

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. Use the **no** form of this command to disable CPP encapsulation.

encapsulation cpp

no encapsulation cpp

Syntax Description This command has no arguments or keywords.

Defaults 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.

Currently, 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 Primary Rate Interfaces (PRIs) only.

Examples The following example configures BRI 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 interface serial 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.

firmware location

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

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

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

Syntax Description

system	If system is specified, the router loads the firmware from a built-in file within the Cisco IOS image.
flash	If flash is specified, the router loads the firmware from the Flash NVRAM located within the router.
<i>filename</i>	The name of the desired firmware file. If system is specified, enter the path to the filename you want to download.

Defaults

None

Command Modes

SPE configuration

Command History

Release	Modification
12.0(4)XI1	This command was introduced.
12.0(6)T	This command was migrated to Release 12.0(6)T.

Usage Guidelines

Use the **firmware location** SPE configuration command to download firmware into your modems. The **no** form of the command reverts the router back to the system embedded default. 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 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.

The **firmware location** command was first supported in Cisco IOS Release 12.0(4)XI1 along with the Resource Pool Management feature (although it can be used independently). For earlier images, use the **copy** command. For the Cisco IOS Release 12.0(4)XI1 images, the **copy {flash | system | tftp} modem** command will be disabled for MICA technologies modems and newer versions of Microcom modems (that is, 56 kbps). Old V.34 Microcom modems still use the **copy** command for downloading in Cisco IOS Release 12.0(4)XI1 images.



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.



Note 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 examples show 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 examples show 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
firmware upgrade	Specifies the method in which the SPE will be downloaded.

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. The **no** form of the command reverts the SPE back to the default SPE firmware upgrade option, busyout.

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

no firmware upgrade

Syntax Description		
	busyout	Starts firmware upgrade immediately. (Default)
	recovery	Delays firmware upgrade until recovery maintenance time.
	reboot	Delays firmware upgrade until reboot.

Defaults Busyout

Command Modes SPE configuration

Command History	Release	Modification
	12.0(6)T	This command introduced.

Usage Guidelines This command is for SPEs that contain more than 1 modem.

The SPE **firmware location** command is designed to integrate all continuous SPE ranges containing the same firmware location. However, the **firmware upgrade** command will not affect the SPE ranges. As such, all SPEs within the SPE range must have the same firmware upgrade mode or the router will default the upgrade mode to busyout. As such, if you want to upgrade a single SPE within an existing SPE range with a different upgrade mode than is currently configured, you must first change the upgrade mode for the entire SPE range and then change the firmware location for the specific SPE being upgraded.

Furthermore, each time you merge SPE ranges due to configuration changes, verify that the configuration of the SPE firmware upgrade remains effective to what is desired.

Examples 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 only be cleared when the SPE is finally downloaded. When all modems within the SPE are in the “pending download”

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. This is the default option for the firmware upgrade process:

```
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 which need to have their SPE upgraded and are also going to be rebooted for maintenance. The new firmware can be configured, but will not take affect until the reboot takes place:

```
firmware upgrade reboot
```

If recovery upgrade is specified, the SPE modem are reloaded based on the modem recovery algorithm. The SPE modems are all set into a “pending upgrade” state when you use the **firmware location** command on this SPE. The “pending upgrade” state continues to allow modems to be allocated to modems for as long as there are active calls on the SPE. Only when no active calls exist on the SPE will the firmware download take place. Furthermore, at the configured “modem recovery maintenance time” (3:00 a.m.), the modem recovery maintenance process will, in a controller fashion, attempt to reload the modems by busying out the modems for a window duration of time to make the download take place. Consult the modem recovery documentation for further details. The recovery upgrade option is the least impacting way to upgrade modems on an active router. Capacity is kept at a maximum. However, this option may take a few days for all modems to be reloaded to the new firmware location:

```
firmware upgrade recovery
```

Related Commands

Command	Description
firmware location	Downloads firmware into the modems from this file location.
modem recovery maintenance time	Specifies the modem maintenance recovery behavior, time of day for the scheduled modem recovery.
modem recovery maintenance window	Specifies the modem maintenance recovery behavior, amount of time for normal recovery to take place.
modem recovery maintenance action	Specifies the modem maintenance recovery behavior, mode of 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. Use the **no** form of this command to disable flow control.

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	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 are assumed.
lock	(Optional) Used to make it impossible to turn off flow control from the remote host when the connected device <i>needs</i> software flow control. This option applies to connections using the Telnet or rlogin protocols.
hardware	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 are assumed. For more information about hardware flow control, see the hardware manual that was shipped with your router.

Defaults

No flow control

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.

flush-at-activation

To discard any data or noise characters that are sitting in the input buffer of the asynchronous line before the line is activated, use the **flush-at-activation** command in line configuration mode. To keep any data or noise characters that are sitting in the input buffer of the asynchronous line before the line is activated, use the **no** form of this command.

flush-at-activation

no flush-at-activation

Syntax Description This command has no keywords or arguments.

Defaults Enabled by default.

Command Modes Line configuration

Command History	Release	Modification
	11.1(5)	This command was introduced.

Usage Guidelines For an incoming call on a line configured with modem control (using the **modem inout** and **modem dialin** commands), the line will be activated when the data set ready (DSR) signal goes high and will be dropped when the DSR signal goes low. While the line is idle, its input buffer may receive characters; for example, modem result codes such as “NO CARRIER” or “RING” or line noise. Such characters are not useful to the line application. Flushing the line input buffer when the DSR goes high using the **flush-at-activation** command is the preferred behavior.



Note

To know whether the DSR signal is going high or low, use the **debug modem** command or the **show line** command. Output of these commands displays the status of DSR signal.

On most Cisco IOS platforms, there may be up to a one-second delay between when the DSR signal goes high and Cisco IOS activates the line. Therefore, some valid data received from the line may be discarded when you issue the **flush-at-activation** command. If it is important to process this valid data rather than discarding it and the application is tolerant of receiving bad data, configure the **no flush-at-activation** command.

The application that is used determines whether the system can differentiate the valid data from the bad data or the system is tolerant of receiving any data. For example, consider that the application used is TCP over IP over PPP. PPP uses a Frame Check Sequence (FCS) in a data frame format to verify the integrity of the received data. If an invalid data pattern is delivered to a PPP receiver, PPP will discard it as a framing or FCS error. So the bad data will not be delivered to the higher layers. Even if some data is delivered up to IP and TCP, TCP has its own FCS which will reject bad data. Therefore, the application is tolerant of receiving the bad data that the line delivers.

Consider another application where incoming character data received from the line is delivered as TCP payload to a server running a pager application. Unless the pager application has implemented its own protocol to verify data integrity, this bad data may cause the pager not to be delivered, or to deliver bad data within the message payload to the receiving pager. So the bad data should not be delivered as payload to the line.

Where an upper-layer framed protocol such as PPP or Serial Line Internet Protocol (SLIP) is always used (asynchronous mode dedicated), the framed protocol may reach link status more quickly when you issue the **no flush-at-activation** command. Since the framed protocol discards any erroneous data received, you do not have to use the **flush-at-activation** command.

If the line application is not tolerant of receiving bad data; for example, when you are using character-mode username/password authentication, always use the **flush-at-activation** command. Otherwise, the bad data may trigger an application failure.

**Note**

Prior to Cisco IOS Release 12.2, the **no flush-at-activation** command was the default on AS5000 platforms with modem ISDN channel aggregation (MICA) and NextPort modems. However, from Cisco IOS Release 12.3 and later, there is no longer any significant delay between when the modem link reaches steady state (DSR high) and when the line is activated so you do not need to use the **no flush-at-activation** command. The modem state STEADY_STATE is mapped to DSR high and TERMINATING is mapped to DSR low when asynchronous lines are the internal digital modem ports.

Examples

The following example shows how to configure lines 1/0 through 1/59 to flush any data in their input buffers when the lines are activated:

```
Router(config)# line 1/0 1/59
Router(config-line)# flush-at-activation
```

Related Commands

Command	Description
activation-character	Defines the character entered at a vacant terminal to begin a terminal session.
debug modem	Observes modem line activity on an access server.
modem dialin	Configures a line to enable a modem attached to the router to accept incoming calls only.
modem inout	Configures a line for both incoming and outgoing calls.
show line	Displays parameters of a terminal line.

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 migrated to Release 12.0(1)T.
	12.0(5)T	This command was modified to only be available 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 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	Specifies the LNS to use for authenticating, and the virtual template to use for cloning, new virtual access interfaces when an incoming L2TP tunnel connection is requested from a specific peer.
	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.

T1 Line

