interface bri

To configure a BRI interface and enter interface configuration mode, use the **interface bri** command in global configuration mode.

Cisco 7200 Series and 7500 Series Routers

interface bri *number*

interface bri *slot*/*port*

Cisco 7200 Series and 7500 Series Routers with BRI Subinterfaces Only

interface bri *number*.*subinterface-number* [**multipoint | point-to-point**]

interface bri *slot*/*port*.*subinterface-number* [**multipoint | point-to-point**]

X.25 on an ISDN BRI Interface

interface bri *number*:**0**

interface bri *slot*/*port*:**0**

Syntax Description

number	Port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the **show interfaces** command.
slot/*port*	On the Cisco 7200 series, slot location and port number of the interface. The slash mark is required.
.*subinterface-number*	Subinterface number in the range from 1 to 4,294,967,293. The *number* that precedes the period (.) must match the *number* this subinterface belongs to. The period is required.
multipoint | point-to-point	(Optional) Specifies a multipoint or point-to-point subinterface. The default is **multipoint**.
:0	Subinterface created by applying the **isdn x25 static-tei** and the **isdn x25 dchannel** commands to the specified BRI interface. This interface must be configured for X.25.

Command Default

The default mode for subinterfaces is multipoint.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.2F	This command was enhanced with the capability to carry X.25 traffic on the D channel.
11.2P	This command was modified to include slot/port syntax for the PA-8B-ST and PA-4B-U port adapters on the Cisco 7200 series.

Usage Guidelines

Subinterfaces can be configured to support partially meshed Frame Relay networks. (Refer to the Frame Relay chapters in the *Cisco IOS Wide-Area Networking Configuration Guide.*)

To specify the BRI interface that is created by enabling X.25 on a specified ISDN BRI interface, use the **interface bri** global configuration command with a subinterface 0 specification.

Examples

The following example configures BRI 0 to call and receive calls from two sites, use PPP encapsulation on outgoing calls, and use Challenge Handshake Authentication Protocol (CHAP) authentication on incoming calls:

```
interface bri 0
 encapsulation ppp
 no keepalive
 dialer map ip 172.16.36.10 name EB1 234
 dialer map ip 172.16.36.9 name EB2 456
 dialer-group 1
 isdn spid1 41346334600101 4633460
 isdn spid2 41346334610101 4633461
 isdn T200 1000
 ppp authentication chap
```

The following example creates a BRI 0:0 interface for X.25 traffic over the D channel and then configures the new interface to carry X.25 traffic:

```
interface bri 0
 isdn x25 dchannel
 isdn x25 static-tei 8
!
interface bri 0:0
 ip address 10.1.1.2 255.255.255.0
 x25 address 31107000000100
 x25 htc 1
 x25 suppress-calling-address
 x25 facility windowsize 2 2
 x25 facility packetsize 256 256
 x25 facility throughput 9600 9600
 x25 map ip 10.1.1.3 31107000000200
```

Related Commands

Command	Description
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
encapsulation	Sets the encapsulation method used by the interface.

Command	Description
isdn spid1, isdn spid2	Defines the SPID number that has been assigned by the ISDN service provider for the B1 channel.
ppp bap call	Sets PPP BACP call parameters.
show interfaces bri	Displays information about the BRI D channel or about one or more B channels.

interface dialer

To define a dialer rotary group, use the **interface dialer** command in global configuration mode.

interface dialer *dialer-rotary-group-number*

no interface dialer *dialer-rotary-group-number*

Syntax Description

dialer-rotary-group-number	Number of the dialer rotary group in the range from 0 to 255.

Command Default

No dialer rotary groups are predefined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Dialer rotary groups allow you to apply a single interface configuration to a set of physical interfaces. This capability allows a group of interfaces to be used as a pool of interfaces for calling many destinations.

Once the interface configuration is propagated to a set of interfaces, those interfaces can be used to place calls using the standard dial-on-demand routing (DDR) criteria. When multiple destinations are configured, any of these interfaces can be used for outgoing calls.

Dialer rotary groups are useful in environments that require multiple calling destinations. Only the rotary group needs to be configured with the **dialer map** commands. The only configuration required for the interfaces is the **dialer rotary-group** command indicating that each interface is part of a dialer rotary group.

Although a dialer rotary group is configured as an interface, it is not a physical interface. Instead, it represents a group of interfaces. Interface configuration commands entered after the **interface dialer** command will be applied to all physical interfaces assigned to specified rotary groups. Individual interfaces in a dialer rotary group do not have individual addresses. The dialer interface has a protocol address, and that address is used by all interfaces in the dialer rotary group.

Examples

The following example identifies interface dialer 1 as the dialer rotary group leader. Interface dialer 1 is not a physical interface, but represents a group of interfaces. The interface configuration commands that follow apply to all interfaces included in this group.

```
interface dialer 1
 encapsulation ppp
 authentication chap
 dialer in-band
 ip address 10.2.3.4
 dialer map ip 10.2.2.5 name YYY 14155553434
 dialer map ip 10.3.2.6 name ZZZ
```

interface multilink

To create a multilink bundle and enter the multilink interface configuration mode to configure the multilink bundle, use the **interface multilink** command in the global configuration mode. To remove a multilink bundle, use the **no** form of this command.

interface multilink *multilink-bundle-number*

no interface multilink

Syntax Description

multilink-bundle-number	Number of the multilink bundle. The range is from 1 to 65535.

Command Default

No multilink bundles are created.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.0	This command was implemented on the Cisco 10000 Series Performance Routing Engine 1 (PRE-1).
12.2(16)BX	This command was implemented on the Cisco 10000 Series PRE-2.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB for the Cisco 10000 Series PRE-2.
12.2(31)SB2	This command was implemented on the Cisco 10000 Series PRE-3 and the range of valid values for multilink interfaces was expanded on the PRE-3.
3.4.0S	The maximum value that can be assigned to the *multilink-bundle-number* argument was changed from 2147483647 to 65535.

Usage Guidelines

Cisco 10000 Series Routers

The following describes the valid multilink interface values for the Cisco 10000 Series Routers:

- 1 to 9999—(PRE-2) Cisco IOS Release 12.2(28)SB and later releases
- 1 to 9999 and 65536 to
  - 1 to 9999 and 65536 to 2147483647 (Cisco IOS Release 12.2(31)SB2 and later releases)
  - 1 to 9999 and 65536 to 2147483647 (Cisco IOS Release 12.2(31)SB2 and later releases)

the range of the *multilink-bundle-number* argument is from 1 to 2147483647.

From Cisco ASR 1000 Series Routers Release 3.4.0S onward, the range of the *multilink-bundle-number* argument is from 1 to 65535.

Examples

The following example shows how to create multilink bundle 1:

```
Router# configure terminal
Router(config)# interface multilink 1
Router(config-if)# ip address 192.168.11.4 255.255.0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ppp multilink
Router(config-if)# keepalive
```

Related Commands

Command	Description
ppp multilink fragment disable	Disables packet fragmentation.
ppp multilink group	Restricts a physical link from joining only a designated multilink group interface.

interface serial

To specify a serial interface created on a channelized E1 or channelized T1 controller (for ISDN PRI, channel-associated signaling, or robbed-bit signaling), use the **interface serial** command in global configuration mode.

Cisco 7200 Series and Cisco 7500 Series Routers

interface serial *slot*/*port*:*timeslot*

no interface serial *slot*/*port*:*timeslot*

Cisco AS5200 Series and Cisco 4000 Series Access Servers

interface serial *controller-number*:*timeslot*

no interface serial *controller-number*:*timeslot*

Syntax Description

slot/*port*	Slot number and port number where the channelized E1 or T1 controller is located. The slash mark is required.
:*timeslot*	For ISDN, the D channel time slot, which is the **:23** channel for channelized T1 and the **:15 channel** for channelized E1. PRI time slots are in the range from 0 to 23 for channelized T1 and in the range from 0 to 30 for channelized E1. For channel-associated signaling or robbed-bit signaling, the channel group number. The colon is required. On a dual port card, it is possible to run channelized on one port and primary rate on the other port.
controller-number	Channelized E1 or T1 controller number.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Examples

The following example configures channel groups on time slots 1 to 11 and ISDN PRI on time slots 12 to 24 of T1 controller 0. Then the examples configures the first two channel groups as serial interfaces 0:0 and 0:1.

```
controller t1 0
channel-group 0 timeslot 1-6
channel-group 1 timeslot 7
channel-group 2 timeslot 8
channel-group 3 timeslot 9-11
pri-group timeslots 12-24
!
interface serial 0:0
ip address 172.18.13.2 255.255.255.0
encapsulation ppp
!
interface serial 0:1
ip address 172.18.13.3 255.255.255.0
encapsulation ppp
```

The following example configures ISDN PRI on T1 controller 4/1 and then configures the D channel on the resulting serial interface 4/1:23:

```
controller t1 4/1
framing crc4
linecode hdb3
pri-group timeslots 1-24

interface serial 4/1:23
ip address 172.18.13.1 255.255.255.0
encapsulation ppp
```

Related Commands

Command	Description
controller	Configures a T1 or E1 controller and enters controller configuration mode.
show controllers t1 call-counters	Displays the total number of calls and call durations on a T1 controller.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

interface virtual-ppp

To configure a virtual-PPP interface, use the **interface virtual-ppp** command in global configuration mode. To disable a virtual-PPP interface, use the **no** form of this command.

interface virtual-ppp *number*

no interface virtual-ppp *number*

Syntax Description

number	Virtual-PPP interface number. The range is from 1 to 2147483647.

