no isdn integrate calltype all

Syntax Description

This command has no arguments or keywords.

Command Default

Integrated mode is disabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Configure this command from a PRI interface only. This command is not supported from a BRI interface.

Any incoming calls from an interface that has been configured for integrate calltype all is rejected with cause-code **invalid number 0x1C** if inbound dial-peer is not selected.

Examples

In the following example, the interface is shut down.

```
Router(config)# interface Serial4/1:15
Router(config-if)# shutdown
```

In the following example, integrated mode is enabled.

```
Router(config)# interface Serial4/1:15
Router(config-if)# isdn integrate calltype all
% This command line will enable the Serial Interface to "integrated service" mode.
% The "isdn incoming-voice voice" setting will be removed from the interface.
% Continue? [confirm]
```

When you confirm, the default incoming-voice configuration is removed from the interface, and the interface is now in integrated service mode. The interface does not reset back to voice mode if an incoming call is originated from the interface.

In the following example, the interface is set to active.

```
Router(config)# interface Serial4/1:15
Router(config-if)# no shutdown
```

Related Commands

Command	Description
dial-peer data	Creates a data dial peer and enters dial-peer configuration mode.

Command	Description
dial-peer search	Optimizes voice or data dial-peer searches.
isdn incoming-voice	Routes all incoming voice calls to the modem and determine how they will be treated.

isdn network-failure-cause

To specify the cause code to pass to the PBX when a call cannot be placed or completed because of internal network failures, use the **isdn network-failure-cause** command in interface configuration mode. To disable use of this cause code, use the **no** form of this command.

isdn network-failure-cause *value*
no isdn network-failure-cause *value*

Syntax Description

value	Number, from 1 to 127. See the table below for a list of failure cause code values.

Command Default

No default behavior or values

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.

Usage Guidelines

The PBX can reroute calls based on the cause code returned by the router.

This command allows the original cause code to be changed to the value specified if the original cause code is not one of the following:

- NORMAL_CLEARING (16)
- USER_BUSY (17)
- NO_USER_RESPONDING (18)
- NO_USER_ANSWER (19)
- NUMBER_CHANGED (22)
- INVALID_NUMBER_FORMAT (28)
- UNSPECIFIED_CAUSE (31)
- UNASSIGNED_NUMBER (1)

The table below describes the cause codes.

Table 1: ISDN Failure Cause Codes

Failure Cause Code	Meaning
1	Unallocated or unassigned number.
2	No route to specified transit network.
3	No route to destination.

Failure Cause Code	Meaning
6	Channel unacceptable.
7	Call awarded and being delivered in an established channel.
16	Normal call clearing.
17	User busy.
18	No user responding.
19	No answer from user (user alerted).
21	Call rejected.
22	Number changed.
26	Nonselected user clearing.
27	Destination out of order.
28	Invalid number format.
29	Facility rejected.
30	Response to status enquiry.
31	Normal, unspecified.
34	No circuit/channel available.
38	Network out of order.
41	Temporary failure.
42	Switch congestion.
43	Access information discarded.
44	Requested channel not available.
45	Preempted.
47	Resources unavailable, unspecified.
49	Quality of service unavailable.
50	Requested facility not subscribed.
52	Outgoing calls barred.
54	Incoming calls barred.
57	Bearer capability not authorized.
58	Bearer capability not available now.

Failure Cause Code	Meaning
63	Service or option not available, unspecified.
65	Bearer capability not implemented.
66	Channel type not implemented.
69	Requested facility not implemented.
70	Only restricted digital information bearer capability is available.
79	Service or option not implemented, unspecified.
81	Invalid call reference value.
82	Identified channel does not exist.
83	Suspended call exists, but this call ID does not.
84	Call ID in use.
85	No call suspended.
86	Call with requested call ID is cleared.
88	Incompatible destination.
91	Invalid transit network selection.
95	Invalid message, unspecified.
96	Mandatory information element missing.
97	Message type nonexistent or not implemented.
98	Message not compatible with call state or message type nonexistent or not implemented.
99	Information element nonexistent or not implemented.
100	Invalid information element contents.
101	Message not compatible with call state.
102	Recovery on timer expiry.
111	Protocol error, unspecified.
127	Interworking, unspecified.

Examples

The following example specifies a cause code to pass to a PBX when a call cannot be placed or completed of internal network failures:

```
isdn network-failure-cause 28
```

isdn outgoing display-ie

To enable the display information element to be sent in the outgoing ISDN message if provided by the upper layers, such as voice or modem. To disable the displaying of the information element in the outgoing ISDN message, use the no form of this command.

isdn outgoing display-ie
no isdn outgoing display-ie

Syntax Description

There are no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The **isdn outoing display-ie** command is direction dependent, such as network-to-user or user-to-network. Not all ISDN switch types support the **isdn outgoing display-ie** command. The following shows the direction dependency by switch type, and this command can be used to override the dependency:

- ETSI (NTT, NET3,and NET5)--Only network-to-user
- DMS--Both ways
- TS014--Only network-to-user
- TS013--Only network-to-user
- 1TR6--Only network-to-user

Note The 4ESS, 5ESS, NI1, and NI2 switch types are not supported in any direction.

Note When the **isdn protocol-emulate** command is switched between network and user, this command reverts to its default value. The **isdn outoing display-ie** command must be enabled again.

Examples

The following is a running configuration, showing how the the **isdn outgoing display-ie** command is used on a specified serial interface:

```
Router# show running-config interface serial0:23
interface Serial0:23
 no ip address
```

```
dialer idle-timeout 999999
isdn switch-type primary-ni
isdn protocol-emulate network
isdn T310 30000
isdn outgoing display-ie
```

Related Commands

Command	Description
isdn protocol-emulate	Configures an ISDN data or voice port to emulate network or user functionality.

isdn protocol-emulate

To emulate the network side of an ISDN configuration for a PRI Net5 or PRI NTT switch type, use the **isdn protocol-emulate** command in interface configuration mode. To disable ISDN emulation, use the **no** form of this command.

isdn protocol-emulate {**network** | **user**}
no isdn protocol-emulate {**network** | **user**}

Syntax Description

network	Network side of an ISDN configuration.
user	User side of an ISDN configuration.

Command Default

No default behavior or values

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 concentrator.
12.1(1)T	This command was introduced in the T train.
12.2(2)XB	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco IAD2420 series. This command is not supported on the access servers in this release.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.3	This command was enhanced to support network emulation capability on the Lucent 4ESS, 5ESS, and Nortel DMS-100 ISDN switch types. These switch types can be configured as a network, but no additional changes were made and not all network side features are supported.
12.3(8)T	Added support for the PRI NTT switch type.

Usage Guidelines

- The current ISDN signaling stack can emulate the ISDN network side, but it does not conform to the specifications of the various switch types in emulating the network side.
- This command enables the Cisco IOS software to replicate the public switched network interface to a Private Branch Exchange (PBX).
- To emulate NT (network) or TE (user) functionality, use this command to configure the layer 2 and layer 3 port protocol of a BRI voice port or a PRI interface.

- Use this command to configure the Cisco AS5300 PRI interface. To disable QSIG signaling, use the **no** form of this command; the layer 2 and layer 3 protocol emulation defaults to **user**.
- This feature is supported for the PRI Net5 and PRI NTT switch types.

