

isdn all-incoming-calls-v120

To configure an ISDN BRI or PRI interface to answer all incoming calls as V.120 when the terminal adapter uses V.120 signalling but does not send the Lower-Layer Compatibility field in Setup messages, use the **isdn all-incoming-calls-v120** command in interface configuration mode. To remove this configuration, use the **no** form of the command.

isdn all-incoming-calls-v120

no isdn all-incoming-calls-v120

Syntax Description This command has no arguments or keywords.

Defaults By default, ISDN interfaces answer calls as synchronous serial with PPP encapsulation.

Command Modes Interface configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines Use this command only when you want *all* incoming calls to be answered as V.120. If you want the interface to automatically detect whether the incoming call uses V.120 or PPP encapsulation, use the **autodetect encapsulation** command.

This command applies only when the incoming call originates on an asynchronous device and needs to terminate in an available vty on the router.

Examples The following partial example shows that BRI 0 is configured to answer all calls as V.120:

```
interface bri 0
 isdn all-incoming-calls-v120
```

Related Commands	Command	Description
	autodetect encapsulation	Enables automatic detection of the encapsulation types in operation over a point-to-point link to a specified serial or ISDN interface.

isdn answer1, isdn answer2

To have the router verify a called-party number or subaddress number in the incoming setup message for ISDN BRI calls, if the number is delivered by the switch, use the **isdn answer1** command in interface configuration mode. To remove the verification request, use the **no** form of this command.

```
isdn answer1 [called-party-number][:subaddress]
```

```
no isdn answer1 [called-party-number][:subaddress]
```

To have the router verify an *additional* called-party number or subaddress number in the incoming setup message for ISDN BRI calls, if the number is delivered by the switch, use the **isdn answer2** command in interface configuration mode. To remove this second verification request, use the **no** form of this command.

```
isdn answer2 [called-party-number][:subaddress]
```

```
no isdn answer2 [called-party-number][:subaddress]
```

Syntax Description

<i>called-party-number</i>	(Optional) Telephone number of the called party. At least one value— <i>called-party-number</i> or <i>subaddress</i> —must be specified. The maximum number of digits for <i>called-party-number</i> is 50.
:	(Optional) Identifies the number that follows as a subaddress. Use the colon (:) when you configure both the called party number and the subaddress, or when you configure only the subaddress.
<i>subaddress</i>	(Optional) Subaddress number used for ISDN multipoint connections. At least one value— <i>called-party-number</i> or <i>subaddress</i> —must be specified. The maximum number of digits for <i>subaddress</i> is 50.

Defaults

The router does not verify the called party or subaddress number.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

If you do not specify the **isdn answer1** or **isdn answer2** command, all calls are processed or accepted. If you specify the **isdn answer1** or **isdn answer2** command, the router must verify the incoming called-party number and the subaddress before processing and/or accepting the call. The verification proceeds from right to left for the called-party number; it also proceeds from right to left for the subaddress number.

You can configure just the called-party number or just the subaddress. In such a case, only that part is verified. To configure a subaddress only, include the colon (:) before the subaddress number.

You can declare a digit a “don’t care” digit by configuring it as an *x* or *X*. In such a case, any incoming digit is allowed.

Examples

In the following example, 5552222 is the called-party number and 1234 is the subaddress:

```
interface bri 0
 isdn answer1 5552222:1234
```

In the following example, only the subaddress is configured:

```
interface bri 0
 isdn answer1 :1234
```

isdn autodetect

To enable the automatic detection of ISDN SPIDs and switch type, use the **isdn autodetect** command in interface configuration mode. To disable the automatic detection of ISDN SPIDs and switch type, use the **no** form of this command.

isdn autodetect

no isdn autodetect

Syntax Description

This command has no arguments or keywords.

Defaults

The automatic detection of ISDN SPIDs and switch type is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

This command applies to North America only. If you are outside of North America, you must use the **isdn switch-type** *switch-type* interface configuration command to specify the ISDN switch type.

Examples

The following example enables the automatic detection of ISDN SPIDs and switch type:

```
isdn autodetect
```

Related Commands

Command	Description
isdn spid1, isdn spid2	Defines the SPID number that has been assigned by the ISDN service provider for the B1 channel.
isdn switch-type (BRI) isdn switch-type (PRI)	Specifies the central office switch type on the ISDN BRI or PRI interface.

isdn bchan-number-order

To configure an ISDN PRI interface to make outgoing call selection in ascending or descending order, use the **isdn bchan-number-order** command in interface configuration mode. To restore the default (descending order), use the **no** form of this command or simply reconfigure the interface with the new value.

isdn bchan-number-order {ascending | descending}

no isdn bchan-number-order

Syntax Description

ascending Makes the outgoing B channel selection in ascending order as follows:

- Channels 1 to 24 for a T1 controller
- Channels 1 to 31 for an E1 controller

descending Makes the outgoing B channel selection in descending order as follows:

- Channels 24 to 1 for a T1 controller
- Channels 31 to 1 for an E1 controller

Defaults

Descending

Command Modes

Interface configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command instructs the router to select the lowest or highest available B channel starting at either channel B1 (ascending) or channel B23 for a T1 and channel B30 for an E1 (descending).

This command is for PRI configuration only.

Examples

The following example configures the outgoing B channel order on a PRI interface to be in ascending order. The router will select the lowest available B channel beginning with channel B1.

```
interface serial5:10
 isdn bchan-number-order ascending
```

isdn busy

To set a false busy signal on an ISDN B channel, use the **isdn busy** command in interface configuration mode. To remove this condition, use the **no** form of this command.

```
isdn busy dsl number b_channel number
```

```
no isdn busy dsl number b_channel number
```

Syntax Description

dsl number	Digital subscriber loop (DSL) number.
b_channel number	B channel or range of B channels to be set to the false busy signal. B channel numbers range from 1 to 24; 0 indicates the entire interface. The state of the channel, which is obtained using the show isdn command with the status keyword, can also be added to the command.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command gives the impression that a call is active when the channel is actually idle.

Use the **b_channel 0** keywords to set a false busy signal on the entire interface.

Use the **show isdn** command with the **status** keyword to display the DSL number and channel state.

Examples

The following example sets the entire PRI interface to a false busy signal; the DSL number was obtained using the **show isdn** command with the **status** keyword, and then used in the command.

```
isdn busy dsl 3 b_channel 0 state 1
```

The following example sets the false busy signal on B channel 11; the DSL number was obtained using the **show isdn** command with the **status** keyword, and then used in the command.

```
isdn busy dsl 3 b_channel 11 state 2
```

Related Commands

Command	Description
isdn service	Takes an individual B channel or an entire PRI interface out of service or sets it to a different channel service state that is passed in to the switch.

isdn call interface

To make an ISDN data call, use the **isdn call interface** command in privileged EXEC mode.

isdn call interface *interface-number dialing-string* [**speed 56** | **64**]

Syntax Description

<i>interface-number</i>	Interface number.
<i>dialing-string</i>	Telephone number used for making ISDN data call.
speed 56	(Optional) Line speed (56 or 64 kbps) used for making ISDN data call.
speed 64	

Defaults

The default B-channel speed is 64 kbps.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

You can use the **isdn call interface** command to test your DDR configuration. You can also use this command to verify the dialing string and speed without having to know the IP address of the remote router or without configuring a dialer map or string.

The **isdn call interface** command is being replaced by the **isdn test call interface** command in Cisco IOS Release 12.2.

Examples

The following example makes an ISDN data call through interface bri 0 to 555-1111 and at a line speed of 56 kbps:

```
isdn call interface bri 0 5551111 speed 56
```

Related Commands

Command	Description
isdn disconnect interface	Disconnects an ISDN data call without bringing down the interface.

isdn caller

To configure ISDN caller ID screening and optionally to enable ISDN caller ID callback for legacy dial-on-demand routing (DDR), use the **isdn caller** command in interface configuration mode. To disable this feature, use the **no** form of this command.

```
isdn caller phone-number [callback] [exact]
```

```
no isdn caller phone-number [callback] [exact]
```

Syntax Description

<i>phone-number</i>	Remote telephone number for which to screen. Use the letter X to represent a single “don’t care” digit. The maximum length of each number is 25 digits.
callback	(Optional) Enables callback.
exact	(Optional) Performs matching on incoming telephone number exactly as entered.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2 F	This command was implemented on additional Cisco router and access server platforms.
12.1	The exact keyword was added.

Usage Guidelines

This command configures the router to accept calls from the specified number.



Note

Caller ID screening requires a local switch or router that is capable of delivering the caller ID to the router. If you enable caller ID screening but do not have such a switch or router, no calls are allowed in. Caller ID screening is available on Cisco 7200 and 7500 series, Cisco 4000 series, Cisco 3000 series, and Cisco 2500 series routers that have one or more BRIs.

When the optional **callback** keyword is used and a call is received from one of the callback numbers, the initial call is rejected (hence, not subject to tolls) and a callback is initiated to that calling number.

When Xs are used in the callback number, dialer caller screening is based on a best match system that uses the *number* of Xs as a criterion. To make callback calls only to specified numbers or ranges of numbers but to accept any other incoming calls, make sure that the number of Xs in any configuration line that uses the **callback** keyword is less than the number of Xs in any configuration line that does not use the keyword.

For example, if you use at most four Xs in the configuration lines with the **callback** keyword, then to accept calls from other numbers use at least five Xs in a configuration line that does not use the keyword.

When a telephone number is entered *without* the **exact** keyword, the software compares each number going from right to left until matching numbers are detected. For example, if the *phone-number* argument is 4085551234, calls from telephone numbers 1234, 51234, 5551234, and 4085551234 would be accepted, but calls from telephone numbers 44 and 4155551234 would be rejected.

If you want to accept a telephone number *exactly* as it is configured, enter it with the **exact** keyword. For example, if the *phone-number* argument is 5551212 and the **exact** keyword is applied, only the telephone number 5551212 is accepted; calls from telephone numbers 408551212 and 51212 would be rejected.

The maximum length of each telephone number is 25 characters. There is no limit on the numbers you can specify per interface.

Examples

The following example configures the router to accept a call containing the numbers 415 555-1234:

```
isdn caller 4155551234
```

The following example configures the router to accept a call only from telephone number 555-1234:

```
isdn caller 5551234 exact
```

In the above example, a call from telephone number 415 555-1234 would be rejected.

The following example configures the router to accept a call with telephone number containing 415 555-12 and any numbers in the last two positions:

```
isdn caller 41555512xx
```

In the following example, callback calls will be made only to numbers in the 555 and 556 exchanges, but any other telephone number can call in:

```
isdn caller 408555xxxx callback
isdn caller 408556xxxx callback
isdn caller xxxxxx
```

Related Commands

Command	Description
show dialer	Displays general diagnostic information for interfaces configured for DDR.

isdn calling-number

To configure an ISDN PRI or BRI interface to present the number of the device making the outgoing call, use the **isdn calling-number** command in interface configuration mode. To remove a previously configured calling number, use the **no** form of this command.

isdn calling-number *calling-number*

no isdn calling-number

Syntax Description

calling-number Number of the device making the outgoing call; only one entry is allowed.

Defaults

No calling number is presented.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

An interface can have only one ISDN calling-number entry.

For ISDN BRI, this command is intended for use when the ISDN network offers TS014 tariffing, in which devices present the calling (billing) number.

For ISDN PRI, this command is intended for use when the network offers better pricing on calls in which devices present the calling number (that is, the billing number). The calling number information is included in the outgoing setup message.



Note

This command cannot be used with German ITR6 ISDN BRI switches. It can be used with all other switches, including all ISDN PRI switches.

Examples

The following example first configures the T1 interface, then configures the D channel interface to present the billing number 4233570925 when it makes outgoing calls:

```
controller t1 1/1
  framing esf
  linecode b8zs
  pri-group timeslots 1-23
  isdn switchtype primary-4ess
!
interface serial 1/1:23
  ip address 10.1.1.1 255.255.255.0
  encapsulation ppp
  isdn calling-number 4233570925
  dialer map ip 10.1.1.2 name dallas 14193460913
```

In the following example, the ISDN BRI interface is configured to present the number 5551212 when it makes outgoing calls:

```
interface bri 0
 isdn calling-number 5551212
```

Related Commands

Command	Description
interface dialer	Configures a BRI interface and enters interface configuration mode.
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller (for ISDN PRI, CAS, or robbed bit signalling).

isdn calling-pty

To specify whether the network-provided or user-provided calling party number is selected when two calling party numbers are sent from a primary NET5 switch on ISDN, use the **isdn calling-pty** command in interface configuration mode. To reset the default value, use the **no** form of this command.

isdn calling-pty { **network-provided** | **user-provided** }

no isdn calling-pty

Syntax Description

network-provided	Network-provided calling party number.
user-provided	User-provided calling party number.

Defaults

User-provided calling party number

Command Modes

Interface configuration

Command History

Release	Modification
12.2	This command was introduced for the primary ISDN NET5 switch.

Usage Guidelines

The **isdn calling-pty** command is useful for customers that use network-provided and user-provided calling party numbers for accounting purposes. The selected number will be used by dialer filters such as that configured with the **isdn caller** command.

Examples

The following example configures the ISDN switch to accept network-provided calling party numbers:

```
interface Serial0:23
  no ip address
  encapsulation ppp
  dialer rotary-group 1
  isdn switch-type primary-net5
  isdn protocol-emulate network
  isdn incoming-voice modem
  isdn calling-number 1111111
  isdn calling-pty network-provided
  isdn T310 40000
  no cdp enable
```

Related Commands

Command	Description
isdn caller	Configures ISDN caller ID screening and optionally enables ISDN caller ID callback for legacy DDR.
isdn calling-number	Configures an ISDN PRI or BRI interface to present the number of the device making the outgoing call.

isdn channel-id invert extended-bit

To invert the value of the extend bit (0x80) in the last octet of the channel ID information element, use the **isdn channel-id invert extended-bit** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

isdn channel-id invert extended-bit

no isdn channel-id invert extended-bit

Syntax Description This command has no arguments or keywords.

Defaults The last octet of the channel ID information element is not inverted.

Command Modes Interface configuration

Command History	Release	Modification
	12.2	This command was introduced.

Usage Guidelines Use this command if you use a primary-DMS 100 switch type to ensure compatibility with a Setup or Call Proceeding message containing a channel ID information element. This command can be used only with ISDN PRI.

This command replaces the **isdn-flip-chan-flag** command.

Examples The following example configures the router to invert the extended bit in the last octet of the channel ID information element:

```
isdn channel-id invert extended-bit
```

isdn conference-code

To activate three-way call conferencing, use the **isdn conference-code** command in interface configuration mode. To disable three-way call conferencing, use the **no** form of this command.

isdn conference-code *range*

no isdn conference-code

Syntax Description

<i>range</i>	Number from 0 to 999 (ISDN conference code).
--------------	--

Defaults

The default code is 60.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

Use this command if your ISDN line is connected to an NI1 or a Nortel DMS-100 Custom switch. Your telephone service provider should provide an ISDN conference code when you order three-way call conferencing.