Command Default

A virtual-PPP interface is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
15.2(4)S	This command was modified. The behavior of the **no** form of this command was modified. A configured pseudowire must be disabled before disabling a virtual-PPP interface.

Usage Guidelines

Use the **interface virtual-ppp** command to enter interface configuration mode and configure a virtual interface with PPP encapsulation.

After configuring a virtual-PPP interface, you can configure a pseudowire by using the **pseudowire** command in interface configuration mode. To disable a virtual-PPP interface that has a configured pseudowire, remove the pseudowire by using the **no pseudowire** command. Disable the virtual-PPP interface by using the **no interface virtual-ppp** command in global configuration mode or interface configuration mode.

Examples

The following example shows how to configure a virtual-PPP interface:

```
Device# configure terminal
Device(config)# interface virtual-ppp 503
```

The following example shows how to remove a virtual-PPP interface that has a configured pseudowire.You must first remove the configured pseudowire or an error is generated. Note that you can remove the virtual-PPP interface in interface configuration mode, as shown below:

```
Device(config)# no interface virtual-ppp 1
% Interface Virtual-PPP1 not removed - Remove the Pseudowire
Device(config)# interface virtual-ppp 1
Device(config-if)# no pseudowire
Device(config-if)# no interface virtual-ppp 1
Device(config-if)# end
```

Related Commands

Command	Description
l2tp-class	Creates a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes and enters L2TP class configuration mode.
pseudowire	Binds a virtual circuit to a Layer 2 pseudowire for an xconnect service.
pseudowire-class	Specifies the name of a Layer 2 pseudowire class and enters pseudowire class configuration mode.

interface virtual-template

To create a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces, use the **interface virtual-template** command in global configuration mode. To remove a virtual template interface, use the **no** form of this command.

interface virtual-template *number*

no **interface virtual-template** *number*

Syntax Description

number	Number used to identify the virtual template interface. Up to 200 virtual template interfaces can be configured. On the Cisco 10000 series router, up to 4095 virtual template interfaces can be configured.

Command Default

No virtual template interface is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2F	This command was introduced.
12.2(4)T	This command was enhanced to increase the maximum number of virtual template interfaces from 25 to 200.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

A virtual template interface is used to provide the configuration for dynamically created virtual access interfaces. It is created by users and can be saved in NVRAM.

After the virtual template interface is created, it can be configured in the same way as a serial interface.

Virtual template interfaces can be created and applied by various applications such as virtual profiles, virtual private dialup networks (VPDNs), PPP over ATM, protocol translation, and Multichassis Multilink PPP (MMP).

Cisco 10000 Series Router

You can configure up to 4095 total virtual template interfaces on the Cisco 10000 series router.

To ensure proper scaling and to minimize CPU utilization, we recommend the following virtual template interface settings:

- A keepalive timer of 30 seconds or greater using the **keepalive** command. The default is 10 seconds.
- Do not enable the Cisco Discovery Protocol (CDP). CDP is disabled by default. Use the **no cdp enable** command to disable CDP, if necessary.

- Disable link-status event messaging using the **no logging event link-status** command.
- To prevent the virtual-access subinterfaces from being registered with the SNMP functionality of the router and using memory, do not use the router's SNMP management tools to monitor PPP sessions. Use the **no virtual-template snmp** command to disable the SNMP management tools.

When a virtual template interface is applied dynamically to an incoming user session, a virtual access interface (VAI) is created.

If you configure a virtual template interface with interface-specific commands, the Cisco 10000 series router does not achieve the highest possible scaling. To verify that the router does not have interface-specific commands within the virtual template interface configuration, use the **test virtual-template** *number* **subinterface** command.

Examples

Cisco 10000 Series Router

The following example creates a virtual template interface called Virtual-Template1:

```
Router(config)# interface Virtual-Template1
Router(config-if)# ip unnumbered Loopback1
Router(config-if)# keepalive 60
Router(config-if)# no peer default ip address
Router(config-if)# ppp authentication pap
Router(config-if)# ppp authorization vpn1
Router(config-if)# ppp accounting vpn1
Router(config-if)# no logging event link-status
Router(config-if)# no virtual-template snmp
```

Virtual Template with PPP Authentication Example

The following example creates and configures virtual template interface 1:

```
interface virtual-template 1 type ethernet
 ip unnumbered ethernet 0
 ppp multilink
 ppp authentication chap
```

IPsec Virtual Template Example

The following example shows how to configure a virtual template for an IPsec virtual tunnel interface.

```
interface virtual-template1 type tunnel
 ip unnumbered Loopback1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile virtualtunnelinterface
```

Related Commands

Command	Description
cdp enable	Enables Cisco Discovery Protocol (CDP) on an interface.
clear interface virtual-access	Tears down the live sessions and frees the memory for other client uses.
keepalive	Enables keepalive packets and to specify the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing down the interface.
show interface virtual-access	Displays the configuration of the active VAI that was created using a virtual template interface.
tunnel protection	Associates a tunnel interface with an IPsec profile.
virtual interface	Sets the zone name for the connected AppleTalk network.

Command	Description
virtual-profile	Enables virtual profiles.
virtual template	Specifies the destination for a tunnel interface.

ip address negotiated

To specify that the IP address for a particular interface is obtained via PPP/IPCP (IP Control Protocol) address negotiation, use the **ip address negotiated** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ip address negotiated [*previous*]

no ip address negotiated [*previous*]

Syntax Description

previous	(Optional) IPCP attempts to negotiate the previously assigned address.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Use the **ip address negotiated** interface command to enable a Cisco router to automatically negotiate its own registered WAN interface IP address from a central server (via PPP/IPCP) and to enable all remote hosts to access the global Internet using this single registered IP address.

Examples

The following example configures an asynchronous interface (interface async1) to obtain its IP address via PPP/IPCP address negotiation:

```
interface async1
 ip address negotiated
 encapsulation ppp
```

Related Commands

Command	Description
encapsulation	Sets the encapsulation method used by the interface.
ip address	Sets a primary or secondary IP address for an interface.
ip unnumbered	Enables IP processing on an interface without assigning an explicit IP address to the interface.

ip address-pool

To enable a global default address pooling mechanism used to supply IP addresses to dial-in asynchronous, synchronous, or ISDN point-to-point interfaces, use the **ip address-pool** command in global configuration mode. To disable IP address pooling globally on all interfaces with the default configuration, use the **no** form of this command.

ip address-pool {**dhcp-pool** | **dhcp-proxy-client** | **local**}

no ip address-pool

Syntax Description

dhcp-pool	Uses on-demand address pooling as the global default address mechanism. This option supports only remote access PPP sessions using a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN). IP addresses are obtained from locally configured virtual routing and forwarding (VRF)-associated Dynamic Host Configuration Protocol (DHCP) pools.
dhcp-proxy-client	Uses the router as the proxy client between a third-party DHCP server and peers connecting to the router as the global default address mechanism.
local	Uses the local address pool named *default* as the global default address mechanism.

Command Default

IP address pooling is disabled globally.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(8)T	The **dhcp-pool** keyword was added.

Usage Guidelines

The global default IP address pooling mechanism applies to all interfaces that have been left in the default setting of the **peer default ip address** command.

If any **peer default ip address** command other than **peer default ip address pool** (the default) is configured, the interface uses that mechanism and not the global default mechanism. Thus all interfaces can be independently configured, or left unconfigured so that the global default configuration applies. This flexibility minimizes the configuration effort on the part of the administrator.

The **ip address-pool dhcp-pool** command supports only remote access PPP sessions using an MPLS VPN. IP addresses are obtained from locally configured VRF-associated DHCP pools. A VRF VPN instance is a per-VPN routing information repository that defines the VPN membership of a customer site.

Examples

The following example specifies the DHCP on-demand address pooling mechanism as the global default mechanism for assigning peer IP addresses:

```
ip address-pool dhcp-pool
```

The following example specifies the DHCP proxy client mechanism as the global default mechanism for assigning peer IP addresses:

```
ip address-pool dhcp-proxy-client
```

The following example specifies a local IP address pool named “default” as the global default mechanism for all interfaces that have been left in their default setting:

```
ip address-pool local
```

Related Commands

Command	Description
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.

ip dhcp-client network-discovery

To control the sending of Dynamic Host Configuration Protocol (DHCP) Inform and Discover messages, use the **ip dhcp-client network-discovery** command in global configuration mode. To change or disable DHCP message control, use the **no** form of this command.

ip dhcp-client network-discovery informs *number-of-messages* **discovers** *number-of-messages* **period** *seconds*

no ip dhcp-client network-discovery informs *number-of-messages* **discovers** *number-of-messages* **period** *seconds*

Syntax Description

informs *number-of-messages*	Number of DHCP Inform messages. Valid choices are 0, 1, or 2 messages. Default is 0 messages.
discovers *number-of-messages*	Number of DHCP Discover messages. Valid choices are 0, 1, or 2 messages. Default is 0 messages.
period *seconds*	Timeout period for retransmission of DHCP Inform and Discover messages. Valid periods are from 3 to 15 seconds. Default is 15 seconds.

Command Default

0 DHCP Inform and Discover messages (network discovery is disabled when both the **informs** and **discovers** keywords are set to 0); 15-second timeout period.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip dhcp-client network-discovery** command allows peer routers to dynamically discover Domain Name System (DNS) and NetBIOS name server information configured on a DHCP server using PPP IP Control Protocol (IPCP) extensions. Setting the number of DHCP Inform or Discover messages to 1 or 2 determines how many times the system sends a DHCP Inform or Discover message before stopping network discovery, as follows:

- When the number of DHCP Inform messages is set to 1, once the first Inform messages is sent the system waits for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of the timeout period, the system sends a DHCP Discover message when the number of Discover messages is not set to 0. If the number of Discover messages is set to 1, network discovery stops. If the number of Discover messages is set to 2, the system waits

again for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of this second timeout period, the system sends a second DHCP Discover message and stops network discovery.

