encapsulation cpp

To enable encapsulation for communication with routers or bridges using the Combinet Proprietary Protocol (CPP), use the **encapsulation cpp** command in interface configuration mode. To disable CPP encapsulation, use the **no** form of this command.

encapsulation cpp

no encapsulation cpp

Syntax Description

This command has no arguments or keywords.

Defaults

CPP encapsulation disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to communicate over an ISDN interface with Cisco 700 and 800 series (formerly Combinet) routers that do not support PPP but do support CPP.

Most Cisco routers *do* support PPP. Cisco routers can communicate over ISDN with these devices by using PPP encapsulation, which supports both routing and fast switching.

The Cisco 700 and 800 series routers support only IP, IPX, and bridging. For AppleTalk, these Cisco routers automatically perform half-bridging.

This command is supported on ISDN BRIs and PRIs only.

Examples

The following example configures BRI interface 0 to communicate with a router or bridge that does not support PPP:

```
interface bri 0
 encapsulation cpp
 cpp callback accept
 cpp authentication
```

The following example configures PRI serial interface 1/1:23 to communicate with a router or bridge that does not support PPP:

```
controller t1 1/1
 framing esf
 linecode b8zs
 pri-group timeslots 1-23
 isdn switchtype primary-4ess
!
```

```
interface Serial1/1:23
 encapsulation cpp
 cpp callback accept
 cpp authentication
```

Related Commands

Command	Description
cpp authentication	Enables negotiation of authentication with a router or bridge that supports the CPP and that is calling in to this router.
cpp callback accept	Enables the router to accept callback from a router or bridge that supports the CPP.

encryption mppe

To enable Microsoft Point-to-Point Encryption (MPPE) on an Industry-Standard Architecture (ISA) card, use the **encryption mppe** command in controller configuration mode. To disable MPPE, use the **no** form of this command.

encryption mppe

no encryption mppe

Syntax Description

This command has no arguments or keywords.

Command Default

IPSec is the default encryption type.

Command Modes

Controller configuration

Command History

Release	Modification
12.0(5)XE5	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

Using the ISA card offloads MPPE from the Route Processor and will improve performance in large-scale environments.

The router must be rebooted for the change to the **encryption mppe** command configuration to take effect.

Examples

The following example enables MPPE encryption on the ISA card in slot 5, port 0:

```
Router(config)# controller isa 5/0
Router(config-controller)# encryption mppe
```

Related Commands

Command	Description
debug ppp mppe	Displays debug messages for MPPE events.
encryption mppe	Enables MPPE encryption on the virtual template.
show ppp mppe	Displays MPPE information for an interface.

firmware location

To download firmware into the modems, use the **firmware location** command in Service Processing Element (SPE) configuration mode. Use the **no** form of this command to revert the router back to the system embedded image default.

firmware location {**system** | **flash**}**:** *filename*

no firmware location {**system** | **flash**}**:** *filename*

Syntax Description

system	Router loads the firmware from a built-in file within the Cisco IOS image.
flash	Router loads the firmware from the Flash NVRAM located within the router.
:filename	The name of the desired firmware file preceded by a colon. If **system** is specified, enter the path to the filename you want to download.

Defaults

No default behavior or values.

Command Modes

SPE configuration

Command History

Release	Modification
12.0(4)XI1	This command was introduced on the Cisco AS5200, Cisco 5300, and Cisco AS5800.
12.0(6)T	This command was integrated into Cisco IOS Release 12.0(6)T.
12.0(7)T	This command was implemented on the Cisco AS5300 and Cisco AS5800 for MICA modems.
12.1(1)XD	This command was implemented on the Cisco AS5400 for the NextPort dial feature card (DFC).
12.1(3)T	This command was implemented on the Cisco AS5400 for the NextPort DFC and on the Cisco AS5800 for the universal port card (UPC).

Usage Guidelines

Use the **firmware location** SPE configuration command to download firmware into your modems. When the access server is booted, the **firmware location** command displays the location for the firmware that is embedded in the Cisco IOS image. If the **firmware location** command was given to download a firmware image from Flash memory and then the **no** version of the exact command is subsequently given, then the **firmware location** command will download the embedded firmware in Cisco IOS software.

You must first copy the SPE image from a TFTP server to the Flash memory using the **copy tftp flash** command. This command specifies the location of the firmware file and downloads the firmware in the range of SPEs. Your range is specified depending on the states you configured using the **firmware upgrade** command.