Examples

The following example specifies 61 as the ISDN conference code:

```
isdn conference-code 61
```

isdn disconnect-cause

To send a specific ISDN cause code to the switch, use the **isdn disconnect-cause** command in interface configuration mode. To return to the default condition, use the **no** form of this command.

isdn disconnect-cause { *cause-code-number* | **busy** | **not-available** }

no isdn disconnect-cause

Syntax Description	
<i>cause-code-number</i>	Sends a cause code number (submitted as integer in the range of 1 through 127) to the switch.
busy	Sends the USER-BUSY code to the switch.
not-available	Sends the CHANNEL-NOT-AVAILABLE code to the switch.

Defaults The default condition is no cause code override. If the **isdn disconnect-cause** command is not configured, the default cause codes for the application are sent.

Command Modes Interface configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines The **isdn disconnect-cause** command overrides specific cause codes (such as modem availability and resource pooling) that are sent to the switch by ISDN applications. When the **isdn disconnect-cause** command is implemented, the configured cause codes are sent to the switch; otherwise, the default cause codes for the application are sent. ISDN protocol errors are still reflected in the cause codes and are not overridden.

Examples The following example sends the CHANNEL-NOT-AVAILABLE code to the ISDN switch:

```
interface serial0:20
 isdn disconnect-cause not-available
```

Related Commands	Command	Description
	isdn disconnect-cause	Sends a specific ISDN cause code to the switch.

isdn disconnect interface

To disconnect an ISDN data call without bringing down the interface, use the **isdn disconnect interface** command in privileged EXEC mode.

isdn disconnect interface *interface-type interface-number* {**b1** | **b2** | **all**}

Syntax Description

<i>interface-type</i>	Interface type and number, such as bri 0.
<i>interface-number</i>	
b1	B channel 1.
b2	B channel 2.
all	B channels 1 and 2.

Defaults

A default interface is not defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

You can use the **isdn disconnect interface** command to disconnect any ongoing data calls placed manually or caused by DDR.

The **isdn disconnect interface** command is being replaced by the **isdn test disconnect interface** command in Cisco IOS Release 12.2.

Examples

The following example disconnects an ISDN data call through interface bri 0 and B channel 1:

```
isdn disconnect interface bri 0 b1
```

Related Commands

Command	Description
isdn call interface	Makes an ISDN data call.

isdn fast-rollover-delay

To control the timing between successive dial attempts, use the **isdn fast-rollover-delay** command in interface configuration mode. To remove or change a value, use the **no** form of this command.

isdn fast-rollover-delay *seconds*

no isdn fast-rollover-delay

Syntax Description	<i>seconds</i>	Number of seconds between dial attempts.

Defaults	No default timer.

Command Modes	Interface configuration

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines

This command provides a timer separate from the dialer wait-for-carrier timer to control the amount of time that elapses before calls are redialed. This delay is provided to allow the old call to be torn down completely before the new call is attempted.

The **isdn fast-rollover-delay** command is necessary on some ISDN switches because the new call may be attempted before the old call is completely torn down, which causes the second call or the callback to fail.

Use this command when *all* the following conditions are true:

- A BRI has two phone numbers configured, one for each B channel.
- You are dialing in to this BRI.
- You have a dialer map or dialer string for each phone number.
- The first call succeeds but the second call continuously fails.

When these conditions occur, set the **isdn fast-rollover-delay** command to 5 seconds and try again. A delay of 5 seconds should cover most cases. Configure sufficient delay to make sure that the ISDN RELEASE_COMPLETE message has been sent or received before the fast rollover call is made. Use the **debug isdn q931** command to display this information.

When the **isdn fast-rollover-delay** command is configured on a client requesting callback, the callback client first confirms whether the callback server has placed a call back to the callback client before dialing any subsequent numbers.

Examples

The following partial example sets the fast-rollover delay that is suggested when all the conditions specified in the list in the “Usage Guidelines” are true:

```
isdn fast-rollover-delay 5
```

Related Commands

Command	Description
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
dialer wait-for-carrier-time (map-class)	Specifies the length of time to wait for a carrier when dialing out to the dial string associated with a specified map class.
ppp callback (DDR)	Enables a dialer interface that is not a DTR interface to function either as a callback client that requests callback or as a callback server that accepts callback requests.

isdn flip-chan-flag

The **isdn flip-chan-flag** command is replaced by the **isdn channel-id invert extended-bit** command. See the description of the **isdn channel-id invert extended-bit** command for more information.

isdn guard-timer

To enable a managed timer for authentication requests, use the **isdn guard-timer** command in interface configuration mode. To reset the timer to its default value, use the **no** form of this command.

isdn guard-timer *msecs* [**on-expiry** {**accept** | **reject**}]

no isdn guard-timer

Syntax Description

<i>msecs</i>	Number of milliseconds that the network access server (NAS) waits for a response from the AAA security server. The valid range is from 1000 through 20,000.
on-expiry	(Optional) Determines whether calls are accepted or rejected after the specified number of milliseconds has expired. If no expiry action is selected, calls are rejected.
accept	(Optional) Calls are accepted if the guard-timer expires before AAA responds.
reject	(Optional) Calls are rejected if the guard-timer expires before AAA responds.

Defaults

The default timer value is eight (8) seconds and calls are rejected when the timer expires.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

The guard-timer starts when the DNIS number is sent to AAA for authentication. When the timer expires, authentication ends and the call is accepted or rejected based on the configured expiry action.

Examples

The following example sets the guard-timer to six (6) seconds and specifies that the call should be rejected if AAA does not respond within that interval:

```
interface serial 1/0/0:23
isdn guard-timer 6000 on-expiry reject
```

Related Commands

Command	Description
aaa preauth	Enables authentication using DNIS numbers.

isdn incoming-voice

To route all incoming voice calls to the modem and determine how they will be treated, use the **isdn incoming-voice** command in interface configuration mode. To disable the setting or return to the default, use the **no** form of this command.

```
isdn incoming-voice { voice | data [56 | 64] | modem [56 | 64] }
```

```
no isdn incoming-voice { voice | data [56 | 64] | modem [56 | 64] }
```

Syntax Description

voice	Incoming voice calls bypass the modems and be handled as a voice call.
data	Incoming voice calls bypass the modems and will be handled as digital data. If the data keyword is selected, you can specify a B-channel bandwidth of either 56 kbps or 64 kbps.
modem	Incoming voice calls are passed over to the digital modems, where they negotiate the appropriate modem connection with the far-end modem. If this keyword is selected, you can specify a B-channel bandwidth of either 56 kbps or 64 kbps. If no argument is entered, the default value is 64.

Defaults

If you do not enter the **56** or **64** keywords after the **data** keyword, the default value will be 64 kbps.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced for ISDN PRI interfaces.
11.1 AA and 12.0(2)XC	This command was implemented on ISDN BRI interfaces.
11.2	This command was enhanced for channelized T1 and integrated into Cisco IOS Release 11.2.
11.3 NA	This command was implemented on additional Cisco router and access server platforms.
12.0(3)T	This command was implemented on additional Cisco router and access server platforms.

Usage Guidelines

Unless you specify otherwise, all calls received by the router and characterized as voice calls are treated as normal ISDN calls, which are handled as digital data and not passed over to the modem. Ordinarily, a data device ignores incoming voice calls, but the tariff structure for data and voice calls might make it less expensive to do “data over voice” calls.

If you use the **voice** keyword, incoming ISDN voice calls will be treated as voice calls and handled by either a modem or a voice DSP as directed by CSM.

If the default value is configured and the bearer capability of the incoming call is the **voice** keyword, the call will be rejected.

To answer incoming voice calls at a configured rate (overriding the incoming data rate in the call), use the **data** keyword.

To establish speedier connections for analog calls to the router, use the **isdn incoming-voice** command with the **modem** keyword to have voice calls routed through digital modems (as pulse-code modulated analog data) instead of being treated as digital data.

Configure this command on each D channel in the access server or router. Incoming circuit-switched data calls are not affected by this command.

**Note**

Use the **isdn incoming-voice modem** command only when you are using ISDN. You must use this command to carry voice over a modem when using ISDN PRI.

Examples

The following example designates incoming ISDN voice calls to be treated as voice calls:

```
interface 10
 isdn incoming-voice voice
```

The following example for channelized T1 configures the D channel (hence, all B channels) to answer all incoming voice calls at 56 kbps:

```
interface serial 0:23
 isdn incoming-voice data 56
```

The following example routes all incoming voice calls through the modem as analog data:

```
interface BRI 0/0
 isdn incoming-voice modem
```

The following example enables incoming and outgoing ISDN calls to route to the modems using the D channel serial interface:

```
interface serial 0:23
 isdn incoming-voice modem
```

isdn layer1-emulate

To configure the Layer 1 operation of a BRI voice port as clock master (NT) or slave (TE), use the **isdn layer1-emulate** command in interface configuration mode. To restore the default (user), use the **no** form of this command.

isdn layer1-emulate {user | network}

no isdn layer1-emulate

Syntax Description

user	Physical interface operation in clock slave mode (as TE).
network	Physical interface operation in clock master mode (as NT).

Defaults

Layer 1 port operation is as user (TE functionality as clock slave).

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the MC3810.
12.1(3)XI	This command was implemented on the Cisco 2600 and Cisco 3600 series.

Usage Guidelines

If you use the **no isdn layer1-emulate network** command, the physical layer port operation defaults to user.

Examples

The following example configures the Layer 1 operation of a BRI voice port as QSIG clock slave (TE):

```
configure terminal
interface bri 1
isdn layer1-emulate user
```

Related Commands

Command	Description
isdn protocol-emulate (dial)	Configures the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI interface to emulate NT (network) or TE (user) functionality.
network-clock-priority	Specifies the clock-recovery priority for the BRI voice ports in a BVM.

isdn leased-line bri

To configure an ISDN BRI for leased-line service, or to configure both 64-kbps leased-line and ISDN service on the same BRI, use the **isdn leased-line bri** command in global configuration mode. To remove or change channel configurations, use the **no** form of this command.

isdn leased-line bri *number/number* [**b1** | **b2** | **128** | **144** | *Return-key*]

no isdn leased-line bri *number/number* [**b1** | **b2** | **128** | **144** | *Return-key*]

Syntax Description

<i>number</i>	BRI interface numbers (enter the slash to separate the physical interface numbers).
b1	(Optional) Uses channel B1 as a 64-kbps leased line and channel B2 for ISDN service on a single ETSI NET3 switch on a Cisco 800 series router.
b2	(Optional) Uses channel B2 as a 64-kbps leased line and channel B1 for ISDN service on a single ETSI NET3 switch on a Cisco 800 series router.
128	(Optional) Combines B1 and B2 channels for 128-kbps leased-line service.
144	(Optional) Combines B1 and B2 channels for 144-kbps leased-line service.
<i>Return-key</i>	(Optional) Configures two 64-kbps leased lines instead of two B channels. Press the Return or Enter key at the end of the isdn leased-line bri number/number command instead of entering a keyword.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(4)T	The b1 and b2 keywords were added to allow the BRI channels on an ETSI NET3 switch on a Cisco 800 series router to be split into leased-line and ISDN services.

Usage Guidelines

Use the **isdn leased-line bri** command to configure an ISDN BRI for leased-line service by aggregating two BRI B channels into a single pipe at a speed of 128 or 144 kbps, or configuring both a 64-kbps leased line and ISDN service on a single European Telecommunications Standards Institute (ETSI) NET3 switch on Cisco 800 series routers.

This command also supports two separate 64-kbps leased lines, where the BRI interface is configured as two separate leased lines instead of two B channels. No keyword is required for this configuration; just press the Return or Enter key at the end of the **isdn leased-line bri number/number** command string. This configuration is different than using the **128** keyword, which configures a single 128-kbps leased line.

When you use the **no isdn leased-line bri** command to change the channel configuration, you must also perform a system reload in order for the change to take effect.

When you use an ISDN BRI interface for access over leased lines, configure the ISDN BRI as a synchronous serial interface and do not configure ISDN calling and called numbers.

Examples

The following example configures the BRI interface for leased-line access at 128 kbps in Japan:

```
isdn leased-line bri0/0 128
```

Because of the leased-line—not dialed—environment, configuration of ISDN called and calling numbers is not needed and not used. The BRI 0 interface is henceforth treated as a synchronous serial interface, with the default High-Level Data Link Control (HDLC) encapsulation.

The following example configures BRI channel B1 for 64-kbps leased-line service and channel B2 for ISDN service:

```
isdn switch-type basic-net3
isdn leased-line bri0/0 b1
!
interface bri0/0
 ip address 10.1.1.1 255.255.255.0
 no ip address
 dialer pool-member 1

interface bri0/0:1
 ip address 10.1.1.2 255.255.255.0
 encapsulation ppp
 no ip address
```

The following example configures two 64-kbps leased lines:

```
isdn leased-line bri0/0
```

Related Commands

Command	Description
isdn switch-type (BRI)	Specifies the central office switch type on the ISDN BRI interface.

isdn map

To override the default ISDN type and plan generated by the router with custom values, use the **isdn map** command in interface configuration mode. To revert to the default ISDN type and plan, use the **no** form of this command.

```
isdn map {address address | regexp | plan plan | type type}
```

```
no isdn map {address address | regexp | plan plan | type type}
```

Syntax Description

address <i>address</i>	Address map, which can be to either the calling or called number.
<i>regexp</i>	Regular expression for pattern matching.
plan <i>plan</i>	ISDN numbering plan.
type <i>type</i>	ISDN number type.

Defaults

The default is the ISDN type and plan generated by the router.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(6)T	This command was introduced.

Usage Guidelines

This function can be configured on a per-number basis or on numbers that match regular expression patterns. Keywords and arguments for any or all of the possible parameters can be included.

Examples

The following example overrides any plan and type used for any ISDN calls with a called or calling number exactly matching 123:

```
int serial1:23
  isdn map address 123 plan isdn type unknown
```

The following example overrides any plan and type used for ISDN calls with a called or calling number that begins with the numerals 12:

```
int serial1:23
  isdn map address 12.* plan data type subscriber
```

The following example matches any number ending with the number 7:

```
int serial1:23
  isdn map address .*7 plan data type subscriber
```

isdn modem-busy-cause

The **isdn modem-busy-cause** command is replaced by the **isdn disconnect-cause** command. See the **isdn disconnect-cause** command for more information.

isdn negotiate-bchan

To enable the router to accept a B channel that is different from the B channel requested in the outgoing call setup message, use the **isdn negotiate-bchan** command in interface configuration mode. To restore the default condition, use the **no** form of this command.

```
isdn negotiate-bchan [resend-setup] [cause-codes cause-code1 [cause-code2...cause-code16]]
```

```
no isdn negotiate-bchan [resend-setup] [cause-codes cause-code1 [cause-code2...cause-code16]]
```

Syntax Description

resend-setup	(Optional) Enables a single reattempt of a setup message if a disconnect message with a cause code of 44 is received before alerting. Supports NET5 and NI2 PRI switches only. (A Code 44 cause code means that the requested circuit or channel is not available. For more information, refer to the International Telecommunications Union [ITU] Q.850 standard.)
cause-codes <i>cause-code</i>	(Optional) Specifies up to 16 cause codes that will alert the gateway to reattempt a call. This reattempt may or may not be on the same B channel as the previous attempt. The value of each <i>cause-code</i> argument is a number from 1 to 127 corresponding to an ISDN cause code number. If the cause-codes keyword is entered, at least one cause code must be entered or the command will not be accepted. Once the cause-codes keyword is entered, cause code 44 will no longer cause a call reattempt unless 44 is specifically entered as one of the cause codes. Note The validity of each cause code is not checked by the gateway.