- When the number of DHCP Inform messages is set to 2, once the first Inform messages is sent, the system waits for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of the timeout period, the system sends another DHCP Inform message. If the number of Discover messages is set to 1, network discovery stops. If the number of Discover messages is set to 2, the system waits again for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of this second timeout period, the system sends a second DHCP Discover message and stops network discovery.

Network discovery also stops when the DHCP server responds to DHCP Inform and Discover messages before the configured number of messages and timeout period are exceeded.

Setting the number of messages to 0 disables sending of DHCP Inform and Discover messages, and is the same as entering the **no ip dhcp-client network-discovery** command. When the **ip dhcp-client network-discovery** command is disabled, the system falls back to the static configurations made using the **async-bootp dns-server** and **async-bootp nb-server** global configuration commands or, as a last resort, to a DNS server address assigned with the **ip name-server** command.

Examples

The following example sets two DHCP Inform and Discovery messages and a timeout period of 12 seconds:

```
ip dhcp-client network-discovery informs 2 discovers 2 period 12
```

Related Commands

Command	Description
async-bootp	Configures extended BOOTP requests for asynchronous interfaces as defined in RFC 1084.
ip dhcp-server	Specifies which DHCP servers to use on a network, and specifies the IP address of one or more DHCP servers available on the network.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip dhcp client route

To configure the Dynamic Host Configuration Protocol (DHCP) client to associate any added routes with a specified tracked object number, use the **ip dhcp client** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

ip dhcp client route track *number*

no ip dhcp client route track

Syntax Description

route track *number*	Associates a tracked object number with the DHCP-installed static route. Valid values for the *number* argument range from 1 to 500.

Command Default

No routes are associated with a track number.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)XE	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **ip dhcp client** command must be configured before the **ip address dhcp** command is configured on an interface. The **ip dhcp client** command is checked only when an IP address is acquired from DHCP. If the **ip dhcp client** command is specified after an IP address has been acquired from DHCP, the **ip dhcp client** command will not take effect until the next time the router acquires an IP address from DHCP.

Examples

The following example configures DHCP on an Ethernet interface and associates tracked object 123 with routes generated from this interface:

```
interface ethernet 0/0
 ip dhcp client route track 123
 ip address dhcp
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an Ethernet interface from the DHCP.

ip dhcp-server

To specify which Dynamic Host Configuration Protocol (DHCP) servers to use on your network, or to specify the IP address of one or more DHCP servers available on the network, use the **ip dhcp-server** command in global configuration mode. To remove a DHCP server IP address, use the **no** form of this command.

ip dhcp-server [*ip-address* | *name*]

no ip dhcp-server [*ip-address* | *name*]

Syntax Description

ip-address	(Optional) IP address of a DHCP server.
name	(Optional) Name of a DHCP server.

Command Default

The IP limited broadcast address of 255.255.255.255 is used for transactions if no DHCP server is specified. This default allows automatic detection of DHCP servers.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A DHCP server temporarily allocates network addresses to clients through the access server on an as-needed basis. While the client is active, the address is automatically renewed in a minimum of 20-minute increments. When the user terminates the session, the interface connection is terminated so that network resources can be quickly reused. You can specify up to ten servers on the network.

In normal situations, if a SLIP or PPP session fails (for example, if a modem line disconnects), the allocated address will be reserved temporarily to preserve the same IP address for the client when dialed back into the server. This way, the session that was accidentally terminated can often be resumed.

To use the DHCP proxy-client feature, enable your access server to be a proxy-client on asynchronous interfaces by using the **ip address-pool dhcp-proxy-client** command. If you want to specify which DHCP servers are used on your network, use the **ip dhcp-server** command to define up to ten specific DHCP servers.

Note To facilitate transmission, configure intermediary routers (or access servers with router functionality) to use an IP helper address whenever the DHCP server is not on the local LAN and the access server is using broadcasts to interact with the DHCP server. Refer to the chapters about configuring IP addressing in the *Cisco IOS IP Addressing Services Configuration Guide*.

The **ip address-pool dhcp-proxy-client** command initializes proxy-client status to all interfaces defined as asynchronous on the access server. To selectively disable proxy-client status on a single asynchronous interface, use the **no peer default ip address** interface command.

Examples

The following command specifies a DHCP server with the IP address of 172.24.13.81:

```
ip dhcp-server 172.24.13.81
```

Related Commands

Command	Description
ip address-pool	Enables an address pooling mechanism used to supply IP addresses to dial-in asynchronous, synchronous, or ISDN point-to-point interfaces.
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.
show cot dsp	Displays information about the COT DSP configuration or current status.

ip idle-group

To configure interesting traffic on a virtual template interface for the PPP idle timer, use the **ip idle-group** command in interface configuration mode. To remove the configuration, use the **no** form of this command.

ip idle-group {*access-list-number* | *access-list-name*} {**in** | **out**}

no ip idle-group {*access-list-number* | *access-list-name*} {**in** | **out**}

Syntax Description

access-list-number	IP access list number.
access-list-name	IP access list name.
in	Classifies IP inbound traffic for the PPP idle timer.
out	Classifies IP outbound traffic for the PPP idle timer.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The **ip idle-group** command is applied to a virtual template interface and configures interesting traffic on either inbound or outbound traffic.

Examples

The following example specifies access list 101 as interesting for inbound IP traffic and access list 102 as interesting for outbound IP traffic:

```
interface virtual-template 1
 ppp timeout idle 60
 ip idle-group 101 in
 ip idle-group 102 out
```

Related Commands

Command	Description
corlist incoming	Sets the PPP idle timeout parameters on a virtual template interface.

ip local pool

To configure a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface, use the **ip local pool** command in global configuration mode. To remove a range of addresses from a pool (the longer of the **no** forms of this command), or to delete an address pool (the shorter of the **no** forms of this command), use one of the **no** forms of this command.

ip local pool {**default** | *poolname*} [*low-ip-address* [*high-ip-address*]] [**group** *group-name*] [**cache-size** *size*] [**recycle delay** *seconds*]

no ip local pool *poolname low-ip-address* [*high-ip-address*]

no ip local pool {**default** | *poolname*}

Syntax Description

default	Creates a default local IP address pool that is used if no other pool is named.
poolname	Name of the local IP address pool.
low-IP-address [*high-IP-address*]	(Optional) First and, optionally, last address in an IP address range.
group *group-name*	(Optional) Creates a pool group.
cache-size *size*	(Optional) Sets the number of IP address entries on the free list that the system checks before assigning a new IP address. Returned IP addresses are placed at the end of the free list. Before assigning a new IP address to a user, the system checks the number of entries from the end of the list (as defined by the **cache-size** *size* option) to verify that there are no returned IP addresses for that user. The range for the cache size is 0 to 100. The default cache size is 20.
recycle delay *seconds*	(Optional) Indicates the time (in seconds) to hold an IP address in the local pool before making it available for reuse.

Command Default

No address pools are configured. Any pool created without the optional **group** keyword is a member of the base system group.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
11.3AA	This command was enhanced to allow address ranges to be added and removed.
12.1(5)DC	This command was enhanced to allow pool groups to be created.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and support was added for the Cisco 6400 node route processor 25v (NRP-25v) and Cisco 7400 platforms.
12.4(15)T	The **recycle delay** keyword and *seconds* argument were added.

Usage Guidelines

Use the **ip local pool** command to create one or more local address pools from which IP addresses are assigned when a peer connects. You may also add another range of IP addresses to an existing pool. To use a named IP address pool on an interface, use the **peer default ip address pool** interface configuration command. A pool name can also be assigned to a specific user using authentication, authorization, and accounting (AAA) RADIUS and TACACS functions.

If no named local IP address pool is created, a default address pool is used on all point-to-point interfaces after the **ip address-pool local** global configuration command is issued. If no explicit IP address pool is assigned, but pool use is requested by use of the **ip address-pool local** command, the special pool named "default" is used.

The optional **group** keyword and associated group name allows the association of an IP address pool with a named group. Any IP address pool created *without* the **group** keyword automatically becomes a member of a *base* system group.

The optional **recycle delay** keyword and its associated time indicates the time in seconds to hold the IP address from the pool before making it available for reuse.

An IP address pool name can be associated with only one group. Subsequent use of the same pool name, within a pool group, is treated as an extension of that pool, and any attempt to associate an existing local IP address pool name with a different pool group is rejected. Therefore, each use of a pool name is an implicit selection of the associated pool group.

Note To reduce the chances of inadvertent generation of duplicate addresses, the system allows creation of the special pool named "default" only in the base system group, that is, no group name can be specified with the pool name "default."

All IP address pools within a pool group are checked to prevent overlapping addresses; however, no checks are made between any group pool member and a pool not in a group. The specification of a named pool within a pool group allows the existence of overlapping IP addresses with pools in other groups, and with pools in the base system group, but not among pools within a group. Otherwise, processing of the IP address pools is not altered by their membership in a group. In particular, these pool names can be specified in **peer** commands and returned in RADIUS and AAA functions with no special processing.

IP address pools can be associated with Virtual Private Networks (VPNs). This association permits flexible IP address pool specifications that are compatible with a VPN and a VPN routing and forwarding (VRF) instance.

The IP address pools can also be used with the **translate** commands for one-step vty-async connections and in certain AAA or TACACS+ authorization functions. Refer to the chapter "Configuring Protocol Translation and Virtual Asynchronous Devices" in the *Cisco IOS Terminal Services Configuration Guide* and the "System Management" part of the *Cisco IOS Configuration Fundamentals Configuration Guide* for more information.

IP address pools are displayed with the **show ip local pool** EXEC command.

Examples

The following example creates a local IP address pool named "pool2," which contains all IP addresses in the range 172.16.23.0 to 172.16.23.255:

```
ip local pool pool2 172.16.23.0 172.16.23.255
```

The following example configures a pool of 1024 IP addresses:

```
no ip local pool default
ip local pool default 10.1.1.0 10.1.4.255
```

Note Although not required, it is good practice to precede local pool definitions with a **no** form of the command to remove any existing pool, because the specification of an existing pool name is taken as a request to extend that pool with the new IP addresses. If the intention is to extend the pool, the **no** form of the command is not applicable.

The following example configures multiple ranges of IP addresses into one pool:

```
ip local pool default 10.1.1.0 10.1.9.255
ip local pool default 10.2.1.0 10.2.9.255
```

The following examples show how to configure two pool groups and IP address pools in the base system group:

```
ip local pool p1-g1 10.1.1.1 10.1.1.50 group grp1
ip local pool p2-g1 10.1.1.100 10.1.1.110 group grp1
ip local pool p1-g2 10.1.1.1 10.1.1.40 group grp2
ip local pool lp1 10.1.1.1 10.1.1.10
ip local pool p3-g1 10.1.2.1 10.1.2.30 group grp1
ip local pool p2-g2 10.1.1.50 10.1.1.70 group grp2
ip local pool lp2 10.1.2.1 10.1.2.10
```

In the example:

- Group grp1 consists of pools p1-g1, p2-g1, and p3-g1.
- Group grp2 consists of pools p1-g2 and p2-g2.
- Pools lp1 and lp2 are not associated with a group and are therefore members of the base system group.

Note that IP address 10.1.1.1 overlaps groups grp1, grp2, and the base system group. Also note that there is no overlap within any group including the base system group, which is unnamed.

The following examples show configurations of IP address pools and groups for use by a VPN and VRF:

```
ip local pool p1-vpn1 10.1.1.1 10.1.1.50 group vpn1
ip local pool p2-vpn1 10.1.1.100 10.1.1.110 group vpn1
ip local pool p1-vpn2 10.1.1.1 10.1.1.40 group vpn2
ip local pool lp1 10.1.1.1 10.1.1.10
ip local pool p3-vpn1 10.1.2.1 10.1.2.30 group vpn1
ip local pool p2-vpn2 10.1.1.50 10.1.1.70 group vpn2
ip local pool lp2 10.1.2.1 10.1.2.10
```

The examples show configuration of two pool groups, including pools in the base system group, as follows:

- Group vpn1 consists of pools p1-vpn1, p2-vpn1, and p3-vpn1.
- Group vpn2 consists of pools p1-vpn2 and p2-vpn2.
- Pools lp1 and lp2 are not associated with a group and are therefore members of the base system group.

Note that IP address 10.1.1.1 overlaps groups vpn1, vpn2, and the base system group. Also note that there is no overlap within any group including the base system group, which is unnamed.

The VPN needs a configuration that selects the proper group by selecting the proper pool based on remote user data. Thus, each user in a given VPN can select an address space using the pool and associated group appropriate for that VPN. Duplicate addresses in other VPNs (other group names) are not a concern, because the address space of a VPN is specific to that VPN.

In the example, a user in group vpn1 is associated with some combination of the pools p1-vpn1, p2-vpn1, and p3-vpn1, and is allocated addresses from that address space. Addresses are returned to the same pool from which they were allocated.

The following example configures a recycle delay of 30 seconds to hold IP addresses in the pool before making them available for reuse:

```
ip local pool default 10.1.1.0 10.1.9.255 recycle delay 30
```

Related Commands

Command	Description
debug ip peer	Displays additional output when IP address pool groups are defined.
ip address-pool	Enables an address pooling mechanism used to supply IP addresses to dial in asynchronous, synchronous, or ISDN point-to-point interfaces.
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.
show ip local pool	Displays statistics for any defined IP address pools.
translate lat	Translates a LAT connection request automatically to another outgoing protocol connection type.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection type.

ip route

To establish static routes, use the **ip route** command in global configuration mode. To remove static routes, use the **no** form of this command.

ip route [vrf *vrf-name***]** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]

no ip route [vrf *vrf-name***]** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]

Syntax Description

vrf *vrf-name*	(Optional) Configures the name of the VRF by which static routes should be specified.
prefix	IP route prefix for the destination.
mask	Prefix mask for the destination.
ip-address	IP address of the next hop that can be used to reach that network.
interface-type interface-number	Network interface type and interface number.
dhcp	(Optional) Enables a Dynamic Host Configuration Protocol (DHCP) server to assign a static route to a default gateway (option 3). **Note** Specify the **dhcp** keyword for each routing protocol.
distance	(Optional) Administrative distance. The default administrative distance for a static route is 1.
name *next-hop-name*	(Optional) Applies a name to the next hop route.
permanent	(Optional) Specifies that the route will not be removed, even if the interface shuts down.
track *number*	(Optional) Associates a track object with this route. Valid values for the *number* argument range from 1 to 500.
tag *tag*	(Optional) Tag value that can be used as a “match” value for controlling redistribution via route maps.

Command Default

No static routes are established.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.3(2)XE	The **track** keyword and *number* argument were added.
12.3(8)T	The **track** keyword and *number* argument were integrated into Cisco IOS Release 12.3(8)T. The **dhcp** keyword was added.

Release	Modification
12.3(9)	The changes made in Cisco IOS Release 12.3(8)T were added to Cisco IOS Release 12.3(9).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The establishment of a static route is appropriate when the Cisco IOS software cannot dynamically build a route to the destination.

When you specify a DHCP server to assign a static route, the interface type and number and administrative distance may be configured also.

If you specify an administrative distance, you are flagging a static route that can be overridden by dynamic information. For example, routes derived with Enhanced Interior Gateway Routing Protocol (EIGRP) have a default administrative distance of 100. To have a static route that would be overridden by an EIGRP dynamic route, specify an administrative distance greater than 100. Static routes have a default administrative distance of 1.

Static routes that point to an interface on a connected router will be advertised by way of Routing Information Protocol (RIP) and EIGRP regardless of whether **redistribute static** commands are specified for those routing protocols. This situation occurs because static routes that point to an interface are considered in the routing table to be connected and hence lose their static nature. Also, the target of the static route should be included in the **network** (DHCP) command. If this condition is not met, no dynamic routing protocol will advertise the route unless a **redistribute static** command is specified for these protocols. With the following configuration:

```
rtr1 (serial 172.16.188.1/30)--------------> rtr2(Fast Ethernet 172.31.1.1/30) ------>

router [rip | eigrp]
 network 172.16.188.0
 network 172.31.0.0
```

- RIP and EIGRP redistribute the route if the route is pointing to the Fast Ethernet interface:

  ```
  ip route 172.16.188.252 255.255.255.252 FastEthernet 0/0
  ```

  RIP and EIGRP do not redistribute the route with the following **ip route** command because of the split horizon algorithm:

  ```
  ip route 172.16.188.252 255.255.255.252 serial 2/1
  ```

- EIGRP redistributes the route with both of the following commands:

  ```
  ip route 172.16.188.252 255.255.255.252 FastEthernet 0/0
  ip route 172.16.188.252 255.255.255.252 serial 2/1
  ```

With the Open Shortest Path First (OSPF) protocol, static routes that point to an interface are not advertised unless a **redistribute static** command is specified.

Adding a static route to an Ethernet or other broadcast interface (for example, ip route 0.0.0.0 0.0.0.0 Ethernet 1/2) will cause the route to be inserted into the routing table only when the interface is up. This configuration is not generally recommended. When the next hop of a static route points to an interface, the router considers each of the hosts within the range of the route to be directly connected through that interface, and therefore it will send Address Resolution Protocol (ARP) requests to any destination addresses that route through the static route.

A logical outgoing interface, for example, a tunnel, needs to be configured for a static route. If this outgoing interface is deleted from the configuration, the static route is removed from the configuration and hence does not show up in the routing table. To have the static route inserted into the routing table again, configure the outgoing interface once again and add the static route to this interface.

The practical implication of configuring the **ip route 0.0.0.0 0.0.0.0 ethernet 1/2** command is that the router will consider all of the destinations that the router does not know how to reach through some other route as directly connected to Ethernet interface 1/2. So the router will send an ARP request for each host for which it receives packets on this network segment. This configuration can cause high processor utilization and a large ARP cache (along with memory allocation failures). Configuring a default route or other static route that directs the router to forward packets for a large range of destinations to a connected broadcast network segment can cause your router to reload.

Specifying a numerical next hop that is on a directly connected interface will prevent the router from using proxy ARP. However, if the interface with the next hop goes down and the numerical next hop can be reached through a recursive route, you may specify both the next hop and interface (for example, **ip route 0.0.0.0 0.0.0.0 ethernet 1/2 10.1.2.3**) with a static route to prevent routes from passing through an unintended interface.

Note Configuring a default route that points to an interface, such as **ip route 0.0.0.0 0.0.0.0 ethernet 1/2**, displays a warning message. This command causes the router to consider all the destinations that the router cannot reach through an alternate route, as directly connected to Ethernet interface 1/2. Hence, the router sends an ARP request for each host for which it receives packets on this network segment. This configuration can cause high processor utilization and a large ARP cache (along with memory allocation failures). Configuring a default route or other static route that directs the router to forward packets for a large range of destinations to a connected broadcast network segment can cause the router to reload.

The **name** *next-hop-name* keyword and argument combination allows you to associate static routes with names in your running configuration. If you have several static routes, you can specify names that describe the purpose of each static route in order to more easily identify each one.

The **track** *number* keyword and argument combination specifies that the static route will be installed only if the state of the configured track object is up.

Recursive Static Routing

In a recursive static route, only the next hop is specified. The output interface is derived from the next hop.

For the following recursive static route example, all destinations with the IP address prefix address prefix 192.168.1.1/32 are reachable via the host with address 10.0.0.2:

```
ip route 192.168.1.1 255.255.255.255 10.0.0.2
```

A recursive static route is valid (that is, it is a candidate for insertion in the IPv4 routing table) only when the specified next hop resolves, either directly or indirectly, to a valid IPv4 output interface, provided the route does not self-recurse, and the recursion depth does not exceed the maximum IPv4 forwarding recursion depth.

The following example defines a valid recursive IPv4 static route:

```
interface serial 2/0
 ip address 10.0.0.1 255.255.255.252
 exit
ip route 192.168.1.1 255.255.255.255 10.0.0.2
```

The following example defines an invalid recursive IPv4 static route. This static route will not be inserted into the IPv4 routing table because it is self-recursive. The next hop of the static route, 192.168.1.0/30, resolves via the first static route 192.168.1.0/24, which is itself a recursive route (that is, it only specifies a next hop). The next hop of the first route, 192.168.1.0/24, resolves via the directly connected route via the serial interface 2/0. Therefore, the first static route would be used to resolve its own next hop.

```
interface serial 2/0
 ip address 10.0.0.1 255.255.255.252
 exit
ip route 192.168.1.0 255.255.255.0 10.0.0.2
ip route 192.168.1.0 255.255.255.252 192.168.1.100
```

It is not normally useful to manually configure a self-recursive static route, although it is not prohibited. However, a recursive static route that has been inserted in the IPv4 routing table may become self-recursive as a result of some transient change in the network learned through a dynamic routing protocol. If this situation occurs, the fact that the static route has become self-recursive will be detected and the static route will be removed from the IPv4 routing table, although not from the configuration. A subsequent network change may cause the static route to no longer be self-recursive, in which case it will be re-inserted in the IPv4 routing table.

Note IPv4 recursive static routes are checked at one-minute intervals. Therefore, a recursive static route may take up to a minute to be inserted into the routing table once its next hop becomes valid. Likewise, it may take a minute or so for the route to disappear from the table if its next hop becomes invalid.

Examples

The following example shows how to choose an administrative distance of 110. In this case, packets for network 10.0.0.0 will be routed to a router at 172.31.3.4 if dynamic information with an administrative distance less than 110 is not available.

```
ip route 10.0.0.0 255.0.0.0 172.31.3.4 110
```

Note Specifying the next hop without specifying an interface when configuring a static route can cause traffic to pass through an unintended interface if the default interface goes down.

The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6:

```
ip route 172.31.0.0 255.255.0.0 172.31.6.6
```

The following example shows how to route packets for network 192.168.1.0 directly to the next hop at 10.1.2.3. If the interface goes down, this route is removed from the routing table and will not be restored unless the interface comes back up.

```
ip route 192.168.1.0 255.255.255.0 Ethernet 0 10.1.2.3
```

The following example shows how to install the static route only if the state of track object 123 is up:

```
ip route 0.0.0.0 0.0.0.0 Ethernet 0/1 10.1.1.242 track 123
```

The following example shows that using the **dhcp** keyword in a configuration of Ethernet interfaces 1 and 2 enables the interfaces to obtain the next-hop router IP addresses dynamically from a DHCP server:

```
ip route 10.165.200.225 255.255.255.255 ethernet1 dhcp
ip route 10.165.200.226 255.255.255.255 ethernet2 dhcp 20
```

The following example shows that using the **name** *next-hop-name* keyword and argument combination for each static route in the configuration helps you remember the purpose for each static route.

```
ip route 172.0.0.0 255.0.0.0 10.0.0.1 name Seattle2Detroit
```

The name for the static route will be displayed when the **show running-configuration** command is entered:

```
Router# show running-config | include ip route

ip route 172.0.0.0 255.0.0.0 10.0.0.1 name Seattle2Detroit
```

Related Commands

Command	Description
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

ip route (large-scale dial-out)

To establish static routes and define the next hop for large-scale dial-out, use the **ip route** command in global configuration mode. To remove static routes, use the **no** form of this command.

ip route *network-number network-mask* {*ip-address* | *interface*} [*distance*] [**name** *name*]

no ip route

Syntax Description

network-number	IP address of the target network or subnet.
network-mask	Network mask that lets you mask network and subnetwork bits.
ip-address	Internet address of the next hop that can be used to reach that network in standard IP address notation. Example: 10.1.1.1.
interface	Network interface name and number to use.
distance	(Optional) Administrative distance, which is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers.
name *name*	(Optional) Name of the user profile.

Command Default

No static route is established.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

A static route is appropriate when the communication server cannot dynamically build a route to the destination.

If you specify an administrative distance, you are flagging a static route that can be overridden by dynamic information. For example, Interior Gateway Routing Protocol (IGRP)-derived routes have a default administrative distance of 100. To have a static route that would be overridden by an IGRP dynamic route, specify an administrative distance greater than 100. Static routes have a default administrative distance of 1.

Static routes that point to an interface will be advertised using RIP, IGRP, and other dynamic routing protocols, regardless of whether redistribute static commands were specified for those routing protocols. These static routes will be advertised because static routes that point to an interface are considered to be connected in the routing table and hence lose their static nature. However, if you define a static route to an interface that is not in one of the networks defined in a network command, no dynamic routing protocols will advertise the route unless a redistribute static command is specified for these protocols.

The user profile name is passed to an authentication, authorization, and accounting (AAA) server as the next hop for large-scale dial-out, and is the *name* argument with the -out suffix appended. The suffix is automatically supplied and is required because dial-in and user profile names must be unique.

Examples

In the following example, an administrative distance of 110 was chosen. In this case, packets for network 10.0.0.0 will be routed via to the communication server at 172.19.3.4 if dynamic information with an administrative distance less than 110 is not available.

```
ip route 10.0.0.0 255.0.0.0 172.19.3.4 110
```

In the following example, packets for network 172.19.0.0 will be routed to the communication server at 172.19.6.6:

```
ip route 172.19.0.0 255.255.0.0 172.19.6.6
```

In the following example, the user profile named “profile1-out” will be retrieved from the AAA server:

```
ip route 10.0.0.0 255.255.255.255 Dialer0 name profile1
```

Related Commands

Command	Description
show ip route	Displays all static IP routes, or those installed using the AAA route download function.

ip rtp reserve

To reserve a special queue for a set of Real-Time Transport Protocol (RTP) packet flows belonging to a range of User Datagram Protocol (UDP) destination ports, use the **ip rtp reserve** command in interface configuration mode. To disable the special queue for real-time traffic, use the **no** form of this command.

ip rtp reserve *lowest-udp-port range-of-ports* [*maximum-bandwidth*]

no ip rtp reserve

Syntax Description

lowest-udp-port	Lowest UDP port number to which the packets are sent.
range-of-ports	Number, which when added to the lowest UDP port value, yields the highest UDP port value.
maximum-bandwidth	(Optional) Bandwidth, in kilobits per second, reserved for the RTP packets to be sent to the specified UDP ports.

Command Default

This function is disabled by default. No default values are provided for the arguments.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

If the bandwidth needed for RTP packet flows exceeds the maximum bandwidth specified, the reserved queue will degrade to a best-effort queue.

This command helps in improving the delay bounds of voice streams by giving them a higher priority.

Note The **ip rtp reserve** command configuration is retained on the multilink interface on reloading the router. This is displayed in the **show running-configuration interface** *multilink* command output.

Examples

The following example reserves a unique queue for traffic to destination UDP ports in the range 32768 to 32788 and reserves 1000 kbps bandwidth for that traffic:

```
Router(config)# interface multilink 7856
Router(config-if)# ip rtp reserve 32768 20 1000
```

The following example shows the configuration for Multilink interface 7856:

```
Router# show running-configuration interface multilink 7856

Building configuration...
Current configuration : 118 bytes
!
 interface Multilink7856
```

```
 no ip address
 ppp multilink
 ppp multilink group 7856
 !
ip rtp reserve 2008 192 40
end
```

Related Commands

Command	Description
ppp multilink	Enables MLP on an interface and, optionally, enables dynamic bandwidth allocation.
ppp multilink fragment delay	Specifies a maximum size, in units of time, for packet fragments on an MLP bundle.
ppp multilink interleave	Enables interleaving of packets among the fragments of larger packets on an MLP bundle.
show running-configuration	Displays the current running configuration.

ip tcp async-mobility server

To enable asynchronous listening, which in turn allows TCP connections to TCP port 57, use the **ip tcp async-mobility server** command in global configuration mode. To turn listening off, use the **no** form of this command.

ip tcp async-mobility server

no ip tcp async-mobility server

Syntax Description

This command has no arguments or keywords.

Command Default

Asynchronous listening is disabled (turned off).

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

After asynchronous listening is turned on by the **ip tcp async-mobility server** command, use the **tunnel** command to establish a network layer connection to a remote host. Both commands must be used to enable asynchronous mobility.

Examples

The following example shows how to configure asynchronous mobility. The **tunnel** command is used to establish a network layer connection with an IBM host named "mktg."