Examples

The following example configures the interface (configured for Net5) to emulate the network-side ISDN:

```
Router(config)# int s0:15
Router(config-if)# isdn protocol-emulate network
```

The following example configures the layer 2 and layer 3 function of T1 PRI interface 23:

```
interface serial 1:23
 isdn protocol-emulate network
```

The following example configures the layer 2 and layer 3 function of a BRI voice port:

```
interface bri 1
 isdn protocol-emulate user
```

The following example configures the layer 2 and layer 3 function of an E1 PRI interface:

```
interface serial 4:23
 isdn protocol-emulate user
```

Related Commands

Command	Description
isdn bchan-number-order	Configures an ISDN PRI interface to make outgoing call selection in ascending, descending, or round-robin order.
isdn logging	Enables logging of ISDN syslog messages.
isdn switch-type (PRI)	Specifies the central office switch type on the ISDN PRI interface.
network-clock-priority	Specifies the clock-recovery priority for the BRI voice ports in a BVM.
pri-group nec-fusion	Configures the NEC PBX to support FCCS.
show cdapi	Displays the CDAPI.
show rawmsg	Displays the raw messages owned by the required component.

isdn rlm-group

To specify a Redundant Link Manager (RLM) group number for ISDN to use, enter the **isdn rlm-group**command in controller configuration mode. To disable this function, use the **no** form of this command.

isdn rlm-group *number*
no isdn rlm-group *number*

Syntax Description

number	Number of the RLM group. Valid range is from 0 to 5.

Command Default

No RLM group is specified and the ISDN D channel is reserved for signaling information.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.4(16)	This command was removed from the Cisco IOS software code on the Cisco 2800 series and Cisco 3800 series platforms.
12.4(15)T	This command was removed from the Cisco IOS software code on the Cisco 2800 series and Cisco 3800 series platforms.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

RLM delivers ISDN Q.921 frames over an IP network. RLM affects D-channel signaling only; it does not affect the B channels. The time slot assigned originally to the D channel is freed and used as a B channel because D signaling occurs over the IP network.

The **isdn rlm-group** command allows RLM to be used to transport the D-channel information (signaling) over Ethernet.

The **isdn rlm-group** is supported only on the Cisco AS5300, AS5350, AS5400, and AS5850 series access servers. This command is not supported on Cisco 1800 series, 2800 series, 3700 series, and 3800 series platforms.

Prior to Cisco IOS Releases 12.4(16) and 12.4(15)T, the **isdn rlm-group** command could be entered on Cisco 2800 series and 3800 series platforms even though it was not supported. In some conditions, this could cause the router to reload. Effective with Cisco IOS Releases 12.4(16) and 12.4(15)T, the **isdn rlm-group** command is no longer available on the Cisco 2800 series and 3800 series platforms.

Examples

The following example defines RLM group 1:

```
interface Serial0:23
 ip address 10.0.0.1 255.0.0.0
 encapsulation ppp
 dialer map ip 10.0.0.2 name map1 1111111
```

```
dialer load-threshold 1 either
dialer-group 1
isdn switch-type primary-ni
isdn incoming-voice modem
isdn rlm-group 1
ppp authentication chap
ppp multilink
hold-queue 75 in
```

Related Commands

Command	Description
clear interface virtual-access	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole RLM group.
retry keepalive	Allows consecutive keepalive failures a specified amount of time before the link is declared down.
server (RLM)	Defines the IP addresses of the server.
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under the RLM group.
timer	Overwrites the default setting of timeout values.

isdn skipsend-idverify

To stop the user side of a BRI interface from sending ID verify information, use the **isdn skipsend-idverify** command in interface configuration mode. To restore the user-side notification, use the **no** form of this command.

isdn skipsend-idverify
no isdn skipsend-idverify

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the user side sends the ID verify information. The **no** form of this command is in effect by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(3)XI	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

For user-side BRI interfaces, you can send ID verify messages to confirm the status of a particular terminal endpoint identifier (TEI) when there is doubt about whether the TEI is in use (for example, after a Layer 1/Layer 2 flap). ID is the TEI value.

For network-side BRI interfaces, the command should always be set. In some cases, the command will automatically be configured after the BRI network-side protocol emulation is set. If not, you can manually configure the command on the network-side BRI interface. After the command has been configured either automatically or manually, it cannot be further changed. A network-side BRI interface should always be set so that it does not send ID verify information.

Examples

The following example shows user-side output, with the default in effect, so the ID verify is sent:

```
Router# show isdn status br0/0
Global ISDN Switchtype = basic-net3
ISDN BRI0/0 interface
        dsl 0, interface ISDN Switchtype = basic-net3
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 95, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 0 CCBs = 0
    The Free Channel Mask:  0x80000003
    Total Allocated ISDN CCBs = 0
```

The following sample output shows network-side output, with the default in effect:

```
Ovld02#show isdn status
Global ISDN Switchtype = basic-net3
```

```
ISDN BRI0/1/0:0 interface
        dsl 0, interface ISDN Switchtype = basic-qsig
         **** User side configuration ****
    Layer 1 Status:
        DEACTIVATED
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = TEI_ASSIGNED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 0 CCBs = 0
    The Free Channel Mask:  0x80000003
ISDN BRI0/1/1:0 interface
        dsl 1, interface ISDN Switchtype = basic-net3
    Layer 1 Status:
        SHUTDOWN
    Layer 2 Status:
        Layer 2 NOT Activated
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 1 CCBs = 0
    The Free Channel Mask:  0x00000000
ISDN Serial0/3/0:23 interface
        ******* Network side configuration *******
        dsl 2, interface ISDN Switchtype = primary-qsig
         **** Network side configuration ****
 --More--
Mar 31 17:29:43.447 CST: %SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement
will be required in    Layer 1 Status:
        DEACTIVATED
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = TEI_ASSIGNED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 2 CCBs = 0
    The Free Channel Mask:  0x00000000
    Number of L2 Discards = 0, L2 Session ID = 0
    Total Allocated ISDN CCBs = 0
```

The following sample output shows the BRI interface with the **isdn skipsend-idverify** command in effect (so the ID verify will *not* be sent):

```
Router# show run interface br0/0
Building configuration...
Current configuration : 185 bytes
!
interface BRI0/0
 no ip address
 encapsulation ppp
 no ip mroute-cache
 isdn switch-type basic-net3
 isdn point-to-point-setup
 isdn incoming-voice voice
 isdn skipsend-idverify
end
```

The following example shows the return to default so that the ID verify will be sent:

```
Router# configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#interface br0/0
router(config-if)#no isdn skipsend-idverify
router(config-if)#
```

The following output shows that the skip send has been removed (so the ID verify information *will* be sent):

```
Router# show run interface br0/0
Building configuration...
Current configuration : 161 bytes
!
interface BRI0/0
 no ip address
 encapsulation ppp
 no ip mroute-cache
 isdn switch-type basic-net3
 isdn point-to-point-setup
 isdn incoming-voice voice
end
```

This configuration example shows the warning message that appears when the command is applied or when the **no** form of the command is entered on a network-side BRI interface:

```
Router# configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#int br1/1
router(config-if)#isdn skipsend-idverify
% Network side should never send ID VERIFY  <---- warning message
router(config-if)#
```

Related Commands

Command	Description
interface bri	Specifies the interface and enters interface configuration mode.

isdn spoofing

To enable ISDN spoofing so that loss of Layer 1 or Layer 2 connectivity of the ISDN BRI interface is not detected by the Trunk Group Resource Manager (TGRM) or similar application, use the **isdn spoofing** command in interface configuration mode. To disable ISDN spoofing so the TGRM or similar application can detect when the BRI interface is not operational (when the Layer 1 or Layer 2 connection is down), use the **no** form of this command.

isdn spoofing
no isdn spoofing

Syntax Description

This command has no arguments or keywords.