The **firmware location** command was first supported in Cisco IOS Release 12.0(4)XI1. For earlier images, use the **copy** command. For Cisco IOS Release 12.0(4)XI1 images, the **copy flash modem** command is disabled for MICA technologies modems and newer versions of the 56-kbps Microcom modems. The older V.34 Microcom modems still use the **copy** command for downloading in Cisco IOS Release 12.0(4)XI1 images.

You cannot use the **firmware location** command on SPE that are in Bad state.

Note This command should be used when traffic is low because the **firmware location** download will not begin until the modems have no active calls. Otherwise, use the **firmware upgrade** command to customize the scheduling of modem downloads for your needs.

The **firmware location** command is a configuration command—if you do not save it using the **write memory** command, then the configuration will not be saved; hence, the downloading of the specified firmware will not occur after the next reboot.

Examples

The following configuration example sets the SPEs, specifies the firmware file location, opens the file (if on Flash memory), and downloads to the SPE on the Cisco AS5400:

```
Router(config)# spe 1/03
Router(config-spe)# firmware location flash
Router(config-spe)# end
```

The following example sets the SPEs, specifies the firmware file location in Flash memory, downloads to the SPE, and reports on the status using the **show spe version** command on the Cisco AS5800:

```
Router(config)# spe 1/03
Router(config-spe)# firmware location flash:np_6_75
Started downloading firmware flash:np_6_75.spe
Router(config-spe)#

Router# show spe version 1/03
.
.
.
SPE          SPE     SPE  SPE   Port          Call
SPE#    Port #       State        Busyout Shut Crash State        Type
1/03/00 0000-0011    ACTIVE             0    0     0 _____________ _____________
1/03/01 0012-0023    ACTIVE             0    0     0 _____________ _____________
1/03/02 0024-0035    ACTIVE             0    0     0 _____________ _____________
1/03/03 0036-0047    ACTIVE             0    0     0 _____________ _____________
1/03/04 0048-0059    ACTIVE             0    0     0 _____________ _____________
1/03/05 0060-0071    ACTIVE             0    0     0 _____________ _____________
1/03/06 0072-0083    ACTIVE             0    0     0 _____________ _____________
1/03/07 0084-0095    ACTIVE             0    0     0 _____________ _____________
1/03/08 0096-0107    ACTIVE             0    0     0 _____________ _____________
1/03/09 0108-0119    ACTIVE             0    0     0 _____________ _____________
1/03/10 0120-0131    ACTIVE             0    0     0 _____________ _____________
1/03/11 0132-0143    ACTIVE             0    0     0 _____________ _____________...
```

The following display shows downloads of firmware that was not bundled with the Cisco IOS image:

```
spe 1/2 1/4
 firmware location flash:portware.2620.ios
spe 2/2 2/8
 firmware location flash:mcom-fw-dsp.5.1.9_47.22.bin
spe 2/12 2/23
 firmware location feature_card_flash
```

The following display shows downloads of firmware that was bundled with the Cisco IOS image:

```
spe 2/9 2/9
 firmware location system:/ucode/microcom_firmware
spe 1/5 1/7
 firmware location system:/ucode/mica_port_firmware
```

Related Commands

Command	Description
clear port	Resets the NextPort port and clears any active call.
clear spe	Reboots all specified SPEs.
copy tftp flash	Copies the SPE image from a TFTP server to the Flash memory.
firmware upgrade	Specifies the method in which the SPE will be downloaded.
show spe version	Displays the firmware version on an SPE.
spe download maintenance	Performs download maintenance on SPEs that are marked for recovery.
spe recovery	Sets an SPE port for recovery.

firmware upgrade

To modify the way in which the Service Processing Element (SPE) will be downloaded, use the **firmware upgrade** command in SPE configuration mode. To revert to the default SPE firmware upgrade option, busyout, use the **no** form of this command.

firmware upgrade {**busyout** | **recovery** | **reboot**}

no firmware upgrade

Syntax Description

busyout	Upgrades when all calls are terminated on the SPE.
recovery	Upgrades during download maintenance time.
reboot	Upgrades at the next reboot.

Defaults

An upgrade occurs when all calls are terminated on the SPE (**busyout**).

Command Modes

SPE configuration

Command History

Release	Modification
12.0(4)XI1	This command was introduced on the Cisco AS5200, Cisco 5300, and Cisco AS5800.
12.0(6)T	This command was integrated into Cisco IOS Release 12.0(6)T.
12.0(7)T	This command was introduced on the Cisco AS5300 and Cisco AS5800 for MICA technologies modems.
12.1(1)XD	This command was implemented on the Cisco AS5400 for the NextPort dial feature card (DFC).
12.1(3)T	This command was implemented on the Cisco AS5400 for NextPort DFC and Cisco AS5800 for universal port card (UPC).