Defaults

B channel negotiation is not enabled. Most PRI switch types set the default channel ID to Exclusive in the setup message. An exception is the NI2 switch, which sets the default to Preferred.

If the **cause-codes** keyword is not entered, it is assumed that you want ISDN cause code 44.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2	The resend-setup keyword was implemented for NET5 and NI2 PRI switches.
12.2(15)T	The cause-codes keyword was implemented on the Cisco AS5350 and Cisco AS5400.

Usage Guidelines

The **isdn negotiate-bchan** command enables the router to negotiate the B channel by setting the channel ID information element to Preferred in the setup message. If this command is not configured, the channel ID is set to the default of the switch, which is usually Exclusive. Exclusive means that only the requested B channel is accepted. If the requested B channel is not available, the call is cleared.

The **isdn negotiate-bchan** command is supported for all PRI switch types. The **resend-setup** keyword is supported only for NET5 and NI2 switches. This command is not supported for BRI interfaces.

The **cause-codes** keyword allows you to configure the gateway to reattempt a call when a cause code other than 44 is received from the PSTN.

Refer to the “[ISDN Cause Codes](#)” table in the appendix of the *Cisco IOS Debug Command Reference*, Release 12.2, for a list of ISDN cause codes.

Examples

The following example enables a call to be reattempted when a disconnect with cause code of 44 is received before alerting:

```
interface serial0:23
 isdn negotiate-bchan resend-setup
```

The following example shows that cause codes 34, 44, and 63 have been configured:

```
interface serial0:23
 isdn negotiate-bchan resend-setup cause-codes 34 44 63
```

Related Commands

Command	Description
isdn bchan-number-order	Configures an ISDN PRI interface to make an outgoing call selection in ascending or descending order.
isdn switch-type (PRI)	Specifies the Central Office switch type on the ISDN PRI interface.

isdn not-end-to-end

To override the speed that the network reports it will use to deliver the call data, use the **isdn not-end-to-end** command in interface configuration mode. To disable the configured end-to-end speed, use the **no** form of this command.

```
isdn not-end-to-end {56 | 64}
```

```
no isdn not-end-to-end
```

Syntax Description

56	Answers all voice calls at 56 kbps.
64	Answers all voice calls at 64 kbps.

Defaults

The default line speed is 64 kbps.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines



Note

The **isdn not-end-to-end** command is valid only when an incoming Layer 3 Setup message contains a Progress Information Element in the message. The command is validated on a call-by-call basis, depending upon the message.

This command might be needed to handle incoming calls properly. Although a call might originate at a speed of 56 kbps, the network or internetworking networks might improperly deliver the call to the user at a speed of 64 kbps. This creates a speed mismatch and causes the data to be garbled. Enabling this command makes the router look more closely at the information elements of the incoming call to determine a speed.

A speed mismatch can occur when the source and destination ISDN ports do not belong to the same network.

Examples

The following example sets the line speed for incoming calls to 56 kbps:

```
isdn not-end-to-end 56
```

isdn number

To change the maximum number of digits in a called number information element, use the **isdn number** command in interface configuration mode.

isdn number [**called enbloc** *limit*]

Syntax Description	called	Attributes for the ISDN number of the called party.
	enbloc	Allows the ISDN terminal to send the ISDN number of the called party in a single SETUP message.
	<i>limit</i>	Maximum number of digits allowed in a SETUP message, in the range from 1 to 32.

Defaults 20 digits

Command Modes Interface configuration

Command History	Release	Modification
	12.2	This command was introduced.

Usage Guidelines The maximum number of digits sent in the initial call SETUP is defaulted to 20 digits. The default of 20 digits chosen because some switches cannot handle more than 20 digits. Some countries in Europe are changing their calling plans and will require calls to be made using more than 20 digits.

The **isdn number called enbloc** command is used when the maximum number of octets in the called number information element in a SETUP message must be changed from the 20-digit default to the user desired limit. With this command, the user can configure the maximum number from 1 to 32 digits. This command is available for ISDN interfaces and applicable to both BRI and PRI interfaces.



Note

This command is enabled for only the following switch types:

BRI_NET3_STYPE
PRI_NET5_SYTPE

Examples The following example configures the called number information element for 32 digits:

```
Router(config-if) isdn number called enbloc 32
```

isdn nsf-service

To configure Network Specific Facilities (NSF) on an ISDN PRI for outgoing calls configured as voice calls, use the **isdn nsf-service** command in interface configuration mode. To remove NSF on an ISDN PRI, use the **no** form of this command.

```
isdn nsf-service {megacom | sdn}
```

```
no isdn nsf-service {megacom | sdn}
```

Syntax Description	megacom	Dial voice calls using AT&T Megacom NSF.
	sdn	Dial voice calls using AT&T SDN NSF.

Defaults	Disabled
----------	----------

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	11.3(5)T	This command was introduced.

Usage Guidelines	This command is used specifically on a PRI (channelized T1) to request NSF services supported on primary AT&T 4ESS (primary-4ess) switch types only.
------------------	---

Examples	The following example sets outgoing voice calls to use AT&T SDN NSF:
----------	--

```
interface serial 0:23
 isdn-nsf-service sdn
```

Related Commands	Command	Description
	dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
	dialer voice-call	Configures the dialer map class for an NSF dialing plan to support outgoing voice calls.
	map-class dialer	Defines a class of shared configuration parameters associated with the dialer map command for outgoing calls from an ISDN interface and for PPP callback.

isdn outgoing ie redirecting-number

To enable passing of the redirect number information element (IE) from the Cisco router to its peer, use the **isdn outgoing ie redirecting-number** command in interface configuration mode. To disable passing of the redirect number IE from the Cisco router to its peer, use the **no** form of this command.

isdn outgoing ie redirecting-number

no isdn outgoing ie redirecting-number

Syntax Description

This command has no arguments or keywords.

Defaults

The redirecting number IE will be passed in the setup message for the following switch types only by default:

- basic-dms100
- basic-ni
- primary-dms100
- primary-4ESS
- primary-5ESS
- primary-ni
- primary-ni2c

For all other switch types, the redirecting number IE will not be passed by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T5	This command was introduced.

Usage Guidelines

Use the **isdn outgoing ie redirecting-number** command to enable passing of the redirect number IE from the Cisco router to its peer. Some switch types do not support the redirect number IE, so to ensure compatibility with a peer that does support the redirect number IE you may enable the passing of the redirect number IE using the **isdn outgoing ie redirecting-number** command.

Examples

The following example enables the passing of the redirect number IE for a NET5 switch on a serial interface:

```
interface Serial 0:15
  isdn outgoing ie redirecting-number
```

isdn outgoing-voice

To set information transfer capability on outgoing calls for all switch types, use the **isdn outgoing-voice** command in interface configuration mode. To revert to the default state, use the **no** form of this command.

```
isdn outgoing-voice {info-transfer-capability {3.1kHz-audio | speech}}
```

```
no isdn outgoing-voice
```

Syntax Description	Command	Description
	info-transfer-capability	Specifies information transfer capability for voice calls.
	3.1kHz-audio	Sets capability to 3.1 kHz audio.
	speech	Sets capability to speech.

Defaults No information transfer capabilities set.

Command Modes Interface configuration

Command History	Release	Modification
	11.3	This command was introduced.

Usage Guidelines This command is used on outgoing voice calls only, and sets standard information transfer capability.

Examples The following example sets information transfer capability on outgoing voice calls to speech:

```
interface serial 0:23
 isdn outgoing-voice info-transfer-capability speech
```

Related Commands	Command	Description
	isdn incoming-voice	Specifies how to process incoming ISDN voice and data calls.

isdn overlap-receiving

To enable overlap receiving on an ISDN interface, use the **isdn overlap-receiving** command in interface configuration mode. To disable overlap receiving on an ISDN interface, use the **no** form of this command.

isdn overlap-receiving [**T302** *milliseconds*]

no isdn overlap-receiving

Syntax Description	T302 <i>milliseconds</i>	(Optional) The number of milliseconds that the T302 timer should wait before expiring. Valid values for the <i>milliseconds</i> argument range from 500 to 20000. The default value is 10000 (10 seconds).
---------------------------	---------------------------------	--

Defaults Overlap receiving is not enabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.1	This command was introduced.

Usage Guidelines In some situations, the default timer value of the T302 timer is too long. You can shorten the duration of the timer by specifying the **T302** keyword with the number of milliseconds necessary.

When configuring outbound peer matching and overlap receiving, use the **isdn overlap-receiving** command with the **destination-pattern** command. You must configure the commands to allow the router to wait for all the digits to be received before the call is routed. To do this, use the **T** control character after the digits in the destination pattern specified with the **destination-pattern** command. Optionally, you can shorten the duration of the T302 timer when you specify the **isdn overlap-receiving** command.

Examples The following example shows how to enable overlap receiving on the ISDN interface:

```
interface serial 0:23
 isdn overlap-receiving
```

The following example shows how to enable overlap receiving on the ISDN interface and set the T302 timer to 2 seconds:

```
interface serial 0:23
 isdn overlap-receiving T302 2000
```

Related Commands

Command	Description
destination-pattern	Specifies either the prefix or full E.164 telephone number to be used for a dial peer.
isdn service	Takes an individual B channel or an entire PRI interface out of service or sets it to a different channel service state that is passed in to the switch.

isdn overlap-receiving calltypes all

To enable overlap receiving for all call types, use the **isdn overlap-receiving calltypes all** command in interface configuration mode. To disable overlap receiving for all call types, use the **no** form of this command.

isdn overlap-receiving calltypes all

no isdn overlap-receiving calltypes all

Syntax Description This commands has no arguments or keywords.

Defaults Overlap receiving is not enabled.

Command Modes Interface configuration

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

Usage Guidelines The **isdn overlap-receiving calltypes all** command enables overlap receiving for all nonvoice calls that use data dial peers, and it enables an ISDN interface to proceed with a call when a sufficient number of digits are received. These digits are determined by the **destination-pattern** command under the data dial peer configuration.

This command is supported on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 routers.

Examples The following example shows how to enable overlap receiving:

```
interface serial 0:23
 isdn overlap-receiving calltypes all
```

Related Commands	Command	Description
	destination-pattern	Specifies either the prefix or full E.164 telephone number to be used for a dial peer.
	dial-peer no-match disconnect-cause	Disconnects the incoming ISDN or CAS call when no inbound voice or modem dial peer is matched.
	isdn overlap-receiving	Enables overlap receiving on an ISDN interface.

isdn piafs-enabled

To enable the PRI to take Personal Handyphone Internet Access Forum Standard (PIAFS) calls on MICA technologies modems, use the **isdn piafs-enabled** command in interface configuration mode. To disable the function, use the **no** form of this command.

isdn piafs-enabled

no isdn piafs-enabled

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(2)XH	This command was introduced on the Cisco AS5300.
	12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T and support was added for the Cisco AS5800.
	12.2(2)XA	Support was added for PIAFS version 2.1 using Cisco MICA 8.2.3.0 was added. Note PIAFS 2.1 is not supported on Cisco AS5800 universal access servers for this release.
	12.2(2)XB1	This command was implemented on the Cisco AS5800 platform.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples The following example shows how to enable the PRI to take PIAFS calls:

```
Router(config)# interface serial 0:23
Router(config-if)# isdn piafs-enabled
```

isdn point-to-point-setup

To configure the ISDN port to send SETUP messages on the static TEI, use the **isdn point-to-point-setup** command in interface configuration mode. To restore the default, use the **no** form of this command.

isdn point-to-point-setup

no isdn point-to-point-setup

Syntax Description This command has no arguments or keywords.

Defaults The BRI port sends SETUP messages on the static TEI (TEI 127).

Command Modes Interface configuration

Command History	Release	Modification
	12.1(3)XI	This command was introduced.

Usage Guidelines This command only applies if a static TEI has been activated with the **isdn static-tei command**.

Examples The following example configures the BRI port to send SETUP messages on the static TEI:

```
interface bri 1
isdn point-to-point-setup
```

Related Commands	Command	Description
	isdn tei-negotiation (global)	Configures when Layer 2 becomes active and ISDN TEI negotiation occurs.

isdn protocol-emulate (dial)

To configure the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI interface to emulate NT (network) or TE (user) functionality, use the **isdn protocol-emulate** command in interface configuration mode. To restore the default (user), use the **no** form of this command.

isdn protocol-emulate {user | network}

no isdn protocol-emulate

Syntax Description	user	Layer 2 and Layer 3 port protocol operation as TE (port functions as QSIG slave).
	network	Layer 2 and Layer 3 port protocol operation as NT (port functions as QSIG master).

Defaults Port functions as Q.SIG slave.

Command Modes Interface configuration

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.

Usage Guidelines You can use this command to configure the Cisco AS5300 PRI interface to serve as either the primary Q.SIG slave or the primary Q.SIG master. To disable Q.SIG signalling, use the **no** form of this command. If you use the **no isdn protocol-emulate** command, the Layer 2 and Layer 3 protocol emulation defaults to user.

Examples The following example configures the Layer 2 and Layer 3 function of T1 PRI interface 23 to act as the Q.SIG master (NT):

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

The following example configures the Layer 2 and Layer 3 function of a BRI voice port to operate as Q.SIG slave (TE):

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

The following example configures the Layer 2 and Layer 3 function of an E1 PRI interface to operate as Q.SIG slave (TE):

```
interface serial 1:15
 isdn protocol-emulate user
```

Related Commands

Command	Description
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 your NEC PBX to support FCCS
show cdapi	Displays the CDAPI.
show rawmsg	Displays the raw messages owned by the required component.

isdn reject

To reject an incoming ISDN BRI or PRI call based on type, use the **isdn reject** command in interface configuration mode. To re-allow the incoming call type, use the **no** form of this command.

```
isdn reject {{cause cause-code} {data [56 | 64]} | piafs | v110 | v120 | vod | {voice [3.1khz | 7khz | speech]}}
```

```
no isdn reject {{cause cause-code} {data [56 | 64]} | piafs | v110 | v120 | vod | {voice [3.1khz | 7khz | speech]}}
```

Syntax Description

cause <i>cause-code</i>	Rejects call based on cause code value.
data [56 64]	Rejects incoming data call. If the optional 56 or 64 keyword is not specified, all data calls, including data over voice, are rejected. Use the optional 56 keyword to reject data coming in at 56 kbps. Use the optional 64 keyword to reject data coming in at 64 kbps.
piafs	Rejects incoming Personal Handyphone Internet Access Forum Standard (PIAFS) calls.
v110	Rejects incoming V.110 calls.
v120	Rejects incoming V.120 calls.
vod	Rejects incoming voice-over-data calls, or calls characterized by 64 kbps unrestricted digital data. Although the bearer capability for these calls indicates an incoming data call, the call is treated as voice over data. See the “Usage Guidelines” for more information.
voice [3.1khz 7khz speech]	Rejects incoming voice and modem calls characterized by one of three information transfer capability types: 3.1 kHz, 7 kHz, and speech, which are defined by using, in corresponding order, the 3.1khz , 7khz , and speech keywords. If none of the optional keywords is used, all voice calls except voice over data are rejected.