```
framing {sf | esf}
```

E1 Line

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

Syntax Description	Keyword	Description
	sf	Specifies Super Frame as the T1 frame type.
	esf	Specifies Extended Super Frame as the T1 frame type.
	crc4	Specifies CRC4 frame as the E1 frame type.
	no-crc4	Specifies no CRC4 frame as the E1 frame type.
	australia	(Optional) Specifies the 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 T1 or E1 fractional data line. The service provider determines which framing type, either the **sf**, **esf**, or **crc4** keyword, is required for your T1/E1 circuit.

Examples

The following example selects Extended Super Frame 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 linecode 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. Use the **no** form of the command to remove an interface from the member list.

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

no group-range *interface*

Syntax Description

<i>low-end-of-range</i>	Beginning interface number to be made a member of the group interface.
<i>high-end-of-range</i>	Ending interface number to be made a member of 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.

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.

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 the command.

initiate-to ip *ip-address*

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

Syntax Description	ip <i>ip-address</i>	The IP address of the router that will be tunneled to.
--------------------	-----------------------------	--

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

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 LAC configured to request dial-in can be configured with multiple **initiate-to** commands to tunnel to more than one IP address.

An LNS configured to request dialout can only be configured 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 an L2TP tunnel to the peer at IP address 10.3.2.1 for tunneling dialout 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 VPDN group to request L2F or L2TP tunnels to a home gateway and creates a request-dialin VPDN subgroup.
	request dialout	Enables an LNS to request VPDN dial-out calls by using L2TP.

interface

To define the IP addresses of the server, use the interface command in interface configuration mode. To disable this function, use the **no** form of this command.

interface *name-tag*

no interface *name-tag*

Syntax Description	<i>name-tag</i>	The logic name to identify the server configuration so that multiple entries of server configuration can be entered.
Defaults	Disabled	
Command Modes	Interface configuration	
Command History	Release	Modification
	11.3(7)	This command was introduced.
Usage Guidelines	Each server can have multiple entries of IP addresses or aliases.	
Related Commands	Command	Description
	clear rlm group	Clears all RLM group time stamps to zero.
	clear interface	Resets the hardware logic on an interface.
	link (RLM)	Specifies the link preference.
	protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
	retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
	server (RLM)	Defines the IP addresses of the server.
	show rlm group statistics	Displays the network latency of the RLM group.
	show rlm group status	Displays the status of the RLM group.
	show rlm group timer	Displays the current RLM group timer values.
	shutdown (RLM)	Shuts down all of the links under the RLM group.
	timer	Overwrites the default setting of timeout values.

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 subinterfaces

To configure a BRI subinterface only, use the following forms of the **interface bri** command in global configuration mode:

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

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

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

```
interface bri number:0
```

```
interface bri slot/port:0
```

Syntax	Description
<i>number</i>	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.
<i>slot/port</i>	On the Cisco 7200 series, slot location and port number of the interface.
<i>.subinterface-number</i>	Subinterface number in the range 1 to 4294967293. The <i>number</i> that precedes the period (.) must match the <i>number</i> this subinterface belongs to.
multipoint point-to-point	(Optional) Specifies a multipoint or point-to-point subinterface. The default is multipoint .
:0	The 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.
11.2F	The capability to carry X.25 traffic on the D channel was added.
11.2P	This command was modified to include slot/port syntax for the PA-8B-ST and PA-4B-U port adapters on Cisco 7200 series routers.

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*.)

Examples

The following example configures BRI 0 to call and receive calls from two sites, use Point-to-Point Protocol (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 131.108.36.10 name EB1 234
  dialer map ip 131.108.36.9 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 window-size 2 2
  x25 facility packet-size 256 256
  x25 facility throughput 9600 9600
  x25 map ip 10.1.1.3 31107000000200
```

Related Commands

Command	Description
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.
encapsulation	Sets the encapsulation method used by the interface.
isdn spid1, isdn spid2	Defines the SPID number that has been assigned by the ISDN service provider for the B1 channel.

Command	Description
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 *number*

Syntax Description	<i>number</i>	Number of the dialer rotary group. It can be number in the range 0 through 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 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 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 1.2.3.4
  dialer map ip 1.2.2.5 name YYY 14155553434
  dialer map ip 1.3.2.6 name ZZZ
```

interface multilink

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

interface multilink *group-number*

no interface multilink

Syntax Description

group-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.
12.0(3)T	Support for MLP was introduced for VIP-based T1 and E1 interfaces on the Cisco 7500 Series.
12.0(4)T	Support for this command was implemented for non-VIP-based T1 and E1 interfaces and on the Cisco 7200 Series.

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
multilink-group	Designates an interface as part of a multilink leased line bundle.
ppp multilink fragmentation	Enables or disables MLP fragmentation. Disabling allows multilink packets to be forwarded across platforms.

interface serial

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

Cisco 7200 series and Cisco 7500 series routers