Usage Guidelines

Three methods of upgrade are available: busyout, reboot, and download-maintenance.

The **reboot** keyword requests the Cisco access servers to upgrade SPE firmware at the next reboot. The **busyout** keyword upgrades SPE firmware after waiting for all calls to be terminated on an SPE and is the default. The **download-maintenance** keyword requests SPE firmware download during maintenance time.

Use this command in conjunction with the **firmware location** command and the **spe download maintenance** command.

The SPE **firmware location** command is designed to integrate all continuous ranges of SPEs containing the same firmware location. However, the **firmware upgrade** command does not affect the ranges of SPEs. As such, all SPEs within the ranges of SPEs must have the same firmware upgrade mode or the router uses the default upgrade mode to busyout state. If you want to upgrade a single SPE within an existing range of SPEs with a different upgrade mode than is currently configured, you must first change

the upgrade mode for the entire range of SPEs and then change the firmware location for the specific SPE being upgraded. Furthermore, each time you merge ranges of SPEs due to configuration changes, verify that the configuration of the SPE firmware upgrade remains effective to what is desired.

Examples

The following example sets the SPEs and specifies the firmware upgrade to take place once all calls are terminated on the SPE:

```
Router(config)# spe 1/03
Router(config-spe)# firmware location
Router(config-spe)# firmware upgrade busyout
Router(config-spe)#
```

If the **busyout upgrade** command is specified, or if no upgrade mode is specified, the SPE modems are set into a "pending download" state when you use the **firmware location** command on the specified SPE. The pending download state prevents any modem in that state to be allocated for new calls until the state is cleared. Modems with active calls remain active for their call durations, but enter the pending download state when they terminate. This pending download state can be cleared only when the SPE is finally downloaded. When all modems within the SPE are in the pending download state and no active calls remain on the SPE, the SPE is reloaded. The **busyout** option is the fastest way to upgrade modems on an active router but can severely impact the capacity of the router during the upgrade. The following example sets the default option for the firmware upgrade process:

```
Router(config-spe)# firmware upgrade busyout
```

If reboot upgrade is specified, the SPE modems are not reloaded to the new firmware location until the router is rebooted. The reboot upgrade option is useful for routers that need their SPE upgraded and also will be rebooted for maintenance. When the new firmware is configured, the configuration takes effect after the reboot takes place. The following example sets the firmware upgrade reboot:

```
Router(config-spe)# firmware upgrade reboot
```

If recovery upgrade is specified, the SPE modems are reloaded based on the modem recovery algorithm. Only when no active calls exist on the SPE does the firmware download take place. Furthermore, at the configured modem recovery maintenance time, the modem recovery maintenance process attempts, in controller fashion, to reload the modems by busying out the modems for a preset window of time to make the download take place. Consult the modem recovery documentation for further details. The recovery upgrade option is the way to upgrade modems on an active router with the least impact. Capacity is kept at a maximum. However, reloading to the new firmware location may take a few days. The following example sets the system for a firmware upgrade recovery:

```
Router(config-spe)# firmware upgrade recovery
```

Related Commands

Command	Description
firmware location	Downloads firmware into the modems from this file location.
modem recovery maintenance	Specifies the scheduled modem maintenance recovery behavior.
show spe version	Displays the firmware version on an SPE.
spe download maintenance	Performs download maintenance on SPEs that are marked for recovery.
spe recovery	Sets an SPE port for recovery.

flowcontrol

To set the method of data flow control between the terminal or other serial device and the router, use the **flowcontrol** command in line configuration mode. To disable flow control, use the **no** form of this command.

flowcontrol {**none** | **software** [**lock**] [**in** | **out**] | **hardware** [**in** | **out**]}

no flowcontrol {**none** | **software** [**lock**] [**in** | **out**] | **hardware** [**in** | **out**]}

Syntax Description

none	Turns off flow control.
software ... [**in**	**out**]	Sets software flow control. An optional keyword specifies the direction: **in** causes the Cisco IOS software to listen to flow control from the attached device, and **out** causes the software to send flow control information to the attached device. If you do not specify a direction, both directions are assumed.
lock	(Optional) Makes it impossible to turn off flow control from the remote host when the connected device *needs* software flow control. This option applies to connections using the Telnet or rlogin protocols.
hardware [**in**	**out**]	Sets hardware flow control. An optional keyword specifies the direction: **in** causes the software to listen to flow control from the attached device, and **out** causes the software to send flow control information to the attached device. If you do not specify a direction, both directions are assumed. For more information about hardware flow control, see the hardware manual that was shipped with your router.