Defaults

Incoming calls are rejected based on D-channel bearer capability information (cause code 65).

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.
12.2	The cause cause-code keyword and argument were added.

Usage Guidelines

The **isdn reject** command rejects incoming calls based on D-channel bearer capability information. If this command is configured with the **cause cause-code** keyword and argument, it will override the default value and use the configured cause code specified to reject the call. For example, if the **isdn reject data** command is configured so that data calls are rejected with cause code set to 65 (“bearer

capability not implemented” and the default), you can change the cause code to 2, so that data calls will then be rejected with cause code 2. Refer to the *ISDN Switch Types, Codes, and Values* appendix in the *Cisco IOS Debug Command Reference* for a list of ISDN cause code values.

The settings for the **isdn incoming-voice** interface configuration command determine how the call is handled based on bearer capability information, as follows:

- **isdn incoming-voice voice**—Calls bypass the modem and are handled as a voice call.
- **isdn incoming-voice data**—Calls bypass the modem and are handled as digital data.
- **isdn incoming-voice modem**—Calls are passed to a digital modem and the call negotiates the appropriate modem connection with the far-end modem.

When the ISDN interface is configured for incoming voice with the **isdn incoming-voice voice** command and the ISDN bearer capability indicates the call as unrestricted digital data (i = 0x8890), the call is handled as voice over data.

You can assign as many reject incoming call type statements as needed to reject unwanted calls on the ISDN interface.

This command works on any Cisco platform that supports ISDN PRI and BRI interfaces.

Examples

The following example configuration rejects all incoming data and voice-over-data calls but accepts voice calls:

```
interface serial 2/0:23
  no ip address
  no logging event link-status
  dialer-group 1
  isdn switch-type primary-net5
  isdn incoming-voice voice
  isdn map address 222 plan isdn type national
  isdn T309 80000
  isdn reject data
  isdn reject vod
  isdn reject v120
  isdn reject v110
  isdn reject piafs
```

The following example sets the ISDN interface to reject incoming PIAFS calls:

```
interface serial 2/0:23
  isdn reject piafs
```

The following example sets cause code 21 to reject all incoming data calls:

```
interface serial 2/0:23
  isdn reject data
  isdn reject cause 21
```

Related Commands

Command	Description
isdn incoming-voice	Specifies how to process incoming ISDN voice and data calls.

isdn send-alerting

To specify that an Alerting message be sent before a Connect message when making ISDN calls, use the **isdn send-alerting** command in interface configuration mode. To disable the Alerting information element, use the **no** form of this command.

isdn send-alerting

no isdn send-alerting

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Some switches may want an Alerting message to be sent by the router before sending a Connect message. This is usually seen in a voice and data type of network.

Examples

In the following example, the **isdn send-alerting** command applies to an ISDN BRI interface:

```
interface BRI0
description connected to PBX 61886
ip address 172.26.1.1 255.255.255.0
encapsulation ppp
isdn send-alerting
isdn sending-complete
dialer idle-timeout 20
dialer map ip 172.26.1.2 name rudder 61884
dialer map ip 172.26.1.3 name bosun 61885
dialer-group 1
ppp authentication chap
```

Related Commands

Command	Description
isdn sending-complete	Specifies that the Sending Complete IE is included in the outgoing Setup message.

isdn sending-complete

To specify that the Sending Complete information element (IE) is included in the outgoing Setup message, use the **isdn sending-complete** command in interface configuration mode. To disable the Sending Complete information element, use the **no** form of this command.

isdn sending-complete

no isdn sending-complete

Syntax Description This command has no arguments or keywords.

Defaults This command is disabled by default.

Command Modes Interface configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines The Sending Complete IE tells the switch that all the digits and information necessary for the call are contained in this Setup message.

Some switches in some countries want a Sending Complete information element to be included in the outgoing Setup message to indicate that the entire number is included. The Sending Complete IE is required in Hong Kong and Taiwan, and the **isdn sending-complete** command forces it to be sent.

Examples In the following example, the **isdn sending-complete** command applies to an ISDN BRI interface:

```
interface BRI0
description connected to PBX 61886
ip address 172.31.1.1 255.255.255.0
encapsulation ppp
isdn sending-complete
dialer idle-timeout 20
dialer map ip 172.31.1.2 name rudder 61884
dialer map ip 172.31.1.3 name bosun 61885
dialer-group 1
ppp authentication chap
```

The following example enables sending complete IE information on a serial interface:

```
interface serial 0:15
description connected to PBX 61886
ip address 10.1.1.1 255.255.255.0
encapsulation ppp
isdn sending-complete
dialer idle-timeout 20
dialer map ip 10.1.1.2 name rudder 61884
dialer map ip 10.1.1.3 name goodie 61885
dialer-group 1
ppp authentication chap
```

Related Commands

Command	Description
isdn send-alerting	Specifies that an Alerting message be sent before a Complete message when making ISDN calls.

isdn service

To take an individual B channel or an entire PRI interface out of service or set it to a different channel service state that is passed to a time-division multiplexing (TDM) switch at the Public Switched Telephone Network (PSTN), use the **isdn service** command in interface configuration mode. To remove the configuration, use the **no** form of the command.

```
isdn service [dsl number | nfas-int number] b_channel number state {0 | 1 | 2}
```

```
no isdn service
```

Syntax Description	
dsl <i>number</i>	(Optional) Digital subscriber loop number; displayed with the show isdn status command. DSL numbers range from 0 to 31.
nfas-int <i>number</i>	(Optional) The Non-Facility Associated Signalling (NFAS) member interface number that has B channel(s) to which you want to do maintenance.
b_channel <i>number</i>	B channel or range of B channels to be set with the passed-in state value. Specifying <i>number</i> as 0 sets the entire PRI interface to a specified state value. B channel numbers range from 0 to 31 or 0 for the complete interface.
state {0 1 2}	Desired channel service state to be set on the channels. The following channel service state values are supported: 0 —In service. Restore a channel or complete interface to service. 1 —Maintenance. “Soft busy.” 2 —Out of service. Immediately take a channel(s) out of service and drop any active calls.

Defaults	
Disabled	

Command Modes	
Interface configuration	

Command History	Release	Modification
	11.3	This command was introduced.
	12.2	The dsl keyword was made optional.

Usage Guidelines	
Use this command to manage channels on ISDN NFAS and Primary Rate Interfaces (PRI) on Cisco routers.	

Use the **b_channel 0** keyword to set the entire PRI interface to the specified state value.

To display the digital subscriber loop (DSL) number on NFAS interfaces, use the **show isdn service EXEC** command. To find the NFAS interface value, use the **pri-group T1** controller configuration command.

Examples

The following example sets all the PRI B channel on the interface to maintenance state.

```
isdn service b_channel 0 state 1
```

The following example restores B channels 2 to 4; the DSL number was obtained using the **show isdn** command with the **status** keyword, and then used in the command:

```
isdn service dsl 2 b_channel 2-4 state 0
```

The following example sets B channel 13 to 24 to the out-of-service state:

```
isdn service nfas-int 3 b_channel 13-24 state 1
```

Related Commands

Command	Description
show isdn	Displays the information about memory, Layer 2 and Layer 3 timers, and the status of PRI channels.

isdn silent-boot

To prevent the transmission and receipt of ISDN packets by the router during the bootstrap loading process, use the **isdn silent-boot** command in global configuration mode. To allow the transmission and receipt of ISDN packets by the router during the bootstrap loading process, use the **no** form of this command.

isdn silent-boot

no isdn silent-boot

Syntax Description This command has no arguments or keywords.

Defaults The transmission and receipt of ISDN packets by the router is allowed during the bootstrap process.

Command Modes Global configuration

Command History	Release	Modification
	12.2	This command was introduced.

Usage Guidelines ISDN traffic will not be sent from any interfaces on the router (ISDN BRI or PRI) when you use the **isdn silent-boot** command. Disabling the ISDN traffic on the router is appropriate when the router is part of a hunt group that is accepting incoming ISDN calls because you do not want the router to receive calls until after it has reloaded and is ready to accept the incoming calls.

Examples The following example disables ISDN traffic:

```
Router(config)# isdn silent-boot
```

isdn snmp busyout b-channel

To enable PRI B channels to be busyied out via SNMP, use the **isdn snmp busyout b-channel** command in interface configuration mode. To prevent B channels from being busyied out via SNMP, use the **no** form of this command.

isdn snmp busyout b-channel

no isdn snmp busyout b-channel

Syntax Description

This command has no arguments or keywords.

Defaults

The default value is TRUE; that is, setting busyout using SNMP is allowed.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

To busy out B-channels on a PRI, the ISDN switch must support service messages. The **isdn snmp busyout b-channel** command sets the MIB object, cpmDS0BusyoutAllow, indicating whether or not the switch supports service messages, thereby allowing the busyout of B channels. When the network access server receives an SNMP request for a busyout, it checks the value of this object. If the **no isdn snmp busyout b-channel** command is configured, the busyout request fails.

Examples

The following example allows the busyout of B-channels for serial interface 0:23:

```
configure terminal
interface serial 0:23
isdn snmp busyout b-channel
```

isdn spid1, isdn spid2

To associate up to three ISDN local directory numbers (LDNs) provided by your telephone service provider to the first service profile identifier (SPID), use the **isdn spid1** command in interface configuration mode. To disable the specified SPID and prevent access to the switch, use the **no** form of this command.

```
isdn spid1 spid-number ldn [ldn] [ldn]
```

```
no isdn spid1 spid-number ldn [ldn] [ldn]
```

To associate up to three ISDN LDNs provided by your telephone service provider to the second service SPID, use the **isdn spid2** interface configuration command. To disable the specified SPID and prevent access to the switch, use the **no** form of this command.

```
isdn spid2 spid-number ldn [ldn] [ldn]
```

```
no isdn spid2 spid-number ldn [ldn] [ldn]
```

Syntax Description

<i>spid-number</i>	Number identifying the service to which you have subscribed. This value is assigned by the ISDN service provider and is usually a 10-digit telephone number with additional digits such as 40855522220101.
<i>ldn</i>	(Optional) ISDN LDN, which is a 7-digit number assigned by the service provider. You can optionally specify a second and third LDN.

Defaults

A default SPID number and ISDN local directory numbers are not defined.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(3)T	This command was enhanced with the option of associating the SPID with up to three LDNs.

Usage Guidelines

This command applies only to North America and is required for DMS-100 and National ISDN switches. Typically, DMS-100 and National ISDN switch implementations using BRI interfaces with SPIDS require two TEIs, two SPIDS, and two phone numbers. If you want to take advantage of both B channels, it is advised you configure the router with the LDN value after the SPID.

**Note**

Some DMS-100 and National ISDN switch installations may be configured as a “hunt group” whereby all calls are initially forwarded to the primary number. Under these circumstances, you should not configure the LDN. You can determine this by enabling the **debug isdn q931** command. If the endpoint identifier (EID) information element is delivered in the incoming setup message, then the switch is addressing the TEIs with the EID, instead of the LDN.

If you want the SPID to be automatically detected, you can specify 0 for the *spid-number* argument.

The ISDN switch checks for the LDN to determine whether both channels can be used to transmit and receive data. If there is not an LDN present, then only the B1 channel can be used for full-duplex communication. However, the B2 channel can still be used to make outgoing calls.

If you include the local directory number in the **no** form of this command, access to the switch is permitted, but the other B channel may not be able to receive incoming calls.

Examples

The following example defines, on the router, a SPID and LDN for the B1 channel:

```
isdn spid1 41555512130101 5551213
```

The following example shows how to specify that the SPID should be automatically detected, that the primary ISDN local directory number is 4085551111, and that the secondary number is 4085552222:

```
isdn spid1 0 4085551111 4085552222
```

The following example defines, on the router, a SPID and LDN for the B2 channel:

```
isdn spid2 41555512140101 5551214
```

The following example specifies that the SPID should be automatically detected, that the primary ISDN local directory number is 4085551111, and that the secondary number is 4085552222:

```
isdn spid2 0 4085551111 4085552222
```

Related Commands

Command	Description
isdn autodetect	Enables the automatic detection of ISDN SPIDs and switch type.

isdn static-tei

To configure a static ISDN Layer 2 terminal endpoint identifier (TEI) over the D channel, use the **isdn static-tei** command in interface configuration mode. To remove a static TEI configuration, use the **no** form of this command.

isdn static-tei *tei-number*

no isdn static-tei *tei-number*

Syntax Description

tei-number Terminal endpoint identifier, in the range from 0 to 63.

Defaults

Dynamic TEI (**no isdn static-tei**)

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Depending on the telephone company you subscribe to, you may have a dynamically or statically assigned TEI for your ISDN service. The default TEI behavior is dynamic, and the **isdn static-tei** command changes that behavior to static for the specified service.

When you reconfigure a TEI with the **isdn static-tei** command, you must activate the configuration using the **shutdown** and **no shutdown** commands.

Examples

The following example configures German Anlagenanschluss ISDN lines. These lines are often provided in a group intended to be connected to single ISDN device such as a private branch exchange. To use the Anlagenanschluss ISDN lines on a Cisco router, you must set the TEI to 0, as follows:

```
Router# configure terminal
Router(config)# interface bri 0
Router(config-if)# isdn static-tei 0
Router(config-if)# shutdown
Router(config-if)# no shutdown
```

Related Commands

Command	Description
interface bri	Configures a BRI interface and enters interface configuration mode.
isdn x25 static-tei	Configure a static TEI for X.25 over the ISDN D channel.
shutdown	Disables an interface.

isdn switch-type (BRI)

To specify the central office switch type on the ISDN interface, use the **isdn switch-type** command in global or interface configuration mode. To remove an ISDN switch type, use the **no** form of this command.

isdn switch-type *switch-type*

no isdn switch-type *switch-type*

Syntax Description	<i>switch-type</i> ISDN service provider switch type. Table 7 in the “Usage Guidelines” section lists the supported switch types.
---------------------------	---

Defaults	No ISDN switch type is specified.
-----------------	-----------------------------------

Command Modes	Global configuration or interface configuration
----------------------	---



Note

This command can be entered in either global configuration or interface configuration mode. When entered in global configuration mode, the **basic-qsig** switch type command specifies that the Cisco MC3810 use QSIG signalling on all BRI interfaces; when entered in interface configuration mode, the command specifies that an individual BRI voice interface use QSIG signalling. The interface configuration mode setting overrides the global configuration setting on individual interfaces.

Command History	Release	Modification
	9.21	This command was introduced as a global command.
	11.3 T	This command was introduced as an interface command.
	12.0(3)XG	The basic-qsig and primary-qsig switch type options were added to support BRI QSIG voice signalling.