```
interface serial slot/port:timeslot
```

Cisco AS5200 series and Cisco 4000 series access servers

```
interface serial number:timeslot
```

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

Defaults You must explicitly specify a serial interface.

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The D channel is always the **:23** channel for T1 and the **:15** 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 131.108.13.2 255.255.255.0
encapsulation ppp
!
interface serial 0:1
ip address 131.108.13.3 255.255.255.0
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 131.108.13.1 255.255.255.0
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	<i>number</i>	Number used to identify the virtual template interface.
---------------------------	---------------	---

Defaults	Disabled. No virtual template number is defined.
-----------------	--

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.2F	This command was introduced.

Usage Guidelines	<p>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 nonvolatile RAM (NVRAM).</p> <p>Once the virtual template interface is created, it can be configured in the same way as a serial interface.</p> <p>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).</p>
-------------------------	--

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. Use the **no** form of this command to disable this feature.

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 <i>default</i> 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 alias

To assign an IP address to the service provided on a TCP port, use the **ip alias** command in interface configuration mode. Use the **no** form of this command to remove the specified address for the router.

ip alias *ip-address tcp-port*

no ip alias *ip-address*

Syntax Description	
<i>ip-address</i>	Specifies the IP address for the service.
<i>tcp-port</i>	Specifies the number of the TCP port.

Defaults No default behavior or values.

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines A user attempting to establish a connection is connected to the first free line in a rotary group using the Telnet protocol.

The IP address must be on the same network or subnet as the router's main address, and must not be used by another host on that network or subnet. Connecting to the IP address has the same effect as connecting to the router's main address, using *tcp-port* as the TCP port.

You can use the **ip alias** command to assign multiple IP addresses to the router. For example, in addition to the primary alias address, you can specify addresses that correspond to lines or rotary groups. Using the **ip alias** command in this way makes the process of connecting to a specific rotary group transparent to the user.

When asynchronous mode is implemented, the Cisco IOS software creates the appropriate IP aliases, which map the asynchronous addresses for the lines to which they are connect. This process is automatic and does not require configuration.

Examples The following example configures connections to IP address 172.30.42.42 to act identically to connections made to the server's primary IP address on TCP port 3001. In other words, a user is connected to the first free line on port 1 of the rotary group that uses the Telnet protocol.

```
ip alias 172.30.42.42 3001
```

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. Use the **no** form of the command to remove a DHCP server's IP address.

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

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

Syntax Description

<i>ip-address</i>	(Optional) IP address of a DHCP server.
<i>name</i>	(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 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 user's SLIP/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 wish 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. See the chapters about configuring IP addressing in the *Cisco IOS IP and IP Routing 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 129.12.13.81:

```
ip dhcp-server 129.12.13.81
```

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 the current DHCP settings on point-to-point interfaces.

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. Use the **no** form of this command to remove a range of addresses from a pool (longer form of the **no** command), or to delete an address pool (shorter form of the **no** command).

```
ip local pool { default | pool-name low-ip-address [high-ip-address] }
```

```
no ip local pool { default | pool-name low-ip-address [high-ip-address] }
```

```
no ip local pool { default | pool-name }
```

Syntax Description	default	Defaults local address pool that is used if no other pool is named.
	<i>pool-name</i>	Name of a specific local address pool.
	<i>low-ip-address</i>	Lowest IP address in the pool.
	<i>high-ip-address</i>	(Optional) Highest IP address in the pool. If this value is omitted only the low-ip-address IP address is included in the local pool.

Defaults No address pools are configured.

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.
	12.0	This command was migrated to Release 12.0.

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, and to add another range of addresses to an existing pool. The **default** address pool is then used on all point-to-point interfaces after the **ip address-pool local** global configuration command is issued. To use a specific, named address pool on an interface, use the **peer default ip address pool** interface configuration command.

These 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 Dial Services Configuration Guide: Terminal Services* and the “System Management” part of the *Cisco IOS Configuration Fundamentals Configuration Guide* for more information. Pools can be displayed with the **show ip local pool** command.

Examples

The following command creates a local IP address pool named quark, which contains all local IP addresses from 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 1.1.1.0 1.1.4.255
#^Z
show ip local pool
  Pool      Begin          End              Free InUse
  default   1.1.1.0        1.1.4.255       1024  0
```