Defaults

Flow control is disabled.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When software flow control is set, the default stop and start characters are Ctrl-S and Ctrl-Q (XOFF and XON). You can change them with the **stop-character** and **start-character** commands.

If a remote Telnet device requires software flow control, the remote system should not be able to turn it off. Using the **lock** option makes it possible to refuse “dangerous” Telnet negotiations if they are inappropriate.

Examples

The following example sets hardware flow control on line 7:

```
line 7
 flowcontrol hardware
```

Related Commands

Command	Description
source template	Sets the flow control start character.
stop-character	Sets the flow control stop character.

force-local-chap

To force the L2TP network server (LNS) to reauthenticate the client, use the **force-local-chap** command in VPDN group configuration mode. To disable reauthentication, use the **no** form of this command.

force-local-chap

no force-local-chap

Syntax Description

This command has no arguments or keywords.

Defaults

Proxy authentication. The Challenge Handshake Authentication Protocol (CHAP) response to the Layer 2 Transport Protocol access concentrator (LAC) authentication challenge is passed to the LNS.

Command Modes

VPDN group configuration

Command History

Release	Modification
11.3(5)AA	This command was introduced.
12.0(1)T	This command was integrated into Cisco IOS Release 12.0(1)T.
12.0(5)T	This command was modified to be available only if the accept-dialin VPDN group configuration mode is enabled.

Usage Guidelines

You must enable the **accept-dialin** command on the VPDN group before you can use the **force-local-chap** command. Removing the **accept-dialin** command will remove the **force-local-chap** command from the VPDN group.

This command is used only if CHAP authentication is enabled for PPP (using the **ppp authentication chap** command). This command forces the LNS to reauthenticate the client in addition to the proxy authentication that occurs at the LAC. If the **force-local-chap** command is used, then the authentication challenge occurs twice. The first challenge comes from the LAC and the second challenge comes from the LNS. Some PPP clients may experience problems with double authentication. If this problem occurs, authentication challenge failures may be seen if the **debug ppp authentication** command is enabled.

Examples

The following example enables CHAP authentication at the LNS:

```
vpdn-group 1
 accept dialin
  protocol l2tp
  virtual-template 1
 terminate-from pat
 force-local-chap
```

Related Commands

Command	Description
accept-dialin	Configures an LNS to accept tunneled PPP connections from a LAC and create an accept dial-in VPDN subgroup.
lcp renegotiation	Allows the LNS to renegotiate the LCP on dial-in calls, using L2TP or L2F.

framing

To select the frame type for the T1 or E1 data line, use the **framing** command in controller configuration mode. To turn off framing, use the **no** form of this command.

T1 Line

framing {**sf** | **esf**}

no framing

E1 Line

framing {**crc4** | **no-crc4**} [**australia**]

no framing

Syntax Description

sf	Super Frame as the T1 frame type.
esf	Extended Superframe as the T1 frame type.
crc4	CRC4 frame as the E1 frame type.
no-crc4	No CRC4 frame as the E1 frame type.
australia	(Optional) E1 frame type used in Australia.

Defaults

Super Frame is the default on a T1 line.

CRC4 frame is the default on an E1 line.

Command Modes

Controller configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use this command in configurations where the router or access server is intended to communicate with a T1 or E1 fractional data line. The service provider determines which framing type (the **sf**, **esf**, or **crc4** keyword) is required for your T1 or E1 circuit.

Examples

The following example selects Extended Superframe as the T1 frame type:

```
framing esf
```

Related Commands

Command	Description
channel-group	Defines the time slots that belong to each T1 or E1 circuit.
linecode	Selects the line code type for T1 or E1 line.

group-range

To create a list of member asynchronous interfaces (associated with a group interface), use the **group-range** command in interface configuration mode. To remove an interface from the member list, use the **no** form of this command.

group-range *low-end-of-interfacerange high-end-of-interfacerange*

no group-range *interface*

Syntax Description

low-end-of-interfacerange	Beginning interface number to be made a member of the group interface.
high-end-of-interfacerange	Ending interface number to be made a member of the group interface.
interface	Interface number to be removed from the group interface.

Defaults

No interfaces are designated as members of a group.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Using the **group-range** command, you create a group of asynchronous interfaces that are associated with a group asynchronous interface on the same device. This group interface is configured by using the **interface group-async** command. This one-to-many structure allows you to configure all associated member interfaces by entering one command on the group interface, rather than entering this command on each interface. You can customize the configuration on a specific interface by using the **member** command. Interface numbers can be removed from the interface group using the **no group-range** command.