Usage Guidelines	For the Cisco AS5300 access server, you have the choice of configuring the isdn-switch-type command to support Q.SIG in either global configuration mode or interface configuration mode. When entered in global configuration mode, the setting applies to the entire Cisco AS5300 access server. When entered in interface configuration mode, the setting applies only to the T1/E1 interface specified. The interface configuration mode setting overrides the global configuration setting.
-------------------------	---

For example, if you have a Q.SIG connection on one line as well as on the PRI port, you can configure the ISDN switch type in one of the following combinations:

- Set the global **isdn-switch-type** command to support Q.SIG and set the interface **isdn-switch-type** command for **interface serial 0:23** to a PRI setting such as 5ess.
- Set the global **isdn-switch-type** command to support PRI 5ess and set the interface **isdn-switch-type** command for **interface serial 1:23** to support Q.SIG.
- Configure the global **isdn-switch-type** command to another setting (such as switch type VN3), set the interface **isdn-switch-type** command for **interface serial 0:23** to a PRI setting, and set the interface **isdn-switch-type** command for **interface serial 1:23** to support Q.SIG.

For the Cisco MC3810 router, if you are using different Cisco MC3810 BRI port interfaces with different ISDN switch types, you can use global and interface commands in any combination, as long as you remember that interface commands always override a global command.

For example, if you have a BRI QSIG switch interface on BRI voice ports 1, 2, 3 and 4, but a BRI 5ess switch interface on BRI backup port 0, you can configure the ISDN switch types in any of the following combinations:

- Enter the **isdn switch-type basic-qsig global configuration command**, and enter the **isdn switch-type bri-5ess command** on interface 0.
- Enter the **isdn switch-type bri-5ess** global configuration command, and enter the **isdn switch-type basic-qsig command** on interfaces 1, 2, 3, and 4 individually.
- Enter the **isdn switch-type bri-5ess** command on interface 0, and enter the **isdn switch-type basic-qsig command** on interfaces 1, 2, 3, and 4 individually.

If you use the **no isdn switch-type** global configuration command, any switch type that was originally entered in global configuration mode is cancelled; however, any switch type originally entered on an interface is not affected. If you use the **no isdn switch-type** interface configuration command, any switch type configuration on the interface is cancelled.

**Note**

In the Cisco MC3810, ISDN BRI voice ports support *only* switch type **basic-qsig**; ISDN BRI backup ports support all other listed switch types, but *not* **basic-qsig**.

**Note**

The dial-peer **codec** command must be configured before any calls can be placed over the connection to the PINX. The default codec type is G729a.

If you are using the Multiple ISDN Switch Types feature to apply ISDN switch types to different interfaces, refer to the chapters “Configuring ISDN BRI” and “Configuring ISDN PRI” in the *Cisco IOS Dial Technologies Configuration Guide* for additional details.

The Cisco IOS command parser accepts the following switch types: basic-nwnet3, vn2, and basic-net3; however, when viewing the NVRAM configuration, the basic-net3 or vn3 switch types are displayed, respectively.

To remove an ISDN switch type from an ISDN interface, specify **the no isdn switch-type switch-type command**.

[Table 7](#) lists supported BRI switch types by geographic area.

Table 7 ISDN Service Provider BRI Switch Types

Keywords by Area	Switch Type
Voice/PBX Systems	
basic-qsig	PINX (PBX) switches with QSIG signalling per Q.931
Australia , Europe, UK	
basic-1tr6	German 1TR6 ISDN switch
basic-net3	NET3 ISDN BRI for Norway NET3, Australia NET3, and New Zealand NET3switch types; ETSI-compliant switch types for Euro-ISDN E-DSS1 signaling system
vn3	French ISDN BRI switches
Japan	
ntt	Japanese NTT ISDN switches
North America	
basic-5ess	Lucent (AT&T) basic rate 5ESS switch
basic-dms100	Northern Telecom DMS-100 basic rate switch
basic-ni	National ISDN switches
All users	
none	No switch defined

Examples

The following example configures the French VN3 ISDN switch type:

```
isdn switch-type vn3
```

The following example uses the Multiple ISDN Switch Types feature and shows use of the global ISDN switch type **basic-ni** keyword (formerly **basic-ni1**) and the **basic-net3** interface-level switch type keyword. ISDN switch type **basic-net3** is applied to BRI interface 0 and overrides the global switch setting.

```
isdn switch-type basic-ni
!
interface BRI0
 isdn switch-type basic-net3
```

The following example configures the Cisco MC3810 router to use BRI QSIG signalling for all of its BRI voice ports:

```
isdn switch-type basic-qsig
```

The following example configures the Cisco MC3810 to use BRI QSIG signalling for BRI voice port 1. On port 1, this setting overrides any different signalling set in the previous example.

```
interface bri 1
 isdn switch-type basic-qsig
```

The following example configures the Cisco AS5300 to support Q.SIG signalling:

```
isdn switch-type primary-qsig
```

isdn switch-type (PRI)

To specify the central office switch type on the ISDN interface, or to configure the Cisco MC3810 PRI interface to support QSIG signalling, use the **isdn switch-type** command in global or interface configuration mode. To disable the switch or QSIG signalling on the ISDN interface, use the **no** form of this command.

isdn switch-type *switch-type*

no isdn switch-type *switch-type*

Syntax Description

switch-type Service provider switch type; see [Table 8](#) for a list of supported switches.

Defaults

The switch type defaults to **none**, which disables the switch on the ISDN interface.

Command Modes

Global configuration or interface configuration



Note

This command can be entered in either global configuration mode or in interface configuration mode. When entered in global configuration mode, the setting applies to the entire Cisco MC3810. When entered in interface configuration mode, the setting applies only to the T1/E1 interface specified. The interface configuration mode setting overrides the global configuration setting.

Command History

Release	Modification
9.21	This command was introduced as a global command.
11.3 T	This command was introduced as an interface command.
12.0(2)T	The primary-qsig-slave and primary-qsig master switch type options were added to support PRI QSIG signalling.

Usage Guidelines

You have a choice of configuring the **isdn-switch-type** command to support QSIG at either the global configuration level or at the interface configuration level. For example, if you have a QSIG connection on one line as well as on the BRI port, you can configure the ISDN switch type in one of the following combinations:

- Set the global **isdn-switch-type** command to support QSIG, and set the interface **isdn-switch-type** command for the **interface bri 0** command to a BRI setting such as 5ess.
- Set the global **isdn-switch-type** command to support BRI 5ess, and set the interface **isdn-switch-type** command for the **interface serial 1:23** command to support QSIG.
- Configure the global **isdn-switch-type** command to another setting (such as switch type VN3), and then set the interface **isdn-switch-type** command for the **interface bri 0** command to a BRI setting, and set the interface **isdn-switch-type** command for the **interface serial 1:23** command to support QSIG.

The voice-port **codec** command must be configured before any calls can be placed over the connection to the PINX. The default codec type is G729a.

To disable the switch on the ISDN interface, specify the **isdn switch-type none** command.

Table 8 lists supported PRI switch types by geographic area.



Note

If you are using the Multiple ISDN Switch Types feature to apply the ISDN switch types to different interfaces, refer to the chapter “Setting Up Basic ISDN Service” in the *Cisco IOS Dial Technologies Configuration Guide* for additional details.

Table 8 ISDN Service Provider PRI Switch Types

Keywords by Area	Switch Type
Voice/PBX Systems	
primary-qsig	Supports QSIG signaling per Q.931. Network side functionality is assigned with the isdn protocol-emulate command.
Australia and Europe	
primary-net5	NET5 ISDN PRI switch types for Asia, Australia, and New Zealand; ETSI-compliant switches for Euro-ISDN E-DSS1 signaling system.
Japan	
primary-ntt	Japanese ISDN PRI switch.
North America	
primary-4ess	AT&T 4ESS switch type for the United States.
primary-5ess	AT&T 5ESS switch type for the United States.
primary-dms100	NT DMS-100 switch type for the United States.
primary-ni	National ISDN switch type.
All users	
none	No switch defined.

Examples

The following example demonstrates the Multiple ISDN Switch Type Feature. The global ISDN switch type setting is basic-net3. The PRI interface (channelized T1 controller), is configured to use the **isdn switch-type primary-net5** command and BRI interface 0 is configured for the **isdn switch-type basic-ni** command (formerly **isdn switch-type basic-ni1**).

```
isdn switch-type basic-net3
!
interface serial0:23
  isdn switch-type primary-net5
  ip address 172.21.24.85 255.255.255.0
!
interface BRI0
  isdn switch-type basic-ni
```

The following example configures T1 interface 23 on the Cisco AS5300 to support Q.SIG signaling:

```
interface serial 1:23
  isdn switch-type primary-qsig
```

Related Commands	Command	Description
	isdn protocol-emulate (dial)	Configures the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI interface to emulate NT (network) or TE (user) functionality.
	pri-group nec-fusion	Configures your NEC PBX to support FCCS.
	show cdapi	Displays the CDAPI.
	show rawmsg	Displays the raw messages owned by the required component.

isdn t306

To set a timer for disconnect messages received by a router, use the **isdn t306** command in interface configuration mode. To reset to the default, use the **default** or **no** form of this command.

isdn t306 *msecs*

default isdn t306

no isdn t306

Syntax Description	<i>msecs</i>	Time, in milliseconds, that the router waits before disconnecting a call after it receives a disconnect message with a progress indicator of 8. Range is from 1 to 400000.
---------------------------	--------------	--

Defaults Default depends on the switch, usually from 5000 to 30000 ms.

Command Modes Interface configuration

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 The T306 timer is designed for routers that are configured as an ISDN network-side switch. When a router receives a disconnect message with a progress indicator of 8, it disconnects the call after waiting for the specified number of milliseconds (ms) while the in-band announcement or error tone is playing. Be sure to set the timer long enough for the announcement to be heard or the tone to be recognized. This command is used only for disconnect messages with a progress indicator of 8; otherwise, the T305 timer is used. The **disable** and **no** forms of this command have the same result: the timer waits for the default number of ms before disconnecting the call.

Examples The following example sets the T306 timer to 60000 ms for serial interface 0:23:

```
interface serial 0:23
  isdn t306 60000
```

Related Commands

Command	Description
isdn t309	Changes the value of the timer to clear the network connection, and release the B channel and call reference when a data-link disconnection has occurred.
isdn t310	Changes the value of the T310 timer for Call Proceeding messages.
isdn timer t321	Changes the value of the T321 timer for D channel switchover when the primary D channel fails.

isdn t310

To set a timer for the call proceeding state, use the **isdn t310** command interface configuration mode. To reset to the default, use the **no** form of this command.

isdn t310 *msecs*

no isdn t310

Syntax Description

<i>msecs</i>	Time, in milliseconds, that the router waits before disconnecting a call after receiving a call proceeding message. Range is from 1 to 400000.
--------------	--

Defaults

Default depends on the switch; usually from 5000 to 30000 ms.

Command Modes

Interface configuration

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 AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

The T310 timer starts when a router receives a call proceeding message; it stops when the call exits the call proceeding state, typically when the call moves to the alerting, connect, or progress state. If the timer expires while the call is in the call proceeding state, the router releases the call. Set the timer to match the specific characteristics of your network.

Examples

The following example sets the T310 timer to 40,000 ms for serial interface 0:23:

```
interface serial 0:23
  isdn t310 40000
```

Related Commands

Command	Description
isdn protocol-emulate	Sets a timer for Disconnect messages.
isdn t306	Changes the value of the T306 timer to disconnect a call after the router sends a disconnect message.

Command	Description
isdn test call interface	Changes the value of the T309 timer to clear the network connection, and to release the B channel and call reference when a data-link disconnection has occurred.
isdn timer t321	Changes the value of the T321 timer for D channel switchover when the primary D channel fails.

isdn test call interface

To make an ISDN data call, use the **isdn test call interface** command in privileged EXEC mode.

isdn test call interface *interface-number dialing-string* [**speed 56 | 64**]

Syntax Description	
<i>interface-number</i>	Interface number.
<i>dialing-string</i>	Telephone number used for making ISDN data call.
speed 56	(Optional) Line speed (56 or 64 kbps) used for making ISDN data call.
speed 64	

Defaults The default B-channel speed is 64 kbps.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2	This command was introduced.

Usage Guidelines You can use the **isdn test call interface** command to test your DDR configuration. You can also use this command to verify the dialing string and speed without having to know the IP address of the remote router or without configuring a dialer map or string.

The **isdn test call interface** command replaces the **isdn call interface** command.

Examples The following example makes an ISDN data call through interface bri 0 to 555-1111 and at a line speed of 56 kbps:

```
isdn test call interface bri 0 5551111 speed 56
```

Related Commands	Command	Description
	isdn caller	Disconnects an ISDN data call without bringing down the interface.

isdn test disconnect interface

To disconnect an ISDN data call without bringing down the interface, use the **isdn test disconnect interface** command in privileged EXEC mode.

isdn test disconnect interface *interface-type interface-number* {**b1** | **b2** | **all**}

Syntax Description

<i>interface-type</i>	Interface type and number, such as bri 0.
<i>interface-number</i>	
b1	B channel 1.
b2	B channel 2.
all	B channels 1 and 2.

Defaults

A default interface is not defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

You can use the **isdn test disconnect interface** command to disconnect any ongoing data calls placed manually or caused by DDR.

The **isdn test disconnect interface** command replaces the **isdn disconnect interface** command.

Examples

The following example disconnects an ISDN data call through interface bri 0 and B channel 1:

```
isdn test disconnect interface bri 0 b1
```

Related Commands

Command	Description
isdn call interface	Makes an ISDN data call.

isdn timer t309

To change the value of the T309 timer to clear the network connection and to release the B channel and call reference when a data-link disconnection has occurred, use the **isdn timer t309** command in interface configuration mode. To restore the default value, use the **no** form of this command.

isdn timer t309 *milliseconds*

no isdn timer t309

Syntax Description

<i>milliseconds</i>	Number of milliseconds (ms) that the router waits before clearing the network connection, and releasing the B channel and call reference. Values are from 0 to 90 ms.
---------------------	---

Defaults

90 ms

Command Modes

Interface configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

When a data link layer malfunction occurs, calls that are not in the active state are cleared. For calls that are not in the active state, the T309 timer is started. The timer is stopped when the data link is reconnected. If the T309 timer expires prior to the reestablishment of the data link, the network clears the connection and call to the remote user, sending a disconnect cause of 27 to indicate that the call destination is out of order. The network releases and disconnects the B channel, and releases the call reference, entering the Null state. The T309 timer is mandatory for routers that are configured as an ISDN network-side switch and by default the timer is set to expire after 90 ms. The implementation of the T309 timer is optional for the user side of the network. The **isdn timer t309** command is used for changing the value of the T309 timer.



Note

Setting the timer to 0 causes the timer expiry to become infinite so that it will never expire.

Examples

The following example sets the T309 timers to 80 ms for serial interface 0:24:

```
interface serial 0:24
  isdn timer t309 80
```

Related Commands

Command	Description
isdn t306	Changes the value of the T306 timer to disconnect a call after the router sends a disconnect message.
isdn t310	Changes the value of the T310 timer for Call Proceeding messages.
isdn timer t321	Changes the value of the T321 timer for D channel switchover when the primary D channel fails.

isdn timer t321

To change the value of the timer for D channel switchover when the primary D channel fails, use the **isdn timer t321** command in interface configuration mode. To restore the default value, use the **no** form of this command.

isdn timer t321 *milliseconds*

no isdn timer t321

Syntax Description	<i>milliseconds</i>	Number of milliseconds (ms) that the router waits before sending a DL-ESTABLISH request on both D channels to request a switchover. Values are from 0 to 30 ms.
---------------------------	---------------------	---

Defaults	30 ms
-----------------	-------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.2	This command was introduced.