```
Router# configure terminal
Router(config)# ip tcp async-mobility server
Router(config)# exit

Router# tunnel mktg
```

Related Commands

Command	Description
tunnel	Sets up a network layer connection to a router.

ip telnet comport

To enable the Cisco IOS Telnet server to use the RFC 2217 Com Port extensions, use the **ip telnet comport** command in global configuration mode. To disable RFC 2217 Com Port extensions, use the **no** form of this command.

ip telnet comport {**disconnect delay** *seconds* | **enable** | **flow level** *number-of-characters* | **receive window** *window-size*}

no ip telnet comport enable

Syntax Description

disconnect delay	(Optional) Delay before TCP closes after the DTR drop. **Note** At lease one of these alternative keywords must be entered.
enable	(Optional) Enables the Cisco IOS Telnet server to use the RFC 2217 Com Port extensions.
flow level	(Optional) Sets the flow control level.
receive window	(Optional) Sets the maximum TCP receive window size.
seconds	Number of seconds to delay the TCP closure. Possible values: 0 to 360.
number-of-charcters	Number of characters to be saved in the device buffer before sending an RFC 2217 SUSPEND message.
window-size	Maximum window size. Possible values: 1 to 4128.

Command Default

Telnet Com Port extensions are enabled

Command Modes

Global configuration

Command History

Release	Modification
11.3(1)	This command was introduced.
12.1	This was integrated into Cisco IOS Release 12.1.
12.2	This was integrated into Cisco IOS Release 12.2.
12.3	This was integrated into Cisco IOS Release 12.3.
12.4	This was integrated into Cisco IOS Release 12.4.

Usage Guidelines

RFC 2217 Telnet Com Port extensions are used to communicate modem hardware signal status from a modem on a network access server (NAS) to a TCP/IP client. An example would be a client PC using a package such as DialOut/EZ (Tacticalsoftware.com) to provide an emulated COM port via a TCP connection to a Cisco AS5000 NAS with integrated modems.

When Com Port extensions are enabled on the NAS, the binary Telnet option (RFC 856) should be used. The Telnet client must connect to TCP ports 6000+ for individual lines, or 7000+ for rotaries on the Cisco NAS.

Setting the Command to Avoid Interruptions

Although the default settings for the **ip telnet comport** command are suitable for most applications, in a few cases some settings should be changed for efficient communications. Two possible situations are described below.

- Preventing Data Buffer Overflows

  Before the application can send data it must determine the modem's readiness for transmission. This checking process generates some initial data. If many of these checks occur in a short period of time, the data will be buffered.

  Command **ip telnet comport can be set** to prevent a buffer overflow from of these trivial data events. In this case, the ip telnet comport flow level (range: 1 through 1023) is adjusted. This enables the PC-hosted comm-serv to send a signal to the remote to prevent (SUSPEND) transmission of any data or commands. When the application is actually ready to receive data, the remote can start transmissions.

- Handling DTR Drops

  When a Data Terminal Ready (DTR, a signal pin on a serial interface) is dropped during a communcation, the PC application may incorrectly interpret the event as an error. This situation can be prevented by changing the disconnect delay (range is 1 to 360 seconds) of command **ip telnet comport** . Adding this delay gives the application time to receive and properly act on the DTR drop message before the tcp connection is closed down.

Examples

The following example disables Telnet Com Port extensions:

```
no ip telnet comport enable
```

Related Commands

Command	Description
debug telnet	Displays information about Telnet option negotiation messages for incoming Telnet connections to a Cisco IOS Telnet server.

ip telnet hidden

To hide IP address or host name information when a Telnet session is established, use the **ip telnet hidden** command in global configuration mode. To make IP address or hostname information visible, use the **no** form of this command.

ip telnet hidden {**addresses** | **hostnames**}

no ip telnet hidden {**addresses** | **hostnames**}

Syntax Description

addresses	Specifies that IP addresses will not be displayed when a Telnet session is established.
hostnames	Specifies that host names will not be displayed when a Telnet session is established.

Command Default

IP addresses and host names are visible

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)	This command was introduced.

Usage Guidelines

By default, when a Telnet client connects to the server, the client will display a message with the server IP address and host name, as shown in the following example:

```
Router# telnet is-dialer

Trying is-dialer.cisco.com (10.20.0.167)... Open
```

The **ip telnet hidden** command can be configured to hide the IP address of the client or the host name of the client in the message. Configuring the **ip telnet hidden addresses** command results in the client displaying a message with the IP address of the server hidden, as shown in the following example:

```
Router# telnet is-dialer

Trying is-dialer.cisco.com address #1 ... Open
```

Configuring the **ip telnet hidden hostnames** command results in the client displaying a message with the host name of the server hidden, as shown in the following example:

```
Router# telnet is-dialer

Trying (10.20.0.167) ... Open
```

Configuring both the **ip telnet hidden addresses** and **ip telnet hidden hostnames** commands results in the client displaying a message with both the IP address and the host name of the server hidden, as shown in the following example:

```
Router# telnet is-dialer

Trying address #1 ... Open
```

Examples

The following example configures the Telnet client to hide both IP addresses and host name information when connecting to the server:

```
ip telnet hidden addresses
ip telnet hidden hostnames
```

Related Commands

Command	Description
busy-message	Creates a “host failed” message that displays when a connection fails.
ip telnet quiet	Suppresses the display of Telnet connection messages.
telnet	Logs in to a host that supports Telnet.

ip telnet quiet

To suppress the display of Telnet connection messages, use the **ip telnet quiet** command in global configuration mode. To cancel this option, use the **no** form of this command.

ip telnet quiet

no ip telnet quiet

Syntax Description

This command has no arguments or keywords.

Command Default

Telnet connection message suppression is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

The **ip telnet quiet** command does not suppress TCP or error messages. It is most useful to Internet service providers, to allow them to hide the onscreen messages displayed during connection, including Internet addresses, from subscription users.

Examples

The following example globally disables onscreen connect messages:

```
ip telnet quiet
```

The following example shows the login and logout messages displayed during login and logout when the **ip telnet quiet** command has *not* been configured to suppress Cisco IOS software messages:

```
Router# telnet Server3

Translating "Server3"...domain server (171.68.89.42) [OK]
Trying Server3--Server3.cisco.com (171.68.89.42)... Open
Kerberos:       No default realm defined for Kerberos!


login:User2
Password:
        Welcome to OpenVMS VAX version V6.1 on node CRAW
    Last interactive login on Tuesday, 15-DEC-1998 11:01
    Last non-interactive login on Sunday,  3-JAN-1999 22:32

Server3)logout
   User2        logged out at  16-FEB-2000 09:38:27.85
[Connection to Server3 closed by foreign host]
```

The following example shows the limited messages displayed during login and logout when the **ip telnet quiet** command has been configured to suppress Cisco IOS software messages:

```
Router# telnet Server3

login:User2
Password:
         Welcome to OpenVMS VAX version V6.1 on node CRAW
     Last interactive login on Tuesday, 15-DEC-1998 11:01
     Last non-interactive login on Sunday,  3-JAN-1999 22:32

Server3)logout
    User2        logged out at  16-FEB-2000 09:38:27.85
```

Related Commands

Command	Description
busy-message	Creates a “host-failed” message that displays when a connection fails.
rlogin	Logs in to a UNIX host using rlogin.
service hide-telnet-address	Hides addresses while trying to establish a Telnet session.
telnet	Logs in to a host that supports Telnet.

ip telnet timeout retransmit

To specify a maximum period that TCP will attempt to retransmit a segment for a Telnet connection, use the **ip telnet timeout** command in global configuration mode. To remove the maximum TCP retransmission period, use the **no** form of this command.

ip telnet timeout retransmit *seconds*

no ip telnet timeout retransmit

Syntax Description

seconds	Number of seconds for the timeout value. Values can range from 1 to 2147483.

Command Default

no ip telnet timeout retransmit

Command Modes

Global configuration

Command History

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

Usage Guidelines

Configure the **ip telnet timeout** command to specify an explicit maximum period that TCP will attempt to retransmit a segment for a Telnet connection. For the default setting (**no ip telnet timeout retransmit**), TCP's retransmit timeout will be based on the estimated round trip time for the connection (typically, seven or eight minutes).

Note If Telnet has no data to transmit, the TCP connection remains indefinitely (regardless of whether the other end is reachable), unless you configure TCP keepalives. This setting has an effect on connections using the Telnet protocol (whether inbound or outbound), not on connections using other protocols such as rlogin and ssh (secure shell).

Examples

The following example sets the TCP retransmit time to a value of 12 hours:

```
Router(config)#ip telnet timeout retransmit 432000
```

Related Commands

Command	Description
service tcp-keepalives-in	Enables TCP keepalives on an inbound connection.
service tcp-keepalives-out	Enables TCP keepalives on an outbound connection.
telnet	Logs in to a host that supports Telnet.

ip telnet tos

To set the type of service (ToS) precedence bits in the IP header for Telnet packets sent by the router, use the **ip telnet tos** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip telnet tos *hex-value*

no ip telnet tos

Syntax Description

hex-value	Hexadecimal value of the ToS precedence bits in the IP header. Valid values range from 0 to FF. The default value is 0xC0.

Command Default

The default ToS value for Telnet packets is 0xC0.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2(10)P	This command was introduced.
11.3(1)	This command was integrated into Cisco IOS Release 11.3(1).
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Compatibility with older Telnet clients may require the configuration of the **ip telnet tos 0** command.

Examples

The following example configures a ToS precedence bit value of 0xF0 in the IP header:

```
Router(config)# ip telnet tos F0
```

The following example displays the output for an invalid ToS precedence value:

```
Router(config)# ip telnet tos F2
%Invalid TOS F2
```

Related Commands

Command	Description
telnet	Logs in to a host that supports Telnet.

ip udptn source-interface

To configure the source IP address for a User Datagram Protocol Telnet (UDPTN) interface connection, use the **ip udptn source-interface** command in global configuration mode. To disable the previously configured UDPTN interface, use the **no** form of this command.

ip udptn source-interface *type number*

no ip udptn source-interface

Syntax Description

type number	The interface type and number whose address is to be used as the source for UDPTN connections.

Command Default The address of the interface closest to the destination is selected as the source address.

Command Modes Global configuration (config)

Command History

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

Examples The following example shows how to configure Virtual Multipoint Interface (VMI) for a UDPTN connection:

```
Router# configure terminal
Router(config)# ip udptn source-interface vmi 23
```

Related Commands

Command	Description
ip tftp source-interface	Specifies the IP address of an interface as the source address for TFTP connections.

ipx compression cipx

To enable compression of Internetwork Packet Exchange (IPX) packet headers in a PPP session, use the **ipx compression cipx** command in interface configuration mode. To disable compression of IPX packet headers in a PPP session, use the **no** form of this command.

ipx compression cipx *number-of-slots*

no ipx compression cipx

Syntax Description

number-of-slots	Number of stored IPX headers allowed. The range is from 10 to 256. A slot is similar to a table entry for a complete IPX header. When a packet is received, the receiver stores the complete IPX header in a slot and tells the destination which slot it used. As subsequent CIPX packets are sent, the receiver uses the slot number field to determine which complete IPX header to associate with the CIPX packet before passing the packet up to IPX.

Command Default No compression of IPX packets during a PPP session. Default number of slots is 16.

Command Modes Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines This interface configuration command enables IPX header compression on PPP links.

Examples The following example enables IPX header compression for PPP:

```
encapsulation ppp
ipx compression cipx 128
```

Related Commands

Command	Description
show ipx compression	Displays the current status and statistics of IPX header compression during PPP sessions.

ipx ppp-client

To enable a nonrouting Internetwork Packet Exchange (IPX) client to connect to an asynchronous interface, the interface must be associated with a loopback interface configured to run IPX. To permit such connections, use the **ipx ppp-client** command in interface configuration mode. To disable a nonrouting IPX client, use the **no** form of this command.

ipx ppp-client loopback *loopback-interface-number*

no ipx ppp-client loopback *loopback-interface-number*

Syntax Description

loopback	Loopback interface configured with a unique IPX network number.
loopback-interface-number	Number of the loopback interface.

Command Default

IPX client connections are not permitted over PPP.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command enables IPX clients to log in to the router from a device running a virtual terminal protocol, then issue the PPP command at the EXEC prompt to connect to a remote device.

You must first configure a loopback interface with a unique IPX network number. The loopback interface is then assigned to an asynchronous interface, which permits IPX clients to connect to the asynchronous interface.

Examples

The following example configures IPX to run over PPP on asynchronous interface 3:

```
ipx routing 0000.0c07.b509
interface loopback0
 no ip address
 ipx network 544
 ipx sap-interval 2000
interface ethernet0
 ip address 172.21.14.64
 ipx network AC150E00
 ipx encapsulation SAP
interface async 3
 ip unnumbered ethernet0
 encapsulation ppp
 async mode interactive
 async default ip address 172.18.1.128
 ipx ppp-client loopback0
 ipx sap-interval 0
```

Related Commands

Command	Description
interface loopback	Creates a loopback interface.
ipx network	Enables IPX routing on a particular interface and optionally selects the type of encapsulation (framing).

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 signaling 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.

Command Default

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

called-party-number	(Optional) Telephone number of the called party. At least one value—*called-party-number* or *subaddress*—must be specified. The maximum number of digits for *called-party-number* 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.
subaddress	(Optional) Subaddress number used for ISDN multipoint connections. At least one value—*called-party-number* or *subaddress*—must be specified. The maximum number of digits for *subaddress* is 50.

Command Default

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 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, 5550122 is the called-party number and 1234 is the subaddress:

```
interface bri 0
 isdn answer1 5550122:1234
```

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.

Command Default

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** (BRI) or **isdn switch-type** (PRI) 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)	Specifies the central office switch type on the ISDN BRI interface.
isdn switch-type (PRI)	Specifies the central office switch type on the ISDN PRI interface.

isdn bcac service audit

To enable service audits on an interface configured for B-Channel Availability Control (BCAC), use the **isdn bcac service audit** command in interface configuration mode. To disable service audits, use the **no** form of this command.

isdn bcac service audit

no isdn bcac service audit

Syntax Description This command has no arguments or keywords.

Command Default This command is disabled by default.

Command Modes Interface configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines This commands starts service audits for all triggers. Use the **isdn bcac service audit trigger** command to selectively enable and disable audit triggers.

Examples The following example shows how to configure service audits on serial interface 2:23:

```
interface serial 2:23
 isdn bcac service audit
```

Related Commands

Command	Description
isdn bcac service audit interface	Specifies that the BCAC service audit needs to be triggered on the entire interface.
isdn bcac service audit trigger	Enables individual BCAC service triggers.
isdn bcac service retry in-serv-on-fail	Specifies that the BCAC service state of the channel needs to be changed to In Service because no acknowledgment was received.
isdn bcac service retry max	Specifies the maximum number of times a BCAC service message can be retransmitted when unacknowledged.
isdn bcac service timer	Changes the value of the BCAC T3M1 or T323 service message timer.
isdn bcac service update linkup	Triggers updates of the BCAC service states between peer nodes through exchange of SERV and SERV ACK messages.

Command	Description
isdn bcac service update provision	Enables the functionality of service status for provisioning ISDN PRI B channels.
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 bcac service audit interface

To specify that B-Channel Availability Control (BCAC) service audit needs to be triggered on the entire interface, use the **isdn bcac service audit interface** command in interface configuration mode. To change or remove the specification, use the **no** form of this command.

isdn bcac service audit interface

no isdn bcac service audit interface

Syntax Description

This command has no arguments or keywords.

Command Default

The default can be to trigger audits on a single channel, a group of channels, or the entire interface, depending upon the type of trigger set. See the "Usage Guidelines" section for the **isdn bcac service audit trigger** command for the list of triggers.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use this command when the service audit needs to be triggered on the entire interface when a condition to trigger the service audit is triggered for any channel.

Examples

The following example shows how to configure service audits on serial interface 2:23:

```
interface serial 2:23
 isdn bcac service audit interface
```

Related Commands

Command	Description
isdn bcac service audit	Enables service audits on an interface configured for BCAC.
isdn bcac service audit trigger	Enables individual BCAC service triggers.
isdn bcac service retry in-serv-on-fail	Specifies that the BCAC service state of the channel needs to be changed to In Service because no acknowledgment was received.
isdn bcac service retry max	Specifies the maximum number of times a BCAC service message can be retransmitted when unacknowledged.
isdn bcac service timer	Changes the value of the BCAC T3M1 or T323 service message timer.
isdn bcac service update linkup	Triggers updates of the BCAC service states between peer nodes through exchange of SERV and SERV ACK messages.

Command	Description
isdn bcac service update provision	Enables the functionality of service status for provisioning ISDN PRI B channels.
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 bcac service audit trigger

To reenable individual B-Channel Availability Control (BCAC) service triggers, use the **isdn bcac service audit trigger** command in interface configuration mode. To disable individual service triggers, use the **no** form of this command.

isdn bcac service audit trigger *number*

no isdn bcac service audit trigger *number*

Syntax Description

number	A number from 1 to 6 that disables specific service triggers; see a list of these triggers in the "Usage Guidelines" section.

Command Default All triggers are configured.

Command Modes Interface configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines The service audit procedure can be used by the either the user or network side to bring both ends of the interface into agreement about the service status through an exchange of SERV and SERV ACK messages.

Following is the list of triggers with the conditions that cause them. Triggers 1 through 4 are triggered by single-channel audits. Trigger 5 occurs on the entire interface. Trigger 6 applies to a group of channels, which in some cases may apply to the entire interface.

- Trigger 1: Upon receiving an incoming call indicating a channel that is in the out-of-service (OOS) or Maint (maintenance) state.
- Trigger 2: Upon receiving an unsolicited SERV ACK message when the received service status differs from the current status.
- Trigger 3: Upon receiving an unallowed response to a SERV message. An unallowed response means a SERV ACK message, which indicates a higher availability than was sent in the SERV message.
- Trigger 4: Upon receiving an ISDN call clearing message with cause code 44 (requested channel not available) when this message is not caused by "glare," which is a SETUP message collision requesting the same channel.
- Trigger 5: Once every 24 hours on all channels.
- Trigger 6: Once every hour on all channels that are in the OOS or Far-end state.

Examples

The following example shows how to disable service trigger 4 on serial interface 2:23:

```
interface serial 2:23
 no isdn bcac service audit trigger 4
```

Related Commands

Command	Description
isdn bcac service audit	Enables service audits on an interface configured for BCAC.
isdn bcac service audit interface	Specifies that the BCAC service audit needs to be triggered on the entire interface.
isdn bcac service retry in-serv-on-fail	Specifies that the BCAC service state of the channel needs to be changed to In Service because no acknowledgment was received.
isdn bcac service retry max	Specifies the maximum number of times a BCAC service message can be retransmitted when unacknowledged.
isdn bcac service timer	Changes the value of the BCAC T3M1 or T323 service message timer.
isdn bcac service update linkup	Triggers updates of the BCAC service states between peer nodes through exchange of SERV and SERV ACK messages.
isdn bcac service update provision	Enables the functionality of service status for provisioning ISDN PRI B channels.
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 bcac service retry in-serv-on-fail

To specify that the B-Channel Availability Control (BCAC) service state of the channel needs to be changed to In Service because no acknowledgment was received, use the **isdn bcac service retry in-serv-on-fail** command in interface configuration mode. To change or remove this specification, use the **no** form of this command.

isdn bcac service retry in-serv-on-fail

no isdn bcac service retry in-serv-on-fail

Syntax Description

This command has no arguments or keywords.

Command Default

Original service state is maintained.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use this command when there is a need to change the service state of a channel to In Service when no acknowledgment is received, even after retransmitting the service message the maximum number of allowed times. If this command is not configured, the original service state is maintained.

Examples

The following example shows how to configure an option whereby, on service message exchange failure, the service state of the concerned channel or channels will be set to In Service:

```
interface serial 2:23
 isdn bcac service retry in-serv-on-fail
```

Related Commands

Command	Description
isdn bcac service audit	Enables service audits on an interface configured for BCAC.
isdn bcac service audit interface	Specifies that the BCAC service audit needs to be triggered on the entire interface.
isdn bcac service audit trigger	Enables individual BCAC service triggers.
isdn bcac service retry max	Specifies the maximum number of times a BCAC service message can be retransmitted when unacknowledged.
isdn bcac service timer	Changes the value of the BCAC T3M1 or T323 service message timer.
isdn bcac service update linkup	Triggers updates of the BCAC service states between peer nodes through exchange of SERV and SERV ACK messages.

Command	Description
isdn bcac service update provision	Enables the functionality of service status for provisioning ISDN PRI B channels.
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 bcac service retry max

To specify the maximum number of times a B-Channel Availability Control (BCAC) service message can be retransmitted when unacknowledged, use the **isdn bcac service retry max** command in interface configuration mode. To remove or change the specification, use the **no** form of this command.

isdn bcac service retry max *retries*

no isdn bcac service retry max *retries*

Syntax Description

retries	A number from 0 to 127 that determines the maximum number of times that a service message can be retransmitted when unacknowledged. Default is 2.

Command Default

Maximum retransmissions is 2.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

When a SERV message is sent to the far side, SERV message timer T3M1 or T323 is started. If no SERV ACK message is received before these timers expire, the SERV message is retransmitted. This command determines how many times retransmission occurs.

Examples

The following example shows how to set the maximum service message retransmissions on serial interface 2:23 to 50:

```
interface serial 2:23
 isdn bcac service retry max 50
```

Related Commands

Command	Description
isdn bcac service audit	Enables service audits on an interface configured for BCAC.
isdn bcac service audit interface	Specifies that the BCAC service audit needs to be triggered on the entire interface.
isdn bcac service audit trigger	Enables individual BCAC service triggers.
isdn bcac service retry in-serv-on-fail	Specifies that the BCAC service state of the channel needs to be changed to In Service because no acknowledgment was received.
isdn bcac service timer	Changes the value of the BCAC T3M1 or T323 service message timer.
isdn bcac service update linkup	Triggers updates of the BCAC service states between peer nodes through exchange of SERV and SERV ACK messages.

Command	Description
isdn bcac service update provision	Enables the functionality of service status for provisioning ISDN PRI B channels.
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 bcac service timer

To change the value of the B-Channel Availability Control (BCAC) T3M1 or T323 service message timer, use the **isdn bcac service timer** command in interface configuration mode. To change the timer value, use the **no** form of this command.

isdn bcac service timer *milliseconds*

no isdn bcac service timer *milliseconds*

Syntax Description

milliseconds	Length, in milliseconds (ms), of the T3M1 or T323 service message timer. Valid range is from 500 to 120000 ms; default is 120000 ms.

Command Default

The T3M1 or T323 service message timer defaults to 120000 ms.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The T3M1 or T323 service message timer is started when a SERV message is sent to the far side.

Examples

The following example shows how to change the service timers to 600 ms on serial interface 2:23:

```
interface serial 2:23
 isdn bcac service timer 600
```

Related Commands

Command	Description
isdn bcac service audit	Enables service audits on an interface configured for BCAC.
isdn bcac service audit interface	Specifies that the BCAC service audit needs to be triggered on the entire interface.
isdn bcac service audit trigger	Enables individual BCAC service triggers.
isdn bcac service retry in-serv-on-fail	Specifies that the BCAC service state of the channel needs to be changed to In Service because no acknowledgment was received.
isdn bcac service retry max	Specifies the maximum number of times a BCAC service message can be retransmitted when unacknowledged.
isdn bcac service update linkup	Triggers updates of the BCAC service states between peer nodes through exchange of SERV and SERV ACK messages.

Command	Description
isdn bcac service update provision	Enables the functionality of service status for provisioning ISDN PRI B channels.
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 bcac service update linkup

To trigger updates of the B-Channel Availability Control (BCAC) service states between peer nodes through exchange of SERV and SERV ACK messages, use the **isdn bcac service update linkup** command in interface configuration mode. To disable triggering of updates, use the **no** form of this command.

isdn bcac service update linkup

no isdn bcac service update linkup

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

This command updates the service states of *all* the channels to the far side of the interface by exchanging SERV and SERV ACK messages whenever ISDN Layer 2 comes up.

Use the **isdn bcac service update linkup** command to bring the service state of the channels on the interface in synchronization with its peer through the exchange of SERV messages. This synchronizing of the service states will be triggered whenever ISDN Layer 2 comes up. This command can be used with the **isdn service** command in cases where the service state of the channels needs to be synchronized when the ISDN Layer 2 comes up, and in particular, when the ISDN Layer 2 comes up after the router has reloaded.

Examples

The following example shows how to trigger service state updates on serial interface 2:23:

```
interface serial 2:23
 isdn bcac service update linkup
```

Related Commands

Command	Description
isdn bcac service audit	Enables service audits on an interface configured for BCAC.
isdn bcac service audit interface	Specifies that the BCAC service audit needs to be triggered on the entire interface.
isdn bcac service audit trigger	Enables individual BCAC service triggers.

Command	Description
isdn bcac service retry in-serv-on-fail	Specifies that the BCAC service state of the channel needs to be changed to In Service because no acknowledgment was received.
isdn bcac service retry max	Specifies the maximum number of times a BCAC service message can be retransmitted when unacknowledged.
isdn bcac service timer	Changes the value of the BCAC T3M1 or T323 service message timer.
isdn bcac service update provision	Enables the functionality of service status for provisioning ISDN PRI B channels.
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 bcac service update provision

To enable functionality of service status for provisioning the ISDN B channels, use the **isdn bcac service update provision** command in interface configuration mode. To disable provisioning, use the **no** form of this command.

isdn bcac service update provision

no isdn bcac service update provision

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

This command enables functionality of service status for provisioning the B channels, which for the Cisco implementation happens only on reboot.

Examples

The following example shows how to enable the service service status for provisioning the B channels on serial interface 2:23:

```
interface serial 2:23
 isdn bcac service update provision
```

Related Commands

Command	Description
isdn bcac service audit	Enables service audits on an interface configured for BCAC.
isdn bcac service audit interface	Specifies that the BCAC service audit needs to be triggered on the entire interface.
isdn bcac service audit trigger	Enables individual BCAC service triggers.
isdn bcac service retry in-serv-on-fail	Specifies that the BCAC service state of the channel needs to be changed to In Service because no acknowledgment was received.
isdn bcac service retry max	Specifies the maximum number of times a BCAC service message can be retransmitted when unacknowledged.
isdn bcac service timer	Changes the value of the BCAC T3M1 or T323 service message timer.

Command	Description
isdn bcac service update linkup	Triggers updates of the BCAC service states between peer nodes through exchange of SERV and SERV ACK messages.
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 bchan-number-order

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

isdn bchan-number-order {**ascending** | **descending**} [**round-robin**]

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
round-robin	(Optional) Enables a round-robin B-channel selection scheme.

Command Default

Selection default is ascending for the network side; descending for the user side.

Command Modes

Interface configuration

Command History

Release	Modification
11.3T	This command was introduced.
12.3(1)	The **round-robin** keyword was added.

Usage Guidelines

This command supports ascending, descending, and round-robin B-channel selection schemes. This command is for PRI configuration only.

This command supports ascending and descending B-channel selection by instructing 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 B31 for an E1 (descending).

In the ascending B-channel selection scheme, for example, if the channel selected for the last call was channel 14, then if channel *x*, where *x* is any channel number less than or equal to 14, becomes available by the time a channel is selected for the next call, that channel will be selected for the call.

In the round-robin B-channel selection scheme, the next channel selected is the current channel number *x* plus 1 for ascending, or current channel number *x* minus 1 for descending configuration.

When the channel selection software routine reaches channel 1 (the bottom for descending) or channel 23 for T1 and channel 31 for E1 (the top for ascending), the software routine wraps around. An example for a descending configuration: After reaching channel 1, the routine goes back to channel 31 or 23 and then decrements the count from there.

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 serial 5:10
 isdn bchan-number-order ascending
```

The following example configures the outgoing B-channel order on a PRI interface to be round-robin in ascending order.

```
interface serial 4:23
 isdn bchan-number-order ascending round-robin
```

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.

Command Default

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.