Examples

The following example defines interfaces 2, 3, 4, 5, 6, and 7 as members of asynchronous group interface 0:

```
interface group-async 0
 group-range 2 7
```

Related Commands

Command	Description
interface group-async	Creates a group interface that will serve as master, to which asynchronous interfaces can be associated as members.
member	Alters the configuration of an asynchronous interface that is a member of a group.

hw-module slot

To enable the router shelf to stop a Dial Shelf Controller (DSC) card, to restart a stopped DSC card, or to cause a reload of any specified dial shelf feature board, use the **hw-module slot** command in privileged EXEC mode.

hw-module slot *shelf-id/slot-number* {**start** | **stop** | **reload**}

Syntax Description

shelf-id/	Dial shelf number. The default shelf ID for the dial shelf is 1. You must type in the forward slash (/) as part of the command.
slot-number	Number of the slot in the shelf where the target feature board or DSC is installed. If the **start** or **stop** keyword is used, the slot number must be either 12 or 13, because these keywords apply only to DSCs.
start	Restarts the specified DSC.
stop	Stops the specified DSC.
reload	Enables a remote reload of an individual feature board without having to use manual online insertion and removal (OIR).

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(6)AA	The **hw-module** command was introduced.
12.1	The **hw-module** command was expanded to become the **hw-module slot** command, and the **reload** keyword was introduced to enable a remote feature board reload.

Usage Guidelines

The **stop** form of this command is issued from the router shelf console instead of through pressing of the attention (ATTN) button on the target DSC. Confirmation of when the start or stop took place is displayed. Warnings are issued and confirmation input is required if a **stop** command will result in a loss of service when backup functionality is not available.

When a DSC card is stopped, removed, then reinstalled, there is no need to restart the card (whether the card is the original or a replacement) because a freshly installed card reboots as the backup DSC automatically. However, if a DSC is stopped, either by using the ATTN button or by issuing the **hw-module slot stop** command, it must be restarted by using the **start** version of the same command, or the DSC must be removed and reinstalled in order to reboot.

Press the ATTN button on the DSCs to shut down a card manually prior to removing the card. This is equivalent to issuing a **hw-module** privileged EXEC command for that card at the router command prompt. Use the ATTN button to shut down the card before it is swapped out or tested in place, or to restart it, if the card has not been removed after having been shut down.

Tips The **hw-module slot** *shelf-id/slot-number* **reload** form of this command is useful for simulating an OIR event in the case of a feature board failure when physical access to the feature board card is restricted.

Entering the **hw-module slot** *shelf-id/slot-number* **reload** command initiates the feature board reload process through power cycling. The **hw-module slot** *shelf-id/slot-number* **reload** command cannot be used to reload DSCs.

Examples

The following example stops one DSC in slot 13 and starts another in slot 12 (which has previously been stopped):

```
hw-module slot 1/13 stop
hw-module slot 1/12 start
```