Usage Guidelines The T321 timer must be implemented when you use the D channel backup procedure involving D channel switchover. The **isdn timer t321** command is used for changing the value of the T321 timer.



Note

Setting the timer to 0 causes the timer expiry to become infinite so that it will never expire.

Examples The following example sets the T321 timers to 25 ms for serial interface 0:23:

```
interface serial 0:23
 isdn timer t321 25
```

Related Commands	Command	Description
	isdn t306	Changes the value of the T306 timer to disconnect a call after the router sends a disconnect message.
	isdn timer t309	Changes the value of the T309 timer to clear the network connection, and to release the B channel and call reference when a data-link disconnection has occurred.
	isdn t310	Changes the value of the T310 timer for Call Proceeding messages.

isdn tei-negotiation (global)

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

isdn tei-negotiation [**first-call** | **powerup**]

no isdn tei-negotiation

Syntax Description

first-call	(Optional) ISDN TEI negotiation should occur when the first ISDN call is placed or received.
powerup	(Optional) ISDN TEI negotiation should occur when the router is powered on.

Defaults

The **powerup** state is the default condition.

Command Modes

Global configuration

Command History

Release	Modification
9.21	This command was introduced as a global command.

Usage Guidelines

This command is for BRI configuration only.

This command is useful for switches that may deactivate Layers 1 and 2 when there are no active calls or primary DMS-100 switches which activate TEI when the first ISDN call is placed or received.

Examples

The following example applies the **isdn tei negotiation first-call** command to BRI interface 0. BRI interface 1 will use the **isdn tei negotiation powerup command**, which is the default setting. Defaults settings do not appear in the router configuration.

```
isdn switch-type basic-net
!
interface bri0
! Configure the ISDN switch type on this interface and set TEI negotiation to first-call.
  isdn switch-type basic-ni
  isdn tei-negotiation first-call
! BRI interface 1 uses the default TEI negotiation value.
interface bri1
```

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 {first-call | powerup} {preserve | remove}
```

Syntax Description

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

Defaults

The **powerup** state is the default condition. Depending upon the ISDN switch type configured, the default will be to preserve or remove the TEI negotiation options. See the “Usage Guidelines” and “Examples” sections for further explanation.

Command Modes

Interface configuration

Command History

Release	Modification
11.3 T	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.

The **preserve** keyword depends on the ISDN switch type configured, that is, the TEI negotiation configured will be preserved during ISN Layer 1 flaps, and when the **clear interface** or the **shut** and **no shut EXEC** commands are executed, on the switch types listed in [Table 9](#).

Table 9 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

Table 9 Switch Types with Preserved TEI Negotiation (continued)

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 **shut** and **no shut** EXEC commands are executed. Use the **remove** keyword to specifically set one of the switches listed in [Table 9](#) to the remove state.

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 first-call
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 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
  cdapi buffers regular 0
  cdapi buffers raw 0
  cdapi buffers large 0
```

isdn transfer-code

To activate call transferring, use the **isdn transfer-code** command in interface configuration mode. To disable call transferring, use the **no** form of this command.

isdn transfer-code *range*

no isdn transfer-code

Syntax Description	<i>range</i>	Number from 0 to 999 (ISDN transfer code).
--------------------	--------------	--

Defaults	The default code is 61.
----------	-------------------------

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	12.0(3)T	This command was introduced.

Usage Guidelines	Use this command if your ISDN line is connected to a NI1 or a Nortel DMS-100 Custom switch. Your telephone service provider should issue an ISDN transfer code when you order call transferring.
------------------	--

Examples	The following example specifies 62 as the ISDN transfer code:
----------	---

```
isdn transfer-code 62
```

isdn twait-disable

To delay a National ISDN BRI switch a random time before activating the Layer 2 interface when the switch starts up, use the **isdn twait-disable** command in interface configuration mode. To remove the delay, use the **no** form of this command.

isdn twait-disable

no isdn twait-disable

Syntax Description This command has no arguments or keywords.

Defaults This command is enabled by default.

Command Modes Interface configuration

Command History	Release	Modification
	11.3	This command was introduced.

Usage Guidelines The random-length delay set by this command prevents mass power failures from causing the network ISDN switches to be overwhelmed when power returns and all the devices startup at the same time. The random delay is in the range 1 to 300 seconds.

Examples The following example configures a random wait period after a power failure:

```
isdn twait-disable
```

isdn v110 only

To selectively accept incoming V.110 calls based on data bit, parity, and stop bit modem communication settings, use the **isdn v110 only** command in interface configuration mode. To change or disable the expected incoming V.110 modem call configuration, use the **no** form of this command.

```
isdn v110 only [databits {5 | 7 | 8}] [parity {even | mark | none | odd | space}]
               [stopbits {1 | 1.5 | 2}]
```

```
no isdn v110 only
```

Syntax Description	
databits {5 7 8}	(Optional) Allowed data bits, as follows: <ul style="list-style-type: none"> • 5—Allow 5 data bits only. • 7—Allow 7 data bits only. • 8—Allow 8 data bits only.
parity {even mark none odd space}	(Optional) Allowed parity, as follows: <ul style="list-style-type: none"> • even—Allow even parity only. • mark—Allow mark parity only. • none—Allow no parity only. • odd—Allow odd parity only. • space—Allow space parity only.
stopbits {1 1.5 2}	(Optional) Allowed stop bits, as follows: <ul style="list-style-type: none"> • 1—Allow 1 stop bit only. • 1.5—Allow 1.5 stop bits only. • 2—Allow 2 stop bits only.

Defaults No default behavior or values.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(4)T	This command was introduced.

Usage Guidelines The **isdn v110 only** command provides a way to screen incoming V.110 modem calls and reject any calls that do not have the communication settings configured as the network expects them to be.

Examples

The following example filters out all V.110 modem calls except those with communication settings of 8 data bits, no parity bit, and 1 stop bit:

```
interface serial 0:23
  isdn v110 only databits 8 parity none stopbits 1
```

isdn v110 padding

To disable the padded V.110 modem speed report required by the V.110 modem standard, use the **no isdn v110 padding** command in interface configuration mode. To reenable the padded V.110 modem speed report, use the **isdn v110 padding** command.

no isdn v110 padding

isdn v110 padding

Syntax Description This command has no arguments or keywords.

Defaults V.110 modem speed padding is enabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.2(8)T	This command was introduced.

Usage Guidelines The **no isdn v110 padding** command is useful for networks with devices such as terminal adapters (TAs) and global system for mobile communication (GSM) handsets that do not fully conform to the V.110 modem standard. The V.110 modem standard specifies that the incoming asynchronous data must be padded by adding stop elements to fit the nearest channel rate. For example, a 14400 bits per second (bps) user data signaling rate is adapted to a synchronous 19200-bps stream rate. The software reports the adapted rate (19200 bps) to the modem for an incoming V.110 call. However, for those devices that do not fully conform to the V.110 specifications, the software must report the speed as 14400 instead of 19200 to the modem for a successful connection. By setting the modem interface to **no isdn v110 padding**, padding is disabled and the actual bit rate can be reported to the modem.

Examples The following example shows how to disable V.110 asynchronous-to-synchronous padding:

```
!
interface Serial0:23
 no ip address
 isdn switch-type primary-ni
 isdn bchan-number-order ascending
 no isdn v110 padding
 no cdp enable
```

isdn voice-priority

To control the priority of data and voice calls for the telephones, fax machines, and modems connected to the router telephone ports, use the **isdn voice-priority** command in interface configuration mode. To disable a specified ISDN voice priority setting and to use the default setting, use the **no** form of this command.

```
isdn voice-priority local-directory-number {in | out} {always | conditional | off}
```

```
no isdn voice-priority local-directory-number
```

Syntax Description		
	<i>local-directory-number</i>	Local ISDN directory number assigned by your telephone service provider.
	in	Incoming voice call.
	out	Outgoing voice call.
	always	Always bump a data call for a voice call.
	conditional	Bump a data call only if there is more than one call to the same destination.
	off	Never bump a data call for a voice call.

Defaults

A data call is never bumped for an incoming or outgoing voice call.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

If an ISDN circuit endpoint is busy with a data call or calls and either a voice call comes in (incoming) or you attempt to place a voice call (outgoing), the data call is handled according to the setting of **isdn voice-priority** command.

If you are in North America and have multiple ISDN directory numbers associated with a SPID, the outgoing voice priority that you set for any of these directory numbers applies to the other directory numbers. For example, if you enter the following commands, the outgoing voice priority for all directory numbers specified in the **isdn spid1** command is set to conditional:

```
isdn spid1 0 4085551111 4085552222 4085553333
isdn voice-priority 5551111 out conditional
```

The setting of the **pots dialing-method** command affects when you hear a busy signal in the following situation:

- A data call cannot be bumped.
- You are trying to make an outgoing call.

If the setting is **overlap**, you hear a busy signal when you pick up the handset. If the setting is **enblock**, you initially hear a dial tone and then a busy signal.

Examples

The following example specifies that a data call for the specified ISDN directory number never be bumped for an incoming or an outgoing voice call:

```
isdn voice-priority 5551111 in off
isdn voice-priority 5551111 out off
```

Related Commands

Command	Description
isdn spid1, isdn spid2	Defines the SPID number that has been assigned by the ISDN service provider for the B1 channel.
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.

isdn x25 dchannel

To create a configurable interface for X.25 traffic over the ISDN D channel, use the **isdn x25 dchannel** command in interface configuration mode. To remove the interface, use the **no** form of this command.

isdn x25 dchannel

no isdn x25 dchannel

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Interface configuration

Command History	Release	Modification
	11.2 F	This command was introduced.

Usage Guidelines This command creates a new, configurable interface, which can be specified as **interface brix:0** in commands, where *x* is the original BRI interface number. For example, on a Cisco 4500 router with an MBRI, if the **isdn x25 dchannel** command is configured on bri5, the new interface is bri5:0 and can be used for configuring the other parameters for X.25 over the D channel. These parameters include the addresses, the map statements, and others. To display the new interface, use the **more system:running-config** command.

Examples The following example creates interface bri 1:0 and configures it for X.25 over the ISDN D channel. This example uses dynamic TEIs, not a static TEI.

```
interface bri1
  isdn x25 dchannel
interface bri1:0
  ip address 10.1.1.2 255.255.255.0
  x25 address 31107000000100
  x25 htc 1
  x25 suppress-calling-address
  x25 facility window-size 2 2
  x25 facility packet-size 256 256
  x25 facility throughput 9600 9600
  x25 map ip 10.1.1.3 31107000000200
  x25 map ip 10.1.1.4 31107000000800
```

Related Commands	Command	Description
	interface bri	Configures a BRI interface and enters interface configuration mode.

isdn x25 static-tei

To configure a static ISDN Layer 2 terminal endpoint identifier (TEI) for X.25 over the ISDN D channel, use the **isdn x25 static-tei** command in interface configuration mode. Use the **no** form of this command if dynamic TEIs will be used on the interface that is to carry X.25 traffic over the D channel.

isdn x25 static-tei *tei-number*

no isdn x25 static-tei *tei-number*

Syntax Description

<i>tei-number</i>	Terminal endpoint identifier, in the range from 0 to 63.
-------------------	--

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

This command applies to ISDN BRI interfaces only. Only one static TEI is allowed per BRI interface. If a second static TEI is configured, the first static TEI is overwritten.

Some switches require a static TEI be used for X.25 over the ISDN D channel.

When the **isdn x25 dchannel** command is invoked without the **isdn x25 static-tei** command, a dynamic TEI is chosen.

Examples

The following example creates static TEI 8 on the X.25-over-ISDN-D channel:

```
interface bri0
 isdn x25 dchannel
 isdn x25 static-tei 8
```

Because the **isdn x25 static-tei** command is missing, the following example configuration sets dynamic TEIs for the ISDN channel:

```
interface bri0
 isdn x25 dchannel
```

Related Commands

Command	Description
interface bri	Configures a BRI interface and enters interface configuration mode.
isdn x25 dchannel	Creates a configurable interface for X.25 traffic over the ISDN D channel.

l2f ignore-mid-sequence

To ignore multiplex ID (MID) sequence numbers for sessions in an Layer 2 Forwarding (L2F) tunnel, use the **l2f ignore-mid-sequence** command in VPDN group mode. To remove the ability to ignore MID sequencing, use the **no** form of this command.

l2f ignore-mid-sequence

no l2f ignore-mid-sequence

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes VPDN group configuration

Command History	Release	Modification
	11.3(5)AA	This command was introduced.
	12.0(1)T	This command was implemented on additional Cisco router or access server platforms.

Usage Guidelines This command applies only to L2F initiated tunnels and control packets for initial link control protocol (LCP) tunnel negotiation.

This command is not required for Cisco-to-Cisco, LAC-to-LNS tunnel endpoints, and is only required if MID sequence numbering is not supported by a third-party hardware vendor.

Examples The following example ignores MID sequencing for L2F sessions between a Cisco router and a non-Cisco hardware device, which does not support MID sequencing:

```
l2f ignore-mid-sequence
```

12f tunnel busy timeout

To configure the amount of time that the router will wait before attempting to recontact a router that was previously busy, use the **12f tunnel busy timeout** command in VPDN group configuration mode. To restore the default value, use the **no** form of this command.

12f tunnel busy timeout *seconds*

no 12f tunnel busy timeout

Syntax Description	<i>seconds</i>	Time, in seconds, to wait before checking for router availability. This value can range from 60 to 6000.
--------------------	----------------	--

Defaults	300 seconds
----------	-------------

Command Modes	VPDN group configuration
---------------	--------------------------

Command History	Release	Modification
	12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.	

Examples The following example configures the router to leave a Layer 2 Forwarding Protocol (L2F) destination router on the busy list for 90 seconds:

```
12f tunnel busy timeout 90
```

Related Commands	Command	Description
	12f tunnel retransmit initial retries	Sets the number of times that the router will attempt to send the initial control packet for tunnel establishment before considering a router busy.
	12f tunnel retransmit retries	Sets the number of times the router will attempt to resend tunnel control packets before tearing the tunnel down.
	12f tunnel timeout setup	Sets the amount of time that the router will wait for a confirmation message after sending out the initial control packet before considering a router busy.

l2f tunnel retransmit initial retries

To set the number of times that the router will attempt to send the initial control packet for tunnel establishment before considering a router busy, use the **l2f tunnel retransmit initial retries** command in VPDN group configuration mode. To restore the default value, use the **no** form of this command.

l2f tunnel retransmit initial retries *number*

no l2f tunnel retransmit initial retries

Syntax Description	<i>number</i>	The number of retries that will be attempted, ranging from 1 to 1000.
---------------------------	---------------	---

Defaults	Two retries
-----------------	-------------

Command Modes	VPDN group configuration
----------------------	--------------------------

Command History	Release	Modification
	12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.	