Command Default

The ISDN BRI interface is spoofing, which means that applications always see the BRI interface connection as operational (unless the interface has been manually shut down [ADMINDOWN state]).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The ISDN BRI interface is spoofing by default. Spoofing makes the ISDN BRI interface available (up) for operation (for dialing in ISDN), even if the interface is down. For an ISDN BRI interface to be set to a down condition, the interface must be manually shut down (IDBS_ADMINDOWN state). Spoofing enables upper layers to dial out even when the interface is down.

Some upper layer modules, such as TGRM and similar applications, allow dial-out only if the channel is available. If the record for TGRM or similar application is notified of the actual status of BRI, then the TGRM or similar application can dial out accordingly. In this case, the **no isdn spoofing** command is appropriate.

Note ISDN spoofing can be applied only to BRI interfaces--it does not apply to PRI interfaces.

Examples

The following example shows how to configure an ISDN BRI interface to disable ISDN spoofing:

```
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface bri0/0

Router(config-if)# no isdn spoofing
```

Related Commands

Command	Description
interface bri	Configures a BRI interface and enters interface configuration mode.
show isdn status	Displays the status of all ISDN interfaces or a specific ISDN interface.

isdn supp-service calldiversion

To ensure that all calls on an ISDN serial interface can be traced if diverted, use the **isdn supp-service calldiversion** command in interface configuration mode. To disable tracing of diverted ISDN calls, use the **no** form of this command.

isdn supp-service calldiversion
no isdn supp-service calldiversion

Syntax Description

This command has no arguments or keywords.

Command Default

VoIP calls, when diverted, are not traceable and are translated into a Redirection Information Element (RedirectionIE).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

You must explicitly specify an ISDN serial interface. The D channel is always the :23 channel for T1 and the :15 channel for E1.

To enable traceability, the call diversion service requires that a VoIP call (when diverted) translates into a divertingLegInformation2 IE instead of a RedirectionIE. When the **isdn supp-service calldiversion** command is configured, the redirecting information coming from the application is packed in the Facility Information Element (FAC IE) as DiversionLeg2 information and sent in the outgoing SETUP message.

The **isdn supp-service calldiversion** command works only for NET5 switches.

Examples

The following example shows how to configure the primary NET5 switch so that the call diversion tracing service is enabled:

```
interface serial3:23
 no ip address
 isdn switch-type primary-net5
 isdn supp-service calldiversion
```

Related Commands

Command	Description
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller for ISDN PRI, CAS, or robbed-bit signaling.

isdn supp-service mcid

To enable an ISDN serial interface for Malicious Caller Identification (MCID), use the **isdn supp-service mcid** command in interface configuration mode. To disable MCID functionality, use the **no** form of this command.

isdn supp-service mcid
no isdn supp-service mcid

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The ISDN interface must use the NET5 switch type, which is set using the **isdn switch-type primary-net5** command. Protocol emulation must be set to user, which is the default for the **isdn protocol-emulate** command. This command is valid only at the ISDN interface level.

Examples

The following configuration example shows MCID enabled for the PRI:

```
interface serial0:23
 isdn switch-type primary-net5
 ip address 10.10.10.0. 255.255.255.0
 isdn supp-service mcid
 isdn T-Activate 5000
```

Related Commands

Command	Description
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller for ISDN PRI, channel-associated signaling, or robbed-bit signaling.
isdn protocol-emulate	Configures the PRI interface to serve as either the primary (user) or the secondary (network).
isdn switch-type	Specifies the central office switch type on the ISDN interface.
isdn t-activate	Specifies how long the ISDN serial interface must wait for the malicious caller to be identified.

isdn supp-service name calling

To set the calling name display parameters sent out on an ISDN serial interface, use the **isdn supp-service name calling** command in interface configuration mode. To disable calling name delivery, use the **no** form of this command.

isdn supp-service name calling [**ie** | **operation-value-tag** | **profile** {**Network Extension operation-value-tag** {**ecma** | **iso** | **local**} | **ROSE**}]
no isdn supp-service name calling

Syntax Description

ie	(Optional) Specifies that the value of the calling name information element (ie) is to be sent.
operation-value-tag	(Optional) Specifies that the operation value tag for the calling name is to be sent.
profile	(Optional) Specifies that a particular protocol profile is to be sent.
Network-Extension	Specifies the networking extension (0x9F).
ecma	Specifies that the European Computer Manufacturers' Association (ECMA) object identifier (OID) global value (protocol profile 0x06 04 2B 0C 09 00) is to be sent.
iso	Specifies that the International Standards Organization (ISO) OID global value (protocol profile 0x06 05 28 EC 2C 00 00) is to be sent.
local	Specifies that the local OID global value (protocol profile 0x02 01 00) is to be sent.
ROSE	(Optional) Specifies that the Remote Operations Service Element (ROSE) value (protocol profile 0x91) is to be sent.

Command Default

Calling name delivery is disabled, so no calling-name display parameters are set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(15)T1	The **ie**, **operation-value-tag**, **profile**, **Network Extension**, **ecma**, **iso**, **local**, and **ROSE** keywordswere added.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You must explicitly specify an ISDN serial interface. The D channel is always the :23 channel for T1 and the :15 channel for E1.

Under the serial interface (interface serial command), the **isdn supp-service name calling** command must be configured so that when the calling name comes in the Facility Information Element (IE) of the ISDN setup message, the gateway sends the calling name to the Cisco Unified Communications Manager as a Display IE. If the **isdn supp-service name calling** command is not configured under the ISDN serial interface, the calling

name in the FacilityIE is sent as user-to-user data to the Cisco Unified Communications Manager without the display data.

Beginning with Cisco IOS Release 12.4(15)T1, the **ie**, **operation-value-tag**, **profile**, **Network Extension**, **ecma**, **iso**, **local**, and **ROSE** keywords were added to provide more specific information in defining calling name information that is to be sent.

Examples

The following example shows the H.323 Display feature without buffering for ISDN trunks being configured at the voice service level:

```
voice service voip
 h323
 h225 display-ie ccm-compatible
```

The following example shows the H.323 Display feature without buffering for ISDN trunks being configured at the voice class level:

```
voice class h323 1
 h225 display-ie ccm-compatible [system]
```

The following example shows the H.323 name display information on ISDN trunks:

```
interface Serial0/3/0:23
 no ip address
 encapsulation hdlc
 isdn switch-type primary-ni
 isdn incoming-voice voice
 isdn map address *. plan isdn type unknown
 isdn supp-service name calling
 isdn bind-l3 ccm-manager
 no cdp enable
```

Related Commands

Command	Description
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller for ISDN PRI, channel-associated signaling, or robbed-bit signaling.

isdn supp-service tbct

To enable ISDN Two B-Channel Transfer (TBCT) on PRI trunks, use the **isdn supp-service tbct** command in interface or trunk group configuration mode. To reset to the default, use the **no** form of this command.

isdn supp-service tbct [**notify-on-clear** | **tbct-with-crflg**]
no isdn supp-service tbct

Syntax Description

notify -on-clear	(Optional) ISDN switch notifies the gateway whenever a transferred call is cleared.
tbct-with-crflg	(Optional) Includes the call reference flag while sending a TBCT request.

Command Default

TBCT is disabled.

Command Modes

Interface configuration (config-if)
Trunk-group configuration (config-trunkgroup)

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

This command enables TBCT for a specific PRI when used in interface configuration mode. This command configures TBCT for all PRIs in a trunk group when used in trunk-group configuration mode.

The **notify-on-clear** keyword is necessary for the gateway to track billing. This keyword is supported only for user-side ISDN interfaces. You must configure the ISDN switch to send a notify message when a call is cleared.