The following example shows a reload of the feature board in slot 7. To verify that you have reloaded the DSC, use the **show dial-shelf** command.

```
Router# hw-module slot 1/7 reload

All calls will be dropped on shelf 1 slot 7, proceed with reload ? [confirm]n

 Router# show dial-shelf

 Slot    Board     CPU       DRAM          I/O Memory   State         Elapsed
          Type     Util    Total (free)   Total (free)                Time
  0        CT1    0%/0%  21535360( 82%)  8388608( 47%)  Up            00:09:27
  1        CT1    0%/0%  21535360( 82%)  8388608( 47%)  Up            00:09:28
  4 Modem(HMM)  19%/19%   6855296( 34%)  6291456( 33%)  Up            00:09:27
  7 Modem(DMM)  40%/40%  46701184( 88%) 16777216( 74%)  Up            00:09:25
 12        DSC    0%/0%  18998144( 83%)  8388608( 66%)  Up            00:10:40
 13        DSC    2%/0%  18998144( 83%)  8388608( 66%)  Up            00:10:35
 Dial shelf set for auto boot

Router# hw-module slot 1/7 reload

All calls will be dropped on shelf 1 slot 7, proceed with reload ? [confirm]y
 Router#
 00:11:17: %DIALSHELF-6-RELOAD: Reload requested for card in shelf 1 slot 7.
 00:11:17: %DSIPPF-5-DS_KEEPALIVE_LOSS: DSIP Keepalive Loss from shelf 1 slot 7
 00:11:38: %DIALSHELF-2-TIMEOUT: Resetting slot 7 after 30 secs in state 'Unknown
 '
Router# show dial-shelf

 Slot    Board     CPU       DRAM          I/O Memory   State         Elapsed
          Type     Util    Total (free)   Total (free)                Time
  0        CT1    0%/0%  21535360( 82%)  8388608( 47%)  Up            00:10:06
  1        CT1    0%/0%  21535360( 82%)  8388608( 47%)  Up            00:10:07
  4 Modem(HMM)    0%/0%   6855296( 34%)  6291456( 33%)  Resetting     00:00:09
  7 Modem(DMM)    0%/0%  46701184( 88%) 16777216( 74%)  Up            00:10:03
 12        DSC    0%/0%  18998144( 83%)  8388608( 66%)  Up            00:11:18
 13        DSC    2%/0%  18998144( 83%)  8388608( 66%)  Up            00:11:14
 Dial shelf set for auto boot
 Router#
 00:17:10: %DIALSHELF-2-TIMEOUT: Resetting slot 7 after 30 secs in state 'Unknown
 '
 00:18:07: %DSIPPF-5-DS_HELLO: DSIP Hello from shelf 1 slot 7 Succeeded
```

```
Router# show dial-shelf

Slot    Board     CPU       DRAM          I/O Memory   State         Elapsed
          Type     Util    Total (free)   Total (free)                Time
  0        CT1    0%/0%  21535360( 82%)  8388608( 47%)  Up           00:17:21
  1        CT1    0%/0%  21535360( 82%)  8388608( 47%)  Up           00:17:23
  4 Modem(HMM)  20%/20%   6855296( 34%)  6291456( 33%)  Up           00:00:56
  7 Modem(DMM)  20%/20%  46701184( 88%) 16777216( 74%)  Up           00:17:19
 12        DSC    0%/0%  18998144( 83%)  8388608( 66%)  Up           00:18:34
 13        DSC    3%/0%  18998144( 83%)  8388608( 66%)  Up           00:18:29
 Dial shelf set for auto boot
```

Related Commands

Command	Description
debug redundancy	Displays information used for troubleshooting dual (redundant) DSC cards.
show redundancy	Displays current or historical status and related information on a redundant DSC.

initiate-to

To specify the IP address that will be tunneled to, use the **initiate-to** command in VPDN group configuration mode. To remove an IP address from the VPDN group, use the **no** form of this command.

initiate-to ip *ip-address*

no initiate-to [**ip** *ip-address*]

Syntax Description

ip *ip-address*	IP address of the router that will be tunneled to.

Defaults

N address is specified.

Command Modes

VPDN group configuration

Command History

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

Usage Guidelines

Before you can use this command, you must enable one of the two request VPDN subgroups by using either the **request dialin** or **request dialout** command.

A Layer 2 Transport Protocol access concentrator (LAC) configured to request dial-in can be configured with multiple **initiate-to** commands to tunnel to more than one IP address.

An L2TP network server (LNS) configured to request dial-out can be configured only with a single **initiate-to** command. If you enter a second **initiate-to** command, it will replace the original **initiate-to** command.

Examples

The following example configures VPDN group 1 to request a Layer 2 Transport Protocol (L2TP) tunnel to the peer at IP address 10.3.2.1 for tunneling dial-out calls from dialer pool 1.

```
vpdn-group 1
 request-dialout
  protocol l2tp
  pool-member 1
 initiate-to ip 10.3.2.1
```

Related Commands

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

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 Only

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.

Defaults

The default mode for subinterfaces is multipoint.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.2 F	This command was enhanced with the capability to carry X.25 traffic on the D channel.
11.2 P	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 bri0
 isdn x25 dchannel
 isdn x25 static-tei 8
!
interface bri0:0
 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.

Defaults

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 multilink interface configuration mode to configure the bundle, use the **interface multilink** command in 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 (a nonzero number).

Defaults

No interfaces are configured.

Command Modes

Global configuration

Command History

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

Examples

The following example creates multilink bundle 1:

```
interface multilink 1
 ip address 192.168.11.4 255.255.255.192
 encapsulation ppp
 ppp multilink
 keepalive
```

Related Commands

Command	Description
ppp multilink fragment disable	Disables packet fragmentation.
ppp multilink group	Restricts a physical link to 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 signalling or robbed-bit signalling, 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.

Defaults

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-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.

interface virtual-template *number*

Syntax Description

number	Number used to identify the virtual template interface. Up to 200 virtual template interfaces can be configured.

Defaults

No virtual template number is defined.