Usage Guidelines	This command can be used only if load sharing is enabled.
-------------------------	---

Examples	The following example configures the router to attempt to send the initial Layer 2 Forwarding (L2F) Protocol control packet five times:
-----------------	---

```
l2f tunnel retransmit initial retries 5
```

Related Commands	Command	Description
	l2f tunnel busy timeout	Configures the amount of time that the router will wait before attempting to recontact a router that was previously busy.
	l2f tunnel retransmit retries	Sets the number of times the router will attempt to resend tunnel control packets before tearing the tunnel down.
	l2f tunnel timeout setup	Sets the amount of time that the router will wait for a confirmation message after sending out the initial control packet before considering a router busy.

I2f tunnel retransmit retries

To set the number of times the router will attempt to resend tunnel control packets before tearing the tunnel down, use the **I2f tunnel retransmit retries** command in VPDN group configuration mode. To restore the default value, use the **no** form of this command.

I2f tunnel retransmit retries *number*

no I2f tunnel retransmit retries

Syntax Description	<i>number</i>	The number of retries that will be attempted, ranging from 5 to 1000.
---------------------------	---------------	---

Defaults	Six retries
-----------------	-------------

Command Modes	VPDN group configuration
----------------------	--------------------------

Command History	Release	Modification
	12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.	

Usage Guidelines	This command does not apply to the initial tunnel setup message or session control packets.
-------------------------	---

Examples	The following example configures the router to attempt to resend Layer 2 Forwarding (L2F) Protocol tunnel control packets ten times before tearing the tunnel down:
-----------------	---

```
I2f tunnel retransmit retries 10
```

Related Commands	Command	Description
	I2f tunnel busy timeout	Configures the amount of time that the router will wait before attempting to recontact a router that was previously busy.
	I2f tunnel retransmit initial retries	Sets the number of times that the router will attempt to send the initial control packet for tunnel establishment before considering a router busy.
	I2f tunnel timeout setup	Sets the amount of time that the router will wait for a confirmation message after sending out the initial control packet before considering a router busy.

l2f tunnel timeout setup

To set the amount of time that the router will wait for a confirmation message after sending out the initial control packet before considering a router busy, use the **l2f tunnel timeout setup** command in VPDN group configuration mode. To restore the default value, use the **no** form of this command.

l2f tunnel timeout setup *seconds*

no l2f tunnel timeout setup

Syntax Description	<i>seconds</i>	Time, in seconds, that the router will wait for a return message. This value can range from 5 to 6000.
---------------------------	----------------	--

Defaults	10 seconds
-----------------	------------

Command Modes	VPDN group configuration
----------------------	--------------------------

Command History	Release	Modification
	12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.	

Usage Guidelines	If the router has not received a confirmation message from the network access server (NAS) before the tunnel timeout setup timer expires, the home gateway (HGW) will be placed on the busy list.
-------------------------	---

Examples	The following example configures the router to wait 25 seconds for confirmation that the initial Layer 2 Forwarding (L2F) Protocol control packet was received:
-----------------	---

```
l2f tunnel timeout setup 25
```

Related Commands	Command	Description
	l2f tunnel busy timeout	Configures the amount of time that the router will wait before attempting to recontact a router that was previously busy.
	l2f tunnel retransmit initial retries	Sets the number of times that the router will attempt to send the initial control packet for tunnel establishment before considering a router busy.
	l2f tunnel retransmit retries	Sets the number of times the router will attempt to resend tunnel control packets before tearing the tunnel down.

l2tp drop out-of-order

To instruct L2TP access concentrator (LAC) or L2TP Network Server (LNS) using Layer 2 Tunneling Protocol (L2TP) to drop packets that are received out of order, use the **l2tp drop out-of-order** command in VPDN group mode. To disable dropping of out-of-sequence packets, use the **no** form of this command.

l2tp drop out-of-order

no l2tp drop out-of-order

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes VPDN group configuration

Command History	Release	Modification
	11.3(5)AA	This command was introduced.
	12.0(1)T	This command was updated for additional Cisco router or access server platforms.

Usage Guidelines This command is valid only for tunnels where sequencing is enabled.

Examples The following example causes the LAC or LNS to drop any packets that are received out of order:

```
l2tp drop out-of-order
```

l2tp flow-control backoff-queuesize



Note

Effective with release 12.2(11)T, the **l2tp flow-control backoff-queuesize** command is no longer available in Cisco IOS software.

To define the maximum number of packets that can be queued locally for a session when a peer's receive window is full, use the **l2tp flow-control backoff-queuesize** command in VPDN group mode. To change the value of the queue size, simply re-enter the command with the new queue size value. To remove a manually configured flow-control backoff value, use the **no** form of this command.

l2tp flow-control backoff-queuesize *queuesize*

no l2tp flow-control backoff-queuesize *queuesize*

Syntax Description

<i>queuesize</i>	Queue size limit on a L2TP access concentrator (LAC) or L2TP network server (LNS) so that when the remote peer receive window is full, the LAC or LNS delays sending additional packets.
------------------	--

Defaults

Layer 2 Transport Protocol (L2TP) flow control backoff queuing is enabled and uses a default value of 25.

Command Modes

VPDN group configuration

Command History

Release	Modification
11.3(5)AA	This command was introduced.
12.0(1)T	This command was implemented on additional Cisco router or access server platforms.
12.2(11)T	Support for this command was removed and it is no longer available in Cisco IOS software.

Usage Guidelines

This command is used for congestion control. This command will not appear as a valid option if the **l2tp flow-control receive-window** command is disabled or if the value is set to zero (for sequencing only).

Examples

The following example uses the **l2tp flow-control receive-window** command option to 8, which in turn enables the **l2tp flow-control backoff-queuesize** command option. When the remote peer's receive window is full, the maximum number packets that can be queued locally for an L2TP session is 35.

```
l2tp flow-control receive-window 8
l2tp flow-control backoff-queuesize 35
```

Related Commands	Command	Description
	l2tp flow-control maximum-ato	Defines the maximum adaptive timeout for congestion control.
	l2tp flow-control receive-window	Defines the receive window on a LAC or LNS and enables either device to send sequence numbers.

l2tp flow-control maximum-ato



Note

Effective with release 12.2(11)T, the **l2tp flow-control maximum-ato** command is no longer available in Cisco IOS software.

To define the maximum adaptive timeout for congestion control, use the **l2tp flow-control maximum-ato** command in VPDN group configuration mode. To reset the timeout to a new value, simply reenter the command with the new value. To remove a manually configured timeout value, use the **no** form of this command.

l2tp flow-control maximum-ato *milliseconds*

no l2tp flow-control maximum-ato *milliseconds*

Syntax Description

<i>milliseconds</i>	Wait time period, in milliseconds, before the L2TP access concentrator (LAC) or L2TP network server (LNS) probes its remote peer receive-window to resume sending packets.
---------------------	--

Defaults

2000 milliseconds

Command Modes

VPDN group configuration

Command History

Release	Modification
11.3(5)AA	This command was introduced.
12.0(1)T	This command was implemented on additional Cisco router or access server platforms.
12.2(11)T	Support for this command was removed and it is no longer available in Cisco IOS software.

Usage Guidelines

This command is used for congestion control between the LAC and LNS. This command will not appear as a valid option if the **l2tp flow-control receive-window** command is disabled or set to zero.

Examples

The following example forces the LAC or LNS to wait 4000 milliseconds before attempting to probe the remote peer's receive status window again:

```
l2tp flow-control maximum-ato 4000
```

Related Commands

Command	Description
I2tp flow-control backoff-queuesize	Defines the maximum number of packets that can be queued locally for a session when the receive window of a peer is full.
I2tp flow-control receive-window	Defines the receive window on a LAC or LNS and enables either device to send sequence numbers.

l2tp flow-control receive-window



Note

Effective with release 12.2(11)T, the **l2tp flow-control receive-window** command is no longer available in Cisco IOS software.

To define the receive window on a L2TP access concentrator (LAC) or Layer 2 Tunneling Protocol Network Server (LNS) and enable either device to send sequence numbers, use the **l2tp flow-control receive-window** command in VPDN group mode. To remove a flow-control receive-window value and disable sequencing, use the **no** form of this command.

l2tp flow-control receive-window *window-size*

no l2tp flow-control receive-window *window-size*

Syntax Description

<i>window-size</i>	The number of packets that can be received by the remote end device before backoff queueing occurs.
--------------------	---

Defaults

Receive window and sequence numbers are disabled.

Command Modes

VPDN group configuration

Command History

Release	Modification
11.3(5)AA	This command was introduced.
12.0(1)T	This command was implemented on additional Cisco router or access server platforms.
12.2(11)T	Support for this command was removed and it is no longer available in Cisco IOS software.

Usage Guidelines

If the receive-window value is set to zero, then sequence numbers are not sent, and congestion control is not enabled. Data zero length body (ZLB) acknowledgments are not sent when congestion control is disabled. If the receive-window value is greater than zero, then congestion control is enabled, and the value that is configured is sent to the L2TP receive window attribute value pair (AVP).

Using the **l2tp flow-control receive-window** command with a value greater than zero allows you to configure the following L2TP (optional) commands:

- **l2tp flow-control maximum-ato**
- **l2tp flow-control backoff-queuesize**

If the **l2tp flow-control receive-window** command is not enabled or the value is set to zero, the **l2tp flow-control maximum-ato** and **2tp flow-control backoff-queuesize** commands will not appear as configurable options by the command parser.

Examples

The following example configures a receive-window value of 25 to be communicated to the remote peer and subsequently enables the configuration of the **l2tp flow-control maximum-ato** and **l2tp flow-control backoff-queuesize** commands.

```
l2tp flow-control receive-window 10
l2tp flow-control maximum-ato 15
l2tp flow-control backoff-queuesize 35
```

Related Commands

Command	Description
l2tp flow-control backoff-queuesize	Defines the maximum number of packets that can be queued locally for a session when the receive window of a peer is full.
l2tp flow-control maximum-ato	Defines the maximum adaptive timeout for congestion control.

l2tp flow-control static-rtt



Note

Effective with release 12.2(11)T, the **l2tp flow-control static-rtt** command is no longer available in Cisco IOS software.

To define a static round-trip time for congestion control, use the **l2tp flow-control static-rtt** command in VPDN group mode. To apply a different value, simply reenter the command with the new value. To disable a static round-trip time, use the **no** form of this command.

l2tp flow-control static-rtt *round-trip-time*

no l2tp flow-control static-rtt *round-trip-time*

Syntax Description

round-trip-time Static round-trip time in milliseconds.

Defaults

Disabled; adaptive timeouts are used.

Command Modes

VPDN group configuration

Command History

Release	Modification
11.3(5)AA	This command was introduced.
12.0(1)T	This command was implemented on additional Cisco router or access server platforms.
12.2(11)T	Support for this command was removed and it is no longer available in Cisco IOS software.

Usage Guidelines

If the LAC/LNS is configured to use a static round-trip time, then adaptive time-outs (ATO) are calculated on the fixed round-trip time value configured using the **l2tp flow-control static-rtt command**. If the device is not configured with the **l2tp flow-control static-rtt** command, then flow control is automatically calculated based on packet send and receive times. You must have the **l2tp-flow control receive-window** command enabled with a value greater than zero to use the **l2tp flow-control maximum-ato** command.

Examples

The following example sets a static round-trip delay of 15000 milliseconds, which in turn disables adaptive timeouts:

```
l2tp flow-control static-rtt 2500
```

Related Commands

Command	Description
I2tp flow-control backoff-queuesize	Defines the maximum number of packets that can be queued locally for a session when the receive window of a peer is full.
I2tp flow-control maximum-ato	Defines the maximum adaptive timeout for congestion control.
I2tp flow-control receive-window	Defines the receive window on a LAC or LNS and enables either device to send sequence numbers.

l2tp hidden

To enable Layer 2 Tunneling Protocol (L2TP) attribute-value (AV) pair hiding, which encrypts the AV pair “value,” use the **l2tp hidden** command in VPDN group mode. To disable L2TP AV pair value hiding, use the **no** form of this command.

l2tp hidden

no l2tp hidden

Syntax Description

This command has no arguments or keywords.

Defaults

L2TP AV pair hiding is disabled.

Command Modes

VPDN group configuration

Command History

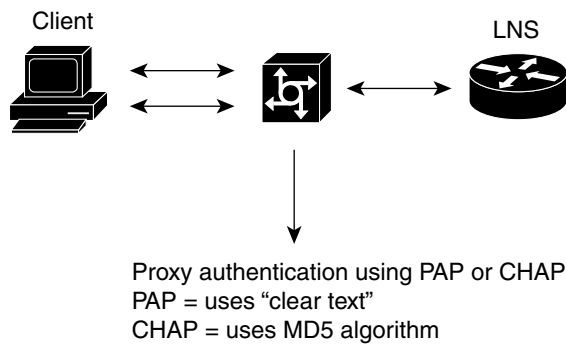
Release	Modification
11.3(5)AA	This command was introduced.
12.0(1)T	This command was implemented on additional Cisco router or access server platforms.

Usage Guidelines

This command is not required if one-time Password Authentication Protocol (PAP) password authentication is used. This command is useful for additional security if PPP is using PAP or proxy authentication between the L2TP access concentrator (LAC) and Layer 2 Tunneling Protocol Network Server (LNS). When AV pair hiding is enabled, the L2TP hiding algorithm is executed, and sensitive passwords that are used between the L2TP AV pairs are encrypted during PAP or proxy authentication.

In [Figure 1](#), the client initiates a PPP session with the LAC, and tunnel authentication begins. The LAC in turn exchanges authentication requests with the LNS. Upon successful authentication between the LAC and LNS, a tunnel is created. Proxy authentication is done by the LAC using either PAP or Challenge Handshake Authentication Protocol (CHAP). Since PAP user name and password information is exchanged between devices in clear-text, it is beneficial to use the **l2tp hidden** command where L2TP AV pair values are encrypted.

Figure 1 LAC-LNS Proxy Authentication



22105

Examples

The following example encrypts the AV pair value exchanged between the LAC and LNS:

```
l2tp hidden
```

l2tp ip tos reflect

To configure a virtual private dialup network (VPDN) group to preserve the ToS field of L2TP-tunneled IP packets, use the **l2tp ip tos reflect** command in VPDN group configuration mode. To specify a type of service (ToS) field of zero for tunneled packets, use the **no** form of this command.

l2tp ip tos reflect

no l2tp ip tos reflect

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes VPDN group configuration

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines The **l2tp ip tos reflect** command can only be configured on L2TP network server (LNS) VPDN groups (VPDN groups that are configured to accept dial-in and/or request dial-out sessions).