On some PBX switches, the call reference flag (including the call reference value of the other call) is mandatory. To include the call reference flag in a TBCT request, use the **tbct - with - crflg** keyword. The call reference flag can be 00 or 80. So, for example, if the call reference value is 02, the call reference flag is 0002 or 8002.

Examples

The following example shows how to enable TBCT for interface 0:23:

```
interface Serial0:23
 isdn supp-service tbct
```

The following example shows how to enable TBCT for trunk group 1:

```
trunk group 1
 isdn supp-service tbct
```

The following example shows how to include the call reference flag in TBCT requests for trunk group 1:

```
trunk group 1
 isdn supp-service tbct tbct-with-crflg
```

Related Commands

Command	Description
call application voice transfer mode	Specifies the call-transfer behavior of a TCL or VoiceXML application.
show call active voice redirect	Displays information about active calls that are being redirected using RTPvt or TBCT.
tbct clear call	Terminates billing statistics for one or more active TBCT calls.
tbct max call-duration	Sets the maximum duration allowed for a call that is redirected using TBCT.
tbct max calls	Sets the maximum number of active calls that can use TBCT.
trunk group	Enters trunk-group configuration mode to define or modify a trunk group.

isdn t-activate



Note Effective with Cisco IOS Release 12.4(11)T, the **isdn t-activate** command is replaced by the **isdn timer** command. See the **isdn timer** command for more information.

To specify how long the gateway waits for a response from the Public Switched Telephone Network (PSTN) after sending a Malicious Call Identification (MCID) request, use the **isdn t-activate** command in interface configuration mode. To disable the timer, use the **no** form of this command.

isdn t-activate *milliseconds*
no isdn t-activate *milliseconds*

Syntax Description

milliseconds	Number of milliseconds (ms) that the router waits for a response from the PSTN after sending a MCID request. Range is 1000 to 15000. Default is 4000; 5000 is recommended.

Command Default

The default wait period is 4000 ms.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(11)T	This command was replaced by the **isdn timer** command.

Usage Guidelines

This command starts a timer when the voice gateway sends a Facility message to the PSTN. If a response is not received within the specified time, the Tool Command Language (TCL) Interactive Voice Response (IVR) script for MCID is notified. Depending on how the script is written, it could reinvoke MCID or perform some other action, such as playing a message if the MCID attempt fails. This command is valid only at the ISDN interface level. The ISDN interface must use the NET5 switch type, which is set using the **isdn switch-type primary-net5** command. Protocol emulation must be set to user, which is the default for the **isdn protocol-emulate** command.

Examples

The following example shows the setting of the timer to a wait period of 5000 ms:

```
interface serial0:23
 isdn switch-type primary-net5
 ip address 10.10.10.0 255.255.255.0
 isdn suppserv mcid
 isdn t-activate 5000
```

Related Commands

Command	Description
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller for ISDN PRI, channel-associated signaling, or robbed-bit signaling.
isdn protocol-emulate	Configures the PRI interface to serve as either the primary (user) or the secondary (network).
isdn switch-type	Specifies the central office switch type on the ISDN interface.
isdn suppserv mcid	Configures an ISDN serial interface for MCID.

isdn tei-negotiation (interface)

To configure when Layer 2 becomes active and ISDN terminal endpoint identifier (TEI) negotiation occurs, use the **isdn tei-negotiation** command in interface configuration mode. To remove TEI negotiation from an interface, use the **no** form of this command.

isdn tei-negotiation {**first-call** | **powerup**} {**preserve** | **remove**}
no isdn tei-negotiation

Syntax Description

first-call	ISDN TEI negotiation occurs when the first ISDN call is placed or received.
powerup	ISDN TEI negotiation occurs when the router is powered up.
preserve	Preserves dynamic TEI negotiation when ISDN Layer 1 flaps, and when the **clear interface** or the **shutdown**and **no shutdown** EXEC commands are executed.
remove	Removes dynamic TEI negotiation when ISDN Layer 1 flaps, and when the **clear interface** or the **shutdown** and **no shutdown** EXEC commands are executed.

Command Default

The **powerup** state is the default condition. Depending on the ISDN switch type configured, the default action is to preserve or remove the TEI negotiation options.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3T	This command was introduced as an interface command.
12.2	The **preserve** and **remove** keywords were added.

Usage Guidelines

This command is for BRI configuration only.

The **first-call** and **powerup**, and **preserve** and **remove**command pairs are mutually exclusive, that is, you must choose only one command from either the **first-call** and **powerup** or **preserve** and **remove**command pairs, per command line.

The **no isdn tei-negotiation**command returns the configuration to default to the **powerup** state.

Use of the **preserve**keyword causes different behavior depending on the ISDN switch type configured, that is, the TEI negotiation configured will be preserved during ISDN Layer 1 flaps, and when the **clear interface** or the **shutdown** and **no shutdown** EXEC commands are executed, on the switch types listed in the table below.

Table 2: Switch Types with Preserved TEI Negotiation

Switch Type	Cisco IOS Keyword
French ISDN switch types	**vn2, vn3**
Lucent (AT&T) basic rate 5ESS switch	**basic-5ess**

Switch Type	Cisco IOS Keyword
Northern Telecom DMS-100 basic rate switch	**basic-dms100**
National ISDN basic rate switch	**basic-ni**
PINX (PBX) switches with QSIG signaling per Q.931	**basic-qsig**

For all other ISDN switch types, the TEI negotiation will be removed during ISDN Layer 1 flaps, and when the **clear interface** or the **shutdown** and **no shutdown** EXEC commands are executed. Use the **remove** keyword to specifically set one of the switches listed in the table above to the remove state.

The **first-call** keyword and its functionality are not supported on U.S. switch types (basic-ni, basic-5ess, basic-dms100, primary-ni, primary-4ess, primary-5ess, and primary-dms100), especially for service profile identifier (SPID) negotiations. The **first-call** keyword and its functionality are supported on European switch types (basic-net3 and primary-net5) to prevent Layer 2 activity when there are no Layer 3 calls.

Examples

The following example shows the ISDN TEI negotiation configuration with default settings. (Defaults settings do not appear in the router configuration.)

```
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 cdapi buffers regular 0
 cdapi buffers raw 0
 cdapi buffers large 0
```

The following example shows how to set TEI negotiation timing to the first call:

```
Router(config-if)# isdn tei-negotiation first-call
Router(config-if)# exit
Router(config)# exit
Router# show startup-config
.
.
.
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 isdn tei-negotiation first-call
 cdapi buffers regular 0
 cdapi buffers raw 0
 cdapi buffers large 0interface BRI0/0
```

The following example shows how to change TEI negotiation timing back to the default power-up state:

```
Router(config-if)# no isdn tei-negotiation
Router(config-if)# exit
Router(config)# exit
Router# show startup-config
.
.
.
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 cdapi buffers regular 0
```

```
 cdapi buffers raw 0
 cdapi buffers large 0
```

The following example shows how to remove TEI negotiation when ISDN Layer 1 flaps (the preserve state is the default for the National ISDN basic rate switch):

```
Router(config-if)# isdn tei-negotiation remove
Router(config-if)# exit
Router(config)# exit
Router# show startup-config
.
.
.
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 isdn tei-negotiation first-call
 isdn tei-negotiation remove
 cdapi buffers regular 0
 cdapi buffers raw 0
 cdapi buffers large 0
```

The following example shows how to return the National ISDN basic rate switch to its default preserve state:

```
Router(config-if)# no isdn tei-negotiation
Router(config-if)# exit
Router(config)# exit
Router# show startup-config
.
.
.
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 isdn tei-negotiation first-call
 cdapi buffers regular 0
 cdapi buffers raw 0
 cdapi buffers large 0
```

iua

To specify backhaul using Stream Control Transmission Protocol (SCTP) and to enter IDSN User Adaptation Layer (IUA) configuration mode, use the **iua** command in terminal configuration mode.

iua

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300 and Cisco AS5850.
12.2(15)T	This command was implemented on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series; and Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.