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

```
no ip local pool default
ip local pool default 9.1.1.0 9.1.9.255
ip local pool default 9.2.1.0 9.2.9.255
^Z

show ip local pool
  Pool      Begin          End              Free   In use   Cache Size
  default   9.1.1.0        9.1.9.255       2304    0         20
           9.2.1.0        9.2.9.255       2304    0
```

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.
show ip local pool	Displays statistics for any defined IP address pools.
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 route (large-scale dial-out)

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

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

no ip route

Syntax Description

<i>network-number</i>	IP address of the target network or subnet.
<i>network-mask</i>	Network mask that lets you mask network and subnetwork bits.
<i>IP address</i>	Internet address of the next hop that can be used to reach that network in standard IP address notation. Example: 1.1.1.1.
<i>interface</i>	Network interface to use.
<i>distance</i>	(Optional) An 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, 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 AAA server as the next hop for large scale dialout, and is the *name* argument with the -out suffix appended. The suffix is automatically supplied and is required since 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 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 macarthur-out will be retrieved from the AAA:

```
ip route 10.0.0.0 255.255.255.255 Dialer0 name macarthur
```

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. Use the **no** form of the command to disable the special queue for real-time traffic.

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

no ip rtp reserve

Syntax Description

<i>lowest-udp-port</i>	Lowest UDP port number to which the packets are sent.
<i>range-of-ports</i>	Number, which added to the lowest-UDP-port value, yields the highest UDP port value.
<i>maximum-bandwidth</i>	(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	Configures a maximum delay allowed for transmission of a packet fragment on a MLP bundle.
ppp multilink interleave	Enables interleaving of RTP packets among the fragments of larger packets on a 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 Disabled. Asynchronous listening is 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 called mktg.

```
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ip tcp async-mobility server
exit

%SYS-5-CONFIG_I: Configured from console by console
tunnel ?
  WORD Address or hostname of a remote system

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

no ip telnet comport

Syntax Description

This command has no arguments or keywords.

Defaults

Telnet Com Port extensions are enabled

Command Modes

Global configuration

Command History

Release	Modification
11.3(1)	This command was introduced.

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 port 6000 + for individual lines, or 7000 + for rotaries on the Cisco NAS.

Examples

The following example disables Telnet Com Port extensions:

```
no ip telnet comport
```

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 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]
Router#
```

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
Router#
```

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	<i>hex-value</i>	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: <pre>ip telnet tos 0</pre>
-----------------	--

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

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. Use the **no** form of this command to disable compression of IPX packet headers in a PPP session.

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.

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. Use the **no** form of this command to disable a nonrouting IPX client.

ipx ppp-client loopback *number*

no ipx ppp-client loopback *number*

Syntax Description	loopback	Loopback interface configured with a unique IPX network number.
	<i>number</i>	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
 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).

ipx nasi-server enable

To enable NetWare Asynchronous Services Interface (NASI) clients to connect to asynchronous devices attached to your router, use the **ipx nasi-server enable** command in global configuration mode. Use the **no** form of this command to prevent NASI clients from connecting through a router.

ipx nasi-server enable

no ipx nasi-server enable

Syntax Description This command has no arguments or keywords.

Defaults NASI is not enabled.

Command Modes Global configuration

Release	Modification
11.1	This command was introduced.

Usage Guidelines When you issue this command, NASI clients can connect to any port on the router other than the console port to access network resources. When the user on the NASI client uses the Windows or DOS application to connect to the router, a list of available tty and vty lines appears, beginning with tty1. The user selects the desired outgoing tty or vty port.

You can configure TACACS+ security on the router so that after the user selects a tty or vty port, a username and password prompt appear for authentication, authorization, and accounting purposes.

Examples The following example shows a minimum configuration to enable NASI client dial-in access with TACACS+ authentication:

```
ipx routing
ipx internal-network ncs001
interface ethernet 0
    ipx network 1
ipx nasi-server enable
! enable TACACS+ authentication for NASI clients using the list name swami
aaa authentication nasi swami tacacs+
line 1 8
    modem inout
```

ipx nasi-server enable

Related Commands	Command	Description
	aaa authentication nasi	Specifies AAA authentication for NASI clients connecting through the access server.
	nasi authentication	Enables AAA authentication for NASI clients connecting to a router.
	show ipx nasi connections	Displays the status of NASI connections
	show ipx spx-protocol	Displays the status of the SPX protocol stack and related counters.