Examples The following example shows an LNS configured to preserve IP ToS for L2TP dial-in sessions:

```
vpdn-group 1
  accept-dialin
  protocol l2tp
  virtual-template 1
  terminate-from hostname althea
  local name berththa
  l2tp ip tos reflect
```

The following examples shows an LNS configured to preserve IP ToS for L2TP dial-out sessions:

```
vpdn-group 1
  request-dialout
  protocol l2tp
  pool-member 1
  initiate-to ip 172.29.49.94
  l2tp ip tos reflect
```

Related Commands

Command	Description
request-dialin	Configures a LAC to request L2F or L2TP tunnels to an LNS and create a request-dialin VPDN subgroup, and specifies a dial-in L2F or L2TP tunnel to a remote peer if a dial-in request is received for a specified domain or DNIS.
request dialout	Enables an LNS to request VPDN dial-out calls by using L2TP.

l2tp ip udp checksum

To enable IP User Data Protocol (UDP) checksums on Layer 2 Tunneling Protocol (L2TP) payload packets, use the **l2tp ip udp checksum** command in VPDN group configuration mode. To disable IP UDP checksums, use the **no** form of this command.

l2tp ip udp checksum

no l2tp ip udp checksum

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes VPDN group configuration

Command History	Release	Modification
	11.3(5)AA	This command was introduced.
	12.0(1)T	This command was implemented on additional Cisco router or access server platforms.

Usage Guidelines Enabling IP UDP checksum packets causes the switching path to revert to process-level switching, which results in slower performance.

Examples The following example enables IP UDP checksums on L2TP payload packets:
`l2tp ip udp checksum`

l2tp security crypto-profile

To enable a virtual private dialup network (VPDN) group to be protected by IP Security (IPSec), use the **l2tp security crypto-profile** command in VPDN group configuration mode. To disable IPSec security for a VPDN group, use the **no** form of this command.

l2tp security crypto-profile *profile-name* [**keep-sa**]

no l2tp security crypto-profile *profile-name* [**keep-sa**]

Syntax Description

<i>profile-name</i>	The name of the crypto profile to be used for IPSec protection of tunneled PPP sessions. The <i>profile-name</i> argument must match that of a profile configured using the crypto map command.
keep-sa	(Optional) Controls the destruction of IPSec security associations (SAs) upon tunnel teardown. By default, any IPSec phase 2 SAs and Internet Key Exchange (IKE) phase 1 SAs are destroyed when the Layer 2 Transport Protocol (L2TP) tunnel is torn down. Using the keep-sa keyword prevents the destruction of IKE phase 1 SAs.

Defaults

IPSec security is disabled.
SAs are destroyed on tunnel teardown.

Command Modes

VPDN group configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

Usage Guidelines

A crypto profile must be configured using the **crypto map** (global IPSec) command before it can be associated with a VPDN group using the **l2tp security crypto-profile** command. Enabling this command for a VPDN group ensures that no L2TP packets will be processed unless they have IPSec protection.

The **keep-sa** keyword can be used to prevent the destruction of IKE phase 1 SAs when the L2TP tunnel between the L2TP access concentrator (LAC) and L2TP network server (LNS) is considered permanent, and the IP addresses of the LAC and LNS rarely change. This option is not useful with short-lived tunnels, such as those generated by client-initiated L2TP tunneling.

Examples

The following example configures VPDN group 1, associates it with the crypto profile named l2tp, and prevents the destruction of IKE phase 1 SAs:

```
vpdn-group 1
 request-dialin
  protocol l2tp
  domain cisco.com
 initiate-to ip 10.0.0.13
 local name LAC
 l2tp security crypto-profile l2tp keep-sa
```

Related Commands

Command	Description
crypto map (global IPsec)	Creates or modifies a crypto map entry or creates a crypto profile that provides a template for configuration of dynamically created crypto maps.

l2tp tunnel authentication

To enable Layer 2 Tunneling Protocol (L2TP) tunnel authentication, use the **l2tp tunnel authentication** command in VPDN group configuration mode. To disable L2TP tunnel authentication, use the **no** form of this command.

l2tp tunnel authentication

no l2tp tunnel authentication

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes VPDN group configuration

Command History

Release	Modification
11.3(5)AA	This command was introduced.
12.0(1)T	This command was implemented on additional Cisco router or access server platforms.

Examples

The following example enables L2TP tunnel authentication:

```
l2tp tunnel authentication
```



Note

L2TP tunnel authentication is enabled by default. Therefore, there is no need to enable this command unless it was previously disabled.

I2tp tunnel bearer capabilities

To set the bearer-capability value used by the Cisco router, use the **l2tp tunnel bearer capabilities** command in VPDN group configuration mode. To restore the default value, use the **no** form of this command.

l2tp tunnel bearer capabilities {none | digital | analog | all}

no l2tp tunnel bearer capabilities

Syntax Description

none	Specifies that no access types are supported. This is the default value.
digital	Specifies that digital access is supported.
analog	Specifies that analog access is supported.
all	Specifies that all access types are supported. This is the default value if the accept-dialout command is configured.

Defaults

none
If the **accept-dialout** command is configured: **all**

Command Modes

VPDN group configuration

Command History

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

Usage Guidelines

By default, Cisco routers use a bearer-capability value of **none**. If the **accept-dialout** command is configured, Cisco routers use a bearer-capability value of **all**. To ensure compatibility with some non-Cisco routers, you may be required to override the default bearer-capability value by configuring the **l2tp tunnel bearer capabilities** command.

Examples

The following example configures the bearer-capability value to support only digital access:

```
l2tp tunnel bearer capabilities digital
```

Related Commands

Command	Description
accept-dialout	Accepts requests to tunnel L2TP dial-out calls and creates an accept-dialout VPDN subgroup.
l2tp tunnel framing capabilities	Sets the framing-capability value used by the Cisco router.

I2tp tunnel busy timeout

To configure the amount of time that the router will wait before attempting to recontact a router that was previously busy, use the **i2tp tunnel busy timeout** command in VPDN group configuration mode. To restore the default value, use the **no** form of this command.

i2tp tunnel busy timeout *seconds*

no i2tp tunnel busy timeout

Syntax Description	<i>seconds</i>	Time, in seconds, to wait before checking for router availability. This value can range from 60 to 6000.
---------------------------	----------------	--

Defaults	300 seconds
-----------------	-------------

Command Modes	VPDN group configuration
----------------------	--------------------------

Command History	Release	Modification
	12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.	

Examples	The following example configures the router to leave a Layer 2 Transport Protocol (L2TP) destination router on the busy list for 90 seconds:
-----------------	--

```
i2tp tunnel busy timeout 90
```

Related Commands	Command	Description
	i2tp tunnel retransmit initial retries	Sets the number of times that the router will attempt to send out the initial control packet for tunnel establishment before considering a router busy.
i2tp tunnel retransmit initial timeout	Sets the amount of time that the router will wait before resending an initial packet out to establish a tunnel.	

l2tp tunnel framing capabilities

To set the framing-capability value used by the Cisco router, use the **l2tp tunnel framing capabilities** command in VPDN group configuration mode. To restore the default value, use the **no** form of this command.

l2tp tunnel framing capabilities { **none** | **synchronous** | **asynchronous** | **all** }

no l2tp tunnel framing capabilities

Syntax Description

none	Specifies that no framing types are supported. This is the default value.
synchronous	Specifies that synchronous framing is supported.
asynchronous	Specifies that asynchronous framing is supported.
all	Specifies that all framing types are supported. This is the default value if the accept-dialout command is configured.

Defaults

none
If the **accept-dialout** command is configured: **all**

Command Modes

VPDN group configuration

Command History

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

Usage Guidelines

By default, Cisco routers use a framing-capability value of **none**. If the **accept-dialout** command is configured, Cisco routers use a framing-capability value of **all**. To ensure compatibility with some non-Cisco routers, you may be required to override the default framing-capability value by configuring the **l2tp tunnel framing capabilities** command.

Examples

The following example configures the framing-capability value to support only asynchronous framing:

```
l2tp tunnel framing capabilities asynchronous
```

Related Commands

Command	Description
accept-dialout	Accepts requests to tunnel L2TP dial-out calls and creates an accept-dialout VPDN subgroup.
l2tp tunnel bearer capabilities	Sets the bearer-capability value used by the Cisco router.

l2tp tunnel hello

To set the number of seconds between sending hello keepalive packets for a Layer 2 Tunneling Protocol (L2TP) tunnel, use the **l2tp tunnel hello** command in VPDN group configuration mode. To change the tunnel hello value, simply reenter the command with the new value. To disable the sending of hello keepalive packets, use the **no** form of this command.

l2tp tunnel hello *hello-interval*

no l2tp tunnel hello *hello-interval*

Syntax Description	<i>hello-interval</i>	The interval, in seconds, that the L2TP access concentrator (LAC) and Layer 2 Tunneling Protocol Network Server (LNS) wait before sending the next L2TP tunnel keepalive packet.
---------------------------	-----------------------	--

Defaults	60 seconds
-----------------	------------

Command Modes	VPDN group configuration
----------------------	--------------------------

Command History	Release	Modification
	11.3(5)AA	This command was introduced.
	12.0(1)T	This command was implemented on additional Cisco router or access server platforms.

Usage Guidelines	The L2TP tunnel keepalive timers do not have use the same value on both sides of the tunnel. For example, a LAC can use a keepalive value of 30 seconds, and an LNS can use the default value of 60 seconds.
-------------------------	--

Examples	The following example sets the L2TP tunnel hello value to 90 seconds:
-----------------	---

```
l2tp tunnel hello 90
```

l2tp tunnel password

To set the password that the router will use to authenticate the tunnel, use the **l2tp tunnel password** command in VPDN group configuration mode. To remove a previously configured password, use the **no** form of this command.

l2tp tunnel password *password*

no l2tp tunnel password *password*

Syntax Description

password String that the router uses for tunnel authentication.

Defaults

Disabled. If the **l2tp tunnel password** is not configured, the password associated with the local name is used. If no local name password is configured, the password associated with the host name is used.

Command Modes

VPDN group configuration

Command History

Release	Modification
11.3(5)AA	This command was introduced.
12.0(1)T	This command was implemented on additional Cisco router or access server platforms.

Usage Guidelines

The password defined with the **l2tp tunnel password** command is also used for attribute-value (AV) pair hiding.

The password hierarchy sequence that is used for tunnel identification and, subsequently, tunnel authentication is as follows:

- A Layer 2 Tunneling Protocol (L2TP) tunnel password is used first (defined by the **l2tp tunnel password** command).
- If no L2TP tunnel password exists, the password associated with the local name is used.
- If a local name password does not exist, the password associated with the host name is used.

The **username** command is used to define the passwords associated with the local name and the host name.

Examples

The following example configures the tunnel password, *dustie*, which will be used to authenticate the tunnel between local and remote peer:

```
l2tp tunnel password dustie
```

Related Commands

Command	Description
hostname	Specifies or modifies the host name for the network server.
local name	Specifies a local host name that the tunnel will use to identify itself.
l2tp hidden	Enables L2TP AV pair hiding, which encrypts the AV pair value.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

l2tp tunnel retransmit initial retries

To set the number of times that the router will attempt to send out the initial control packet for tunnel establishment before considering a router busy, use the **l2tp tunnel retransmit initial retries** command in VPDN group configuration mode. To restore the default value, use the **no** form of this command.

l2tp tunnel retransmit initial retries *number*

no l2tp tunnel retransmit initial retries

Syntax Description	<i>number</i>	The number of retries that will be attempted, ranging from 1 to 1000.
--------------------	---------------	---

Defaults	Two retries
----------	-------------

Command Modes	VPDN group configuration
---------------	--------------------------

Command History	Release	Modification
	12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.	

Examples	The following example configures the router to attempt to send the initial Layer 2 Transport Protocol (L2TP) control packet five times:
----------	---

```
l2tp tunnel retransmit initial retries 5
```

Related Commands	Command	Description
	l2tp tunnel busy timeout	Configures the amount of time that the router will wait before attempting to recontact a router that was previously busy.
l2tp tunnel retransmit initial timeout	Sets the amount of time that the router will wait before resending an initial packet out to establish a tunnel.	

I2tp tunnel retransmit initial timeout

To set the amount of time that the router will wait before resending an initial packet out to establish a tunnel, use the **I2tp tunnel retransmit initial timeout** command in VPDN group configuration mode. To restore the default value, use the **no** form of this command.

I2tp tunnel retransmit initial timeout { **min** | **max** } *seconds*

no I2tp tunnel retransmit initial timeout

Syntax Description

min	The minimum time that the router will wait before resending an initial packet.
max	The maximum time that the router will wait before resending an initial packet.
<i>seconds</i>	Time, in seconds, the router will wait before resending an initial packet. This value can range from 1 to 8.

Defaults

min: 1 second
max: 8 seconds

Command Modes

VPDN group configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

Usage Guidelines

This command will take effect only when load balancing is enabled. The first timeout occurs at the value specified by the **min** *seconds* keyword and argument combination. After each packet that is not acknowledged, the timeout exponentially increases until it reaches the value specified by the **max** *seconds* keyword and argument combination, where it then remains.

Examples

The following example configures the router to attempt resending an initial Layer 2 Transport Protocol (L2TP) packet after 2 seconds following the first failed attempt:

```
I2tp tunnel retransmit initial timeout min 2
```

Related Commands

Command	Description
I2tp tunnel busy timeout	Configures the amount of time that the router will wait before attempting to recontact a router that was previously busy.
I2tp tunnel retransmit initial retries	Sets the number of times that the router will attempt to send out the initial control packet for tunnel establishment before considering a router busy.

l2tp tunnel timeout no-session

To set the duration a router waits after a Layer 2 Tunnel Protocol (L2TP) tunnel becomes empty before tearing down the tunnel, use the **l2tp tunnel timeout no-session** command in VPDN group configuration mode. To restore the default timeout value, use the **no** form of this command.

l2tp tunnel timeout no-session {*seconds* | **never**}

no l2tp tunnel timeout no-session

Syntax Description

<i>seconds</i>	Duration, in seconds, the router waits before tearing down an empty L2TP tunnel. The duration can range from 0 to 86400. If the router is configured as an L2TP access concentrator (LAC), the default is 15 seconds. If the router is configured as an L2TP network server (LNS), the default is 10 seconds.
never	Instructs the router to never tear down an empty L2TP tunnel.

Command Default

Empty tunnels will be torn down after the default timeout.

Command Modes

VPDN group configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(11)T	The never keyword was added.

Usage Guidelines

A router is considered a LAC if it has either a request-dialin or accept-dialout virtual private dialup network (VPDN) group configured. A router is considered an LNS if it has either an accept-dialin or request-dialout VPDN group configured.

Examples

The following example configures the router to never tear down empty L2TP tunnels:

```
l2tp tunnel timeout no-session never
```

The following example returns the router to the default timeout duration to tear down empty L2TP tunnels. This default value depends on whether the router is configured as a LAC or an LNS.

```
no l2tp tunnel timeout no-session
```

Related Commands	Command	Description
	accept-dialin	Accepts requests to create either L2F or L2TP tunnels for dial-in.
	accept-dialout	Accepts requests to tunnel L2TP dial-out calls and creates an accept-dialout VPDN subgroup
	request-dialin	Configures a LAC to request L2F or L2TP tunnels to an LNS and create a request-dialin VPDN subgroup, and specifies a dial-in L2F or L2TP tunnel to a remote peer if a dial-in request is received for a specified domain or DNIS.
	request dialout	Enables an LNS to request VPDN dial-out calls by using L2TP.