Usage Guidelines

You must first enter IUA configuration mode to access SCTP configuration mode. First enter IUA configuration mode by using the example below and then enter sctp at the Router(config-iua)#prompt to bring up SCTP configuration mode. See the sctp command.

Examples

The following example shows how to enter iua configuration mode:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# iua
Router(config-iua)#
```

The following example shows how to configure the failover-timer by setting the failover time (in milliseconds) to 1 second for a particular AS:

```
Router(config-iua)# as as5400-3 fail-over-timer 1000
```

The following example configure the number of SCTP streams for this AS to 57, which is the maximum value allowed:

```
Router(config-iua)# as as5400-3 sctp-streams 57
```

Related Commands

Command	Description
isdn bind -L3 iua-backhaul	Specifies ISDN backhaul using SCTP for an interface.
show iua as	Shows information about the current condition of an AS.
show iua asp	Shows information about the current condition of an ASP.

ivr asr-server

To specify the location of an external media server that provides automatic speech recognition (ASR) functionality to voice applications, use the **ivr asr-server** command in global configuration mode. To remove the server location, use the **no** form of this command.

ivr asr-server *url*
no ivr asr-server

Syntax Description

url	Location of the ASR resource on the media server, in uniform resource locator (URL) format.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 26.2.1	This command was modified to display warning message for insecure protocol usage.
12.4(15)T	The *url* argument was modified to accept a Media Resource Control Protocol version 2 (MRCP v2) server URL.
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

This command sets the server location globally for all voice applications on the gateway.

For Nuance media servers that use the default installation, specify the URL as follows:

ivr asr -server rtsp://*host***:***port]***/recognizer**

(*host* is the host name of the media server; **:***port* is optional.)

For media servers using MRCP v2, specify the URL as follows:

ivr asr -server sip:*server-name@host-name* | *ip-address*

You can specify the location of the media server within a VoiceXML document, overriding the Cisco gateway configuration. For more information, see the Cisco VoiceXML Programmer's Guide.

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

Examples

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

```
Device(config)#ivr asr-server rtsp://asr_serv/recognizer
SECURITY WARNING - Module: DEFAULT_VOICE_CONFIG, Command: ivr asr-server
rtsp://asr_serv/recognizer,
Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of
encryption and authentication,
Description: ivr asr-server configured with insecure RTSP URL, Remediation: Use secure
protocols instead of insecure RTSP
Device(config)#
```

Examples

The following example specifies that voice applications use the ASR server named "asr_serv":

```
Router(config)# ivr asr-server rtsp://asr_serv/recognizer
```

The following example specifies that voice applications use the MRCP v2 ASR server named "asr_mrcpv2serv":

```
Router(config)# ivr asr-server sip:asr_mrcpv2serv@mediaserver.com
```

Related Commands

Command	Description
ivr tts -server	Specifies the location of a media server that provides TTS functionality to voice applications.
ivr tts -voice-profile	Specifies the location of the voice profile that is used by the TTS server.

ivr autoload mode

To load files from TFTP to memory using either verbose or silent mode, use the **ivr autoload mode** command in global configuration mode. To disable this function, use the **no** form of this command.

ivr autoload mode { **verbose** | **silent** } { **url** *location* | [**retry** *number*] }
no ivr autoload

Syntax Description

verbose	Displays the file transfer activity to the console. This mode is recommended while debugging.
silent	Performs the file transfer in silent mode, meaning that no file transfer activity is displayed to the console.
url *location*	URL that is used to locate the index file that contains a list of all available audio files.
retry *number*	(Optional) Number of times that the system tries to transfer a file when there are errors. This parameter applies to each file transfer. Range is from 1 to 5. Default is 3.

Command Default

Silent

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 26.2.1	This command was modified to display warning message for insecure protocol usage.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.0(7)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.

Usage Guidelines

The index file contains a list of audio files (URL) that can be downloaded from the TFTP server. Use the **ivr autoload mode** command to download audio files from TFTP to memory. The command only starts up a background process. The background process (loader) does the actual downloading of the files.

The background process first reads the index file from either Flash or TFTP. It parses the files line by line looking for the URL. It ignores lines that start with # as comment lines. Once it has a correct URL, it tries to read that.au file into memory and creates a media object. If there are any errors during the reading of the file, it retries the configured number of times. If the mode is set to **verbose**, the loader logs the transaction to console. Once parsing has reached the end of the index file, the background process exits memory.

Perform the following checks before initiating the background process. If one of the checks fails, it indicates the background process is not started, and instead you see an error response to the command.

- Check if any prompt is being actively used (IVR is actively playing some prompts). If there are active prompts, the command fails, displaying the following error message (.au files are also referred to as prompts): "Command is not allowed when prompts are active".

- Check if there is already a background process in progress. If there is a process, the command fails, displaying the following error: "Previous autoload command is still in progress".
- If the **ivr autoload url** command has already been configured, the user sees the following response when the command is issued: "Previous command is being replaced".
- When the **no ivr autoload url** command is issued, while there was already an **ivr autoload url** command in progress, the original command is aborted.

The audio files (prompts) loaded using the **ivr autoload url** command are not dynamically swapped out of memory. They are considered to be autoloaded prompts, as opposed to dynamic prompts. (See the **ivr prompt memory** command for details on dynamic prompts.)



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

Examples

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

```
Device(config)#ivr autoload mode silent url tftp://blue/orange/tclware/index4
SECURITY WARNING - Module: IVR, Command: ivr autoload mode silent url
tftp://blue/orange/tclware/index4,
Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of
encryption and authentication,
Description: IVR autoload mode configured with insecure TFTP protocol - vulnerable to content
 tampering,
Remediation: Use secure protocols such as HTTPS, SFTP, or SCP instead of insecure HTTP,
FTP, or TFTP
```

The following example configures verbose mode:

```
ivr autoload mode verbose url tftp://blue/orange/tclware/index4 retry 3
```

The following example shows the resulting index file:

```
more index4
tftp://blue/orange/tclware/au/en/en_one.au
tftp://blue/orange/tclware/au/ch/ch_one.au
tftp://blue/orange/tclware/au/ch/ch_one.au
```

The following example shows an index file on Flash memory:

flash:index

Related Commands

Command	Description
ivr prompt memory	Configures the maximum amount of memory that the dynamic audio files occupy in memory.

ivr prompt memory

To configure the maximum amount of memory that the dynamic audio files (prompts) occupy in memory, use the **ivr prompt memory** command in global configuration mode. To disable the maximum memory size, use the **no** form of this command.

ivr prompt memory *size* **files** *number*
no ivr prompt memory

Syntax Description

size	Maximum memory to be used by the free dynamic prompts, in kilobytes. Range is 128 to 16384. The default is 128.
files *number*	Number of files that can stay in memory. Range is 50 to 1000. The default is 200.

Command Default

Memory size: 128 KB Number of files: 200

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

When both the *number* and *size* parameters are specified, the minimum memory out of the two is used for memory calculations.

All the prompts that are not autoloaded or fixed are considered dynamic. Dynamic prompts are loaded in to memory from TFTP or Flash, as and when they are needed. When they are actively used for playing prompts, they are considered to be in "active" state. However, once the prompt playing is complete, these prompts are no longer active and are considered to be in a free state.

The free prompts either stay in memory or are removed from memory depending on the availability of space in memory for these free prompts. This command essentially specifies a maximum memory to be used for these free prompts.

The free prompts are saved in memory and are queued in a wait queue. When the wait queueis full (either because the totally memory occupied by the free prompts exceeds the maximum configured value or the number of files in the wait queue exceeds maximum configured), oldest free prompts are removed from memory.

Examples

The following example sets memory size to 2048 KB and number of files to 500:

```
ivr prompt memory 2048 files 500
```

Related Commands

Command	Description
ivr autoload	Loads files from a particular TFTP server.
show call prompt -mem-usage	Displays the memory site use by prompts.
ivr prompt streamed	Streams audio prompts from particular media types during playback.

ivr autoload url

To load files from a particular TFTP server (as indicated by a defined URL), use the **ivr autoload** command in global configuration mode. To disable this function, use the **no** form of this command.

ivr autoload url *location*
no ivr autoload url *location*

Syntax Description

url *location*	URL that is to be used to locate the index file that contains a list of all available audio files.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 26.2.1	This command was modified to display warning message for insecure protocol usage.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.0(7)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.

Usage Guidelines

The index file contains a list of audio files URLs that can be downloaded from the TFTP server. Use the **ivr autoload url** command to download audio files from TFTP to memory. The command starts a background process (loader) that does the actual downloading of the files.

The background process first reads the index file from either Flash memory or TFTP. It parses the files line by line, looking for the URL. It ignores lines that start with # as comment lines. Once it has a correct URL, it tries to read that .au file into memory and creates a media object. If there are any errors during the reading of the file, it retries the configured number of times. If the *mode* is set to "verbose," in the **ivr autoload mode** command the loader logs the transaction to console. Once parsing has reached the end of the index file, the background process exits memory.

Perform the following checks before initiating the background process. If one of the checks fails, it indicates that the background process is not started, and instead you see an error response to the command.

- Check to see if any prompt is being actively used (IVR is actively playing some prompts). If there are active prompts, the command fails, displaying the following error message (.au files are also referred to as prompts): "Command is not allowed when prompts are active"
- Check to see if there is already a background process in progress. If there is a process, the command fails, displaying the following error: "Previous autoload command is still in progress"
- Check to see if an earlier **ivr autoload url** command has already been configured. If configured, the user sees the following response when the command is issued again: "previous command is being replaced"

- When the **no ivr autoload url** command is issued, if there is already an **ivr autoload url** command in progress, it is aborted.

The audio files (prompts) loaded using the **ivr autoload** command are not dynamically swapped out of memory. They are considered as autoloaded prompts as opposed to "dynamic" prompts. See the **ivr prompt memory** command for details on dynamic prompts.

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

Examples

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

```
Device(config)#ivr autoload url tftp://blue/orange/tclware/index4
 previous autoload command will be replaced

SECURITY WARNING - Module: DEFAULT_VOICE_CONFIG, Command: ivr autoload url
tftp://blue/orange/tclware/index4 ,
Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of
encryption and authentication,
Description: ivr autoload url voice configured with insecure FTP/HTTP/TFTP URL protocol,
Remediation: Use secure protocols such as HTTPS, SFTP, or SCP instead of insecure HTTP,
FTP, or TFTP
Device(config)#
```

Examples

The following example loads audio files from the TFTP server (located at //jurai/mgindi/tclware/index4):

```
ivr autoload url tftp://jurai/mgindi/tclware/index4
```

The following example shows the resulting index file:

```
more index4
tftp://jurai/mgindi/tclware/au/en/en_one.au
tftp://jurai/mgindi/tclware/au/ch/ch_one.au
tftp://jurai/mgindi/tclware/au/ch/ch_one.au
```

The following example shows an index file on Flash:

```
flash:index
```

Related Commands

Command	Description
ivr prompt memory	Configures the maximum amount of memory that the dynamic audio files (prompts) occupy in memory.

ivr contact-center

To enable a specific set of debug commands on a Cisco router that is being used in a contact center, use the **ivr command-cente**r command in global configuration mode. To stop automatically enabling these debug commands after the router is reloaded, use the **no** form of this command.

ivr command-center
no ivr command-center

Syntax Description

This command has no arguments or keywords.

Command Default

Specific individual debug commands must be manually enabled each time the router is reloaded.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T2	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(15)T4	The ccapi, cch323, and ccsip error debugs were included in the output display.
12.4(20)YA	This command was integrated into Cisco IOS Release 12.4(20)YA.

Usage Guidelines

To troubleshoot a Cisco router that is being used in a contact center, it is often necessary to enable specific debug commands to display error messages. Typically, you must manually enable the individual debug commands each time the router is reloaded. Use the **ivr contact-center** command to enable the following debug commands and to automatically re-enable these commands each time the router is reloaded:

- **debug ccsip error**
- **debug cch323 error**
- **debug http client error**
- **debug mrcp error**
- **debug rtsp error**
- **debug voip application error**
- **debug voip application vxml error**
- **debug voice ccapi error**

While this command is configured, the listed debug commands cannot be disabled. Attempts to disable any of these debug commands while the **ivr contact-center** command is configured will display a warning message and the debug command will not be disabled.

Configuring the **no ivr contact-center** command does not disable the listed debug commands. To disable these debug commands after configuring the **no ivr contact-center** command, you must either manually

disable each individual debug command or reload the router, after which these debug commands are not re-enabled.

You can verify that the listed debug commands are enabled after you configure the **ivr contact-center** command by using the **show debug**command.

Examples

The following partial output from the **show running-config** command shows that the **ivr contact-center** command is enabled:

```
Router# show running-confi
Building configuration...
Current configuration : 20256 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname c5400-02
!
! ***** snipped *****
!
ivr contact-center
ivr prompt memory 16384 files 1000
ivr asr-server rtsp://CVPASR/media/speechrecognizer
ivr tts-server rtsp://CVPTTS/media/speechsynthesizer
!
! ***** snipped *****
```

The following output from the **show debug**command displays current debugging information that includes the error debug messages automatically enabled by the **ivr contact-center**command:

To display current debugging information that includes the error debug messages automatically enabled by "ivr contact-center", use the show debug command in privileged EXEC mode.

```
c3825-01(config)#ivr contact-center
c3825-01(config)#end
Router# show debug
CCH323 SPI: Error debug is enabled
CCAPI:
  debug voip ccapi error call is ON (filter is OFF)
  debug voip ccapi error software is ON
CCSIP SPI: SIP error debug tracing is enabled   (filter is OFF)
HTTP Client:
  HTTP Client Error debugging is on
APPLICATION:
  debug voip application error is ON
RTSP:
  RTSP client Protocol Error debugging is on
MRCP:
  MRCP client error debugging is on
VXML:
  debug voip application vxml error software is ON
  debug voip application vxml error call is ON (filter is OFF)
c3825-01#
```

Related Commands

Command	Description
debug http client error	Displays error messages for the HTTP client.
debug mrcp error	Displays error messages for Media Resource Control Protocol (MRCP) operations.
debug rtsp error	Displays debug information about the Real-Time Streaming Protocol (RTSP) client.
debug voip application error	Displays error messages for all voice applications.
debug voip application vxml error	Displays error messages for a VoiceXML application.
debug voice ccapi error	Displays error messages for the call control application programming interface (CCAPI) contents.
debug ccsip error	Displays Session Initiation Protocol (SIP)-related error messages.
debug cch323 error	Displays error messages for components within the H.323 subsystem.
show debug	Displays current debugging information automatically enabled by **ivr contact-center** command.

ivr language link

To link configured language packages, use the **ivr language link** command in global configuration mode. To delink the configured language packages, use the **no** form of this command.

ivr language link {**all** | **on-demand**}
no ivr language link

Syntax Description

all	Links all the configured language packages.
on-demand	Links the language packages when asked for.

Command Modes

Global configuration (config)

Command Default

The language packages are not linked.

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to link all the configured language packages:

```
Router# configure terminal
Router(config)# ivr language link all
```

Related Commands

Command	Description
ivr asr-server	Specifies the location of an external media server that provides ASR functionality to voice applications.

ivr prompt cutoff-threshold

To configure the maximum delay time for audio prompts, use the **ivr prompt cut-off threshold** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ivr prompt cutoff-threshold *time*
no ivr prompt cutoff-threshold

Syntax Description

time	Maximum delay time, in milliseconds (ms). The range is from 120 to 1000.

Command Default

The maximum delay time is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to configure the maximum delay time for audio prompts:

```
Router# configure terminal
Router(config)# ivr prompt cutoff-threshold 129
```

Related Commands

Command	Description
ivr prompt streamed	Streams audio prompts from particular media types during playback.

ivr prompt streamed

To stream audio prompts from particular media types during playback, use the **ivr prompt streamed** command in global configuration mode. To reset to the default, use the **no** form of this command.

ivr prompt streamed { **all** | **flash** | **http** | **none** }
no ivr prompt streamed { **all** | **flash** | **http** | **none** }

Syntax Description

all	All audio prompts, from all URL types (Flash memory, HTTP).
flash	Audio prompts from Flash memory.
http	Audio prompts from an HTTP URL. This is the default value.
none	No audio prompts from any media type.

Command Default

Audio prompts from HTTP URLs and other media types are not streamed during playback.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 26.2.1	This command was modified to display warning message for insecure protocol usage.
12.4(20)T	The **tftp** keyword was removed.
12.4(15)T	The command default was changed from streaming for audio prompts during playback to no streaming.
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

To enable streaming for multiple media types, either enter this command for each URL type or enter the ivr prompt streamed all command. If you do not enter this command, audio prompts from HTTP servers and Flash servers are not streamed during playback.

Note Prompts from a Real Time Streaming Protocol (RTSP) server are not controlled by this command and are always streamed during playback.

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

Examples

The following example indicates that audio prompts from Flash memory are streamed when they are played back:

```
ivr prompt streamed flash
```

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

```
Device(config)#ivr prompt streamed http
SECURITY WARNING - Module: IVR, Command: ivr prompt streamed http,
Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of
encryption and authentication,
Description: IVR prompt streaming configured with insecure HTTP protocol - vulnerable to
content tampering,
Remediation: Use secure protocols such as HTTPS, SFTP, or SCP instead of insecure HTTP,
FTP, or TFTP
```

Related Commands

Command	Description
ivr prompt memory	Sets the maximum amount of memory that dynamic audio prompts can occupy in memory.

ivr record cpu flash

To configure the maximum percentage allowed for the flash write process in CPU, use the **ivr record cpu flash**command in global configuration mode. To disable this configuration, use the **no** form of this command.

ivr record cpu flash *number*
no ivr record cpu flash

Syntax Description

number	Numeric label that specifies the maximum percentage allowed for the flash write process in the CPU. The range is from 1 to 99. The default is 99.

Command Default

The maximum percentage is configured to 99.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows that the flash recording allowed is set to 50 percent:

```
Router# configure terminal
Router(config)# ivr record cpu flash 50
```

Related Commands

Command	Description
ivr prompt streamed	Streams audio prompts from particular media types during playback.

ivr record jitter

To set the maximum amount of jitter memory that can be used to record voice messages during a single call session, use the **ivr record jitter** command in global configuration mode. To free up the allocated jitter memory, use **no** form of this command.

ivr record jitter *WORD kilobytes*
no ivr record jitter *WORD*

Syntax Description

WORD	Specifies string containing url scheme.
tftp: | http:	Specifies the protocol.
kilobytes	Memory size in kilobytes. Range is from 1024 to 32,000.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 26.2.1	This command was modified to display warning message for insecure protocol usage.
IOS XE Fuji Release 16.8.1	This command was introduced.

Usage Guidelines

Use this command to limit the maximum jitter memory allowed for audio recordings during a single call session on a VoiceXML-enabled gateway.

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

Examples

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

```
Device(config)#ivr record jitter http://10.10.10.70//tftpboot/COLT-DE-CUCM.cfg 1024
SECURITY WARNING - Module: IVR, Command: ivr record jitter
http://10.10.10.70//tftpboot/COLT-DE-CUCM.cfg 1024 ,
Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of
encryption and authentication,
Description: IVR record jitter configured with insecure URL protocol - vulnerable to data
interception,
Remediation: Use secure protocols such as HTTPS, SFTP, or SCP instead of insecure HTTP,
FTP, or TFTP
```

Related Commands

Command	Description
ivr record memory session	Sets the maximum amount of memory that can be used to record voice message during a single call session.
ivr record memory system	Sets the maximum amount of memory that can be used to store all voice recordings on the VoiceXML-enabled gateway.

ivr record memory session

To set the maximum amount of memory that can be used to record voice messages during a single call session, use the **ivr record memory session** command in global configuration mode. To reset to the default, use the **no** form of this command.

ivr record memory session *kilobytes*
no ivr record memory session

Syntax Description

kilobytes	Memory size, in kilobytes. Range is 0 to 256000. The default is 256.

Command Default

256 KB

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300.
12.2(11)T	This command was implemented on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

Use this command to limit the maximum memory allowed for audio recordings during a single call session on a VoiceXML-enabled gateway.

Note This command configures memory limits only for voice messages recorded to local memory on the gateway. Memory limits are not configurable on the gateway for HTTP, Real Time Streaming Protocol (RTSP), or Simple Mail Transfer Protocol (SMTP) recordings.

Examples

The following example sets the maximum memory limit to 512 KB for a single call session:

```
ivr record memory session 512
```

Related Commands

Command	Description
ivr record memory system	Sets the maximum amount of memory that can be used to store all voice recordings on the VoiceXML-enabled gateway.

ivr record memory system

To set the maximum amount of memory that can be used to store all voice recordings on the gateway, use the **ivr record memory system** command in global configuration mode. To reset to the default, use the **no** form of this command.

ivr record memory system *kilobytes*
no ivr record memory system

Syntax Description

kilobytes	Memory limit, in kilobytes. Range is 0 to 256000. If 0 is configured, the RAM recording function is disabled on the gateway. The default for Cisco 3640 and Cisco AS5300 is 10000. The default for Cisco 3660, Cisco AS5350, and Cisco AS5400 is 20000.

Command Default

Cisco 3640 and Cisco AS5300: 10,000 KB Cisco 3660, Cisco AS5350, and Cisco AS5400: 20,000 KB

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300.
12.2(11)T	This command was implemented on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

Use this command to limit the maximum amount of gateway memory that is used for storing all voice recordings.

Note This command configures memory limits only for voice messages recorded to local memory on the gateway. Memory limits are not configurable on the gateway for HTTP, Real Time Streaming Protocol (RTSP), or Simple Mail Transfer Protocol (SMTP) recordings.

Examples

The following example sets the total memory limit for all recordings to 8000 KB:

```
ivr record memory system 8000
```

Related Commands

Command	Description
ivr record memory session	Sets the maximum amount of memory that can be used to record voice messages during a single call session.

ivr tts-server

To specify the location of an external media server that provides text-to-speech (TTS) functionality to voice applications, use the **ivr tts-server** command in global configuration mode. To remove the server location, use the **no** form of this command.

ivr tts-server *url*
no ivr tts-server

Syntax Description

url	Location of the TTS resource on the media server, in uniform resource locator (URL) format.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 26.2.1	This command was modified to display warning message for insecure protocol usage.
12.4(15)T	The *url* argument was modified to accept a Media Resource Control Protocol version 2 (MRCP v2) server URL.
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

This command sets the server location globally for all voice applications on the gateway.

For Nuance media servers that use the default installation, specify the URL as follows:

ivr tts-server rtsp:// *host* **:** *port* **/synthesizer**

(*host* is the host name of the media server; **:***port* is optional.)

For media servers using MRCP v2, specify the URL as follows:

ivr tts -server sip:*server-name@host-name* | *ip-address*

You can specify the location of the media server within a VoiceXML document, overriding the Cisco gateway configuration. For more information, see the Cisco VoiceXML Programmer's Guide.

To specify the voice profile that the TTS server uses for voice synthesis operations, use the **ivr tts-voice-profile** command.

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

Examples

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

```
Device(config)#ivr tts-server rtsp://tts_serv/synthesizer
SECURITY WARNING - Module: DEFAULT_VOICE_CONFIG, Command: ivr tts-server
rtsp://tts_serv/synthesizer,
Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of
encryption and authentication,
Description: ivr tts-server configured with insecure RTSP URL, Remediation: Use secure
protocols instead of insecure RTSP
Device(config)#
```

Examples

The following example specifies that voice applications use the TTS server named "tts_serv":

```
Router(config)# ivr tts-server rtsp://tts_serv/synthesizer
```

The following example specifies that voice applications use the MRCP v2 TTS server named "tts_mrcpv2serv":

```
Router(config)# ivr tts-server sip:tts_mrcpv2serv@mediaserver.com
```

Related Commands

Command	Description
ivr asr -server	Specifies the location of a media server that provides ASR functionality to IVR applications.
ivr tts -voice-profile	Specifies the location of the voice profile that is used by the TTS server.

ivr tts-voice-profile

To specify the location of the voice profile that is used by text-to-speech (TTS) servers, use the **ivr tts-voice-profile** command in global configuration mode. To remove the voice profile, use the **no** form of this command.

ivr tts-voice-profile *url*
no ivr tts-voice-profile

Syntax Description

url	Location of the TTS voice profile file, in URL format.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

This command specifies the voice profile that a TTS server uses for voice synthesis operations. The voice profile is a W3C Simple Markup Language (SML) file that specifies voice parameters like gender, speed, and so forth. The TTS server uses this voice profile unless the markup file that it is translating has overriding values.

The TTS voice profile can be stored on an HTTP server or on RTSP, TFTP, or FTP servers if the media sever supports these locations.

The TTS voice profile location can also be specified in the VoiceXML document by using the Cisco proprietary property com.cisco.tts-voice-profile. The VoiceXML property in the document overrides the value that is configured by using this command.

To specify the location of the external media server that is providing TTS functionality, use the **ivr tts-server** command.

Examples

The following example tells the TTS server to use the voice profile file named "vprofil2", which is located on an HTTP server:

```
ivr tts-voice-profile http://ttserver/vprofil2.sml
```

Related Commands

Command	Description
ivr asr -server	Specifies the location of a media server that provides ASR functionality to IVR applications.
ivr tts -server	Specifies the media server that provides TTS functionality to IVR applications.

ixi application cme

To enter XML application configuration mode for the Cisco Unified CallManager Express (Cisco Unified CME) application, use the **ixi application cme**command in global configuration mode.

ixi application cme

Syntax Description

This command has no arguments or keywords.

Command Default

XML parameters are not set for the Cisco Unified CME application.

Command Modes

Global configuration (config)

Command History

Cisco IOS Release	Modification
12.4(4)XC	This command was introduced.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

In Cisco Unified CME 4.0 and later versions, an XML interface is provided through the Cisco IOS XML Infrastructure (IXI), in which the parser and transport layers are separated from the application itself.

When you are using the Cisco IOS XML Infrastructure, the same HTTP transport layer can be used by multiple applications. The **ixi application cme** command enters XML application configuration mode to allow you to set Cisco IOS XML Infrastructure parameters for the Cisco Unified CME application. In this configuration mode, you can set the response timeout parameter using the **response timeout**command and enable communication with the application using the **no shutdown** command.

The **ixi transport** command allows you to set parameters for the Cisco IOS XML Infrastructure transport layer.

Note The **no** form of the **ixi application cme** command is not supported.

Examples

The following example shows how to configure the Cisco Unified CME application to overwrite the Cisco IOS XML Infrastructure transport-level timeout with a 30-second response timeout and enable XML communication with the application.

```
Router(config)# ixi application cme
Router(conf-xml-app)# response timeout 30
Router(conf-xml-app)# no shutdown
```

Related Commands

Command	Description
ixi transport	Enters XML transport configuration mode.

Command	Description
no shutdown	Enables XML communication with the application.
response (XML application)	Sets a timeout for responding to the XML application and overwrites the IXI transport-level timeout.

ixi application mib

To enter XML application configuration mode, use the **ixi application**command in global configuration mode.

ixi application mib

Syntax Description

mib	XML application for which parameters will be configured. Valid value: **mib**.

Command Default

No XML applications are configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The Cisco IOS XML Infrastructure (IXI) simplifies the implementation and deployment of XML-based applicatiosn in Cisco IOS software. IXI applications can be clients and or servers where the parser and transport layers are separated from the application itself. This modularity provides scalability and enables future XML supports to be developed.

An eXtensible Markup Language (XML) application programming interface (API) supports Cisco IOS commands allowing you to specify certain parameters associated with the XML API.

Once you are in XML application configuration mode, you can use the following commands:

- **default** --XML application configuration parameters defaults.
- **exit** --Apply changes and exit from XML application configuration mode.
- **help** --Display of the interactive help system.
- **no** --Negate a command or set its defaults.
- **response** --Response parameters.
- **shutdown** --Stop the application.

Examples

The following example shows how to enter XML application configuration mode, set the XML application timeout period to 30 seconds, format the response parameters to in human readable XML, and exit XML application configuration mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ixi application mib
Router(conf-xml-app)# response timeout 30
Router(conf-xml-app)# response formatted
Router(conf-xml-app)# exit
```

Related Commands

Command	Description
ixi transport http	Sets XML transport parameters.
response (XML application)	Sets XML application mode response parameters.

ixi transport http

To enter XML transport configuration mode, use the **ixi transport**command in global configuration mode.

ixi transport http

Syntax Description

http	Specifies the http transport protocol.

Command Default

No XML transport is configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The Cisco IOS XML Infrastructure (IXI) simplifies the implementation and deployment of XML-based applications in Cisco IOS software. IXI applications can be clients and or servers where the parser and transport layers are separated from the application itself. This modularity provides scalability and enables future XML supports to be developed. IXI allows applications to be written in a transport independent manner. The **ixi transport** command enters XML transport configuration mode where you can set transport configuration parameters.

Once you are in XML transport configuration mode, you can access the following commands:

- **default** *option* --XML transport configuration command defaults.
- **exit** --Apply changes and exit from XML application configuration mode.
- **help** --Display the interactive help system.
- **no** --Negate a command or set its defaults.
- **request** --Request handling parameters.
- **response size** --Response transport fragment size.
- **shutdown** --Stop the transport.

Examples

The following example shows how to enter XML transport configuration mode, set the XML transport fragment size to 32 Kbytes, and exit XML transport configuration mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ixi transport http
Router(conf-xml-trans)# response size 32

Router(conf-xml-trans)# exit
```

Related Commands

Command	Description
ixi application mib	Sets XML application parameters.
request (XML transport)	Sets XML transport request handling parameters.
response size (XML transport)	Set the XML transport fragment size.