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	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.

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.

Once 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 (VPDN), PPP over ATM, protocol translation, and Multichassis Multilink PPP (MMP).

Examples

The following example creates and configures virtual template interface 1:

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

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.

Defaults

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-proxy-client** | **local**}

no ip address-pool

Syntax Description

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.

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.

Examples

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.

Defaults

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.

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-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.

Defaults

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.

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 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 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 (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 {*named-address-pool* | **default**} {*first-IP-address* [*last-IP-address*]} [**group** *group-name*] [**cache-size** *size*]}

no ip local pool *named-address-pool first-IP-address* [*last-IP-address*]

no ip local pool {*named-address-pool* | **default**}

Syntax Description

named-address-pool	Creates named local IP address pool.
default	Creates default local IP address pool that is used if no other pool is named.
first-IP-address [*last-IP-address*]	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 bottom of the free list. Before assigning a new IP address to a user, the system checks the number of entries from the bottom of the list (as defined by the **cache-size** *size* option) to determine 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.

Defaults

No address pools are configured.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
11.3 AA	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.

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.

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/forwarding instance (VRF).

The IP address pools can also be used with the **translate** commands for one-step vty-async connections and in certain AAA/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 "quark," which contains all IP addresses in the range 172.16.23.0 to 172.16.23.255:

```
ip local pool quark 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.

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.
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.

ip mtu adjust

To enable automatic adjustment of the IP maximum transmission unit (MTU) on a virtual access interface, use the **ip mtu adjust** command in VPDN group configuration mode. To disable automatic adjustment of the IP MTU, use the **no** form of this command.

ip mtu adjust

no ip mtu adjust

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco IOS Release 12.2(3) and 12.2(4)T

Automatic adjustment of the IP MTU is enabled.

Cisco IOS Release 12.2(6) and 12.2(8)T and Later Releases

Automatic adjustment of the IP MTU is disabled.

Command Modes

VPDN group configuration

Command History

Release	Modification
12.2(3)	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(6)	The default setting for this command was changed from enabled to disabled.
12.2(8)T	The default setting for this command was changed from enabled to disabled.

Usage Guidelines

Enabling the **ip mtu adjust** command allows the router to automatically adjust the IP MTU on the virtual access interface associated with the specified virtual private dialup network (VPDN) group. The IP MTU is automatically adjusted to compensate for the size of the Layer 2 header and the MTU of the egress interface.

The IP MTU is adjusted automatically only if there is no IP MTU manually configured on the virtual template interface from which the virtual access interface is cloned. To manually configure an IP MTU on the virtual template interface, use the **ip mtu** command in interface configuration mode.

Examples

The following example enables automatic adjustment of the IP MTU for sessions associated with the VPDN group named cisco1:

```
vpdn-group cisco1
 ip mtu adjust
```

Related Commands

Command	Description
ip mtu	Sets the MTU size of IP packets sent on an interface.
ip pmtu	Allows L2TP VPDN tunnels to participate in path MTU discovery.

ip precedence (VPDN)

To set the precedence value (and an optional IP number or IP name) in the virtual private dialup network (VPDN) Layer 2 encapsulation header, use the **ip precedence** command in VPDN group configuration mode. To copy the IP precedence value of the payload to the Layer 2 encapsulation header, use the **no** form of this command.

ip precedence [*number* | *name*]

no ip precedence [*number* | *name*]

Syntax Description

number | *name*	(Optional) A number or name that sets the precedence bits in the IP header. The values for the *number* argument and the corresponding *name* argument are listed in Table 10, from least to most important.

Command Default

The IP precedence value of the payload is copied to the Layer 2 encapsulation header.

Command Modes

VPDN group configuration

Command History

Release	Modification
12.1(1.1)	This command was introduced.
12.1(1.1)T	This command was integrated into Cisco IOS Release 12.1(1.1)T

Usage Guidelines

Table 10 lists the values for the *number* argument and the corresponding *name* argument for precedence values in the IP header. They are listed from least to most important.

Table 10 Number and Name Values for IP Precedence

Number	Name
0	**routine**
1	**priority**
2	**immediate**
3	**flash**
4	**flash-override**
5	**critical**
6	**internet**
7	**network**

You can set the precedence using either a number or the corresponding name. Once the IP Precedence bits are set, other quality of service (QoS) services such as weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) then operate on the bit settings.

For further information on QoS services, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Examples

The following example sets the IP Precedence to 5 (critical) for packets that traverse the VPDN tunnel associated with VPDN group 1:

```
vpdn-group 1
 ip precedence 5
```

Related Commands

Command	Description
ip tos	Sets the ToS bits in the VPDN Layer 2 encapsulation header.
vpdn-group	Creates a VPDN group and to enters VPDN group configuration mode.

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.

Defaults

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.

Defaults

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

Command Modes

Interface configuration

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.

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:

```
ip rtp reserve 32768 20 1000
```

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.

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.

Defaults

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.

Defaults

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.

Defaults

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.

Defaults

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 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.

Defaults

The default ToS value for Telnet packets is 0xC0.

Command Modes

Global configuration

Command History

Release	Modification
11.2(10)P	This command was introduced.
11.3(1)	Support for this command was added to Cisco IOS Release 11.3(1).

Usage Guidelines

Compatibility with some 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 0x0 in the IP header:

```
ip telnet tos 0
```

Related Commands

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

ip tos (VPDN)

To set the type of service (ToS) bits in the virtual private dialup network (VPDN) Layer 2 encapsulation header, use the **ip tos** command in VPDN group or VPDN template configuration mode. To restore the default setting, use the **no** form of this command.

ip tos {*tos-bit-value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal** | **reflect**}

no set ip tos {*tos-bit-value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal** | **reflect**}

Syntax Description

tos-bit-value	A value (number) from 0 to 15 that sets the ToS bits in the IP header. See Table 11 for more information.
max-reliability	Sets the maximum reliability ToS bits to 2.
max-throughput	Sets the maximum throughput ToS bits to 4.
min-delay	Sets the minimum delay ToS bits to 8.
min-monetary-cost	Sets the minimum monetary cost ToS bits to 1.
normal	Sets the normal ToS bits to 0. This is the default setting.
reflect	Copies the ToS value from the inner IP packet to the Layer 2 encapsulation header.

Command Default

The ToS bits are set to 0, which is equivalent to the **normal** keyword.

Command Modes

VPDN group configuration
VPDN template configuration

Command History

Release	Modification
12.0(5)T	This command was introduced as **l2tp ip tos reflect**.
12.1(1.1)	The **l2tp ip tos reflect** command was replaced by the **ip tos** command, configuration options were added, and support was added for other protocols.
12.1(1.1)T	This command was integrated into Cisco IOS Release 12.1(1.1)T

Usage Guidelines

The **ip tos** command allows you to set four bits in the ToS portion of the Layer 2 encapsulation header. The ToS bits can be set manually, or copied from the header of the inner IP packet by issuing the **reflect** keyword.

The ToS bits of the inner IP header can be set manually using the **set ip tos** (route-map) command. If you then configure the **ip tos reflect** command, the manually configured ToS setting of the inner IP header will be copied to the encapsulation header.

The **reflect** keyword functions only when the inner payload is IP. The encapsulated payload of Multilink PPP (MLP) connections is not IP, therefore the **reflect** keyword has no effect when MLP is tunneled.

Table 11 shows the format of the four ToS bits in binary form.

Table 11 ToS Bits and Description

T3	T2	T1	T0	Description
0	0	0	0	0 normal forwarding
0	0	0	1	1 minimum monetary cost
0	0	1	0	2 maximum reliability
0	1	0	0	4 maximum throughput
1	0	0	0	8 minimum delay

The T3 bit sets the delay. Setting T3 to 0 equals normal delay, and setting it to 1 equals low delay.

The T2 bit sets the throughput. Setting this bit to 0 equals normal throughput, and setting it to 1 equals maximum throughput. Similarly, the T1 and T0 bits set reliability and monetary cost, respectively. Therefore, as an example, if you want to set a packet with the following requirements:

minimum delay T3 = 1

normal throughput T2 = 0

normal reliability T1 = 0

minimum monetary cost T0 = 1

You would set the ToS to 9, which is 1001 in binary format.

Examples

The following example configures a tunnel server to preserve the IP ToS settings of the encapsulated IP payload for a Layer 2 Tunnel Protocol (L2TP) dial-in sessions:

```
vpdn-group 1
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname router12
 local name router32
 ip tos reflect
```

The following example sets the IP ToS bits to 8 (minimum delay as shown in Table 11) for packets that traverse the VPDN tunnel associated with VPDN group 1:

```
vpdn-group 1
 ip tos 8
```

Related Commands

Command	Description
ip precedence	Sets the precedence value (and an optional IP number or IP name) in the VPDN Layer 2 encapsulation header.
set ip tos (route-map)	Sets the ToS bits in the header of an IP packet.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

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. The default is 16. 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.

Defaults

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.

Defaults

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
 peer 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).