

initiate-to

To specify an IP address that will be used for Layer 2 tunneling, 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* [**limit** *limit-number*] [**priority** *priority-number*]

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

Syntax Description

| | |
|--|---|
| ip <i>ip-address</i> | Specifies the IP address of the router that will be tunneled to. |
| limit <i>limit-number</i> | (Optional) Specifies a limit to the number of connections that can be made to this IP address in the range from 0 to 32767. |
| priority <i>priority-number</i> | (Optional) Specifies a priority for this IP address in the range from 1 to 32767. 1 is the highest priority. |

Defaults

This command is disabled.

Command Modes

VPDN group configuration

Command History

| Release | Modification |
|-----------|---|
| 12.0(5)T | This command was introduced. |
| 12.2(15)T | This command was enhanced with the capability to configure multiple Layer 2 Tunneling Protocol (L2TP) access concentrators (LACs) on an L2TP network server (LNS) within the same VPDN group. |

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.

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

An LNS configured to request dial-out can be configured with multiple **initiate-to** commands to enable tunneling to more than one IP address.

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 dial-out calls from dialer pool 1. This group can tunnel a maximum of five simultaneous users and has the second highest priority for requesting dial-out calls.

```
vpdn-group 1
 request-dialout
  protocol l2tp
  pool-member 1
 initiate-to ip 10.3.2.1 limit 5 priority 2
```

The following example configures VPDN group 1 to request L2TP tunnels to the peers (LACs) at IP addresses 10.0.58.201 and 10.0.58.205. The two LACs configured by the **initiate-to** commands have differing priority values to provide failover redundancy.

```
vpdn-group 1
  accept-dialin
    protocol l2tp
    virtual-template 1
  request-dialout
    protocol l2tp
    pool-member 1
  initiate-to ip 10.0.58.201 priority 1
  initiate-to ip 10.0.58.205 priority 100
  source-ip 10.0.58.211
```

In the previous example, you would configure load balancing among the LACs by setting the **priority** values in the **initiate-to** commands to the same values.

The following partial example shows how to set parameters to control how many times an LNS will retry connecting to a LAC, and the amount of time after which the LAC will declare itself down or busy so that the LNS will try connecting to the next LAC. (Note that the **l2tp tunnel** commands are optional and should be used only if it becomes necessary to change the default settings for these commands.)

```
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
.
.
.
  request-dialout
    protocol l2tp
    pool-member 1
  initiate-to ip 10.0.58.201 priority 1
  initiate-to ip 10.0.58.207 priority 50
  initiate-to ip 10.0.58.205 priority 100
  l2tp tunnel retransmit initial retries 5
  l2tp tunnel retransmit initial timeout min 4
  l2tp tunnel busy timeout 420
.
.
.
```

Related Commands

| Command | Description |
|---|---|
| l2tp tunnel busy timeout | Configures the amount of time that the router will wait before attempting to recontact a router that was previously busy. |
| l2tp tunnel retransmit initial retries | Sets the number of times that the router will attempt to send out the initial control packet for tunnel establishment before considering a router busy. |
| l2tp tunnel retransmit initial timeout | Sets the minimum or maximum amount of time that the router will wait before resending an initial packet out to establish a tunnel. |

| 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. |
| source-ip | Specifies an alternate IP address for a VPDN tunnel that is different from the physical IP address used to open the tunnel. |

interface bri

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

Cisco 7200 Series and 7500 Series Routers

```
interface bri number
```

```
interface bri slot/port
```

Cisco 7200 Series and 7500 Series Routers with BRI Subinterfaces Only

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

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

X.25 on an ISDN BRI Interface

```
interface bri number:0
```

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

| Syntax Description | | |
|---|--|---|
| <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. The slash mark is required. |
| <i>.subinterface-number</i> | | Subinterface number in the range from 1 to 4,294,967,293. The <i>number</i> that precedes the period (.) must match the <i>number</i> 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 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-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 | <i>dialer-rotary-group-number</i> 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 | <i>multilink-bundle-number</i> 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 | <p>The following example creates multilink bundle 1:</p> <pre>interface multilink 1 ip address 192.168.11.4 255.255.255.192 encapsulation ppp ppp multilink keepalive</pre> |
|-----------------|---|

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

| | |
|---------------|--|
| <i>number</i> | 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 |
| <i>previous</i> | (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-pool** | **dhcp-proxy-client** | **local** }

no ip address-pool

| Syntax Description | | |
|--------------------|--------------------------|--|
| | dhcp-pool | Uses on-demand address pooling as the global default address mechanism. This option supports only remote access PPP sessions using a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN). IP addresses are obtained from locally configured virtual routing and forwarding (VRF)-associated Dynamic Host Configuration Protocol (DHCP) pools. |
| | dhcp-proxy-client | Uses the router as the proxy client between a third-party DHCP server and peers connecting to the router as the global default address mechanism. |
| | local | Uses the local address pool named <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. |
| | 12.2(8)T | The dhcp-pool keyword was added. |

Usage Guidelines

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

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

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

Examples

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

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

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

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

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

```
ip address-pool local
```

Related Commands

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

ip dhcp-client network-discovery

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

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

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

Syntax Description

| | |
|--|--|
| informs <i>number-of-messages</i> | Number of DHCP Inform messages. Valid choices are 0, 1, or 2 messages. Default is 0 messages. |
| discovers <i>number-of-messages</i> | Number of DHCP Discover messages. Valid choices are 0, 1, or 2 messages. Default is 0 messages. |
| period <i>seconds</i> | 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 message 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

| | |
|-------------------|---|
| <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 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 idle-group

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

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

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

Syntax Description

| | |
|---------------------------|--|
| <i>access-list-number</i> | IP access list number. |
| <i>access-list-name</i> | IP access list name. |
| in | Classifies IP inbound traffic for the PPP idle timer. |
| out | Classifies IP outbound traffic for the PPP idle timer. |

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

ip local pool

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

```
ip local pool { default | poolname } [low-ip-address [high-ip-address]] [group group-name]
[cache-size size]
```

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

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

Syntax Description

| | |
|---|--|
| default | Creates a default local IP address pool that is used if no other pool is named. |
| <i>poolname</i> | Name of the local IP address pool. |
| <i>low-IP-address</i> [<i>high-IP-address</i>] | First and, optionally, last address in an IP address range. |
| group <i>group-name</i> | (Optional) Creates a pool group. |
| cache-size <i>size</i> | (Optional) Sets the number of IP address entries on the free list that the system checks before assigning a new IP address. Returned IP addresses are placed at the end of the free list. Before assigning a new IP address to a user, the system checks the number of entries from the end of the list (as defined by the cache-size <i>size</i> 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. Any pool created without the optional **group** keyword is a member of the base system group.

Command Modes

Global configuration

Command History

| Release | Modification |
|-----------|--|
| 11.0 | This command was introduced. |
| 11.3 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. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T and support was added for the Cisco 6400 node route processor 25v (NRP-25v) and Cisco 7400 platforms. |

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 and 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 or TACACS+ authorization functions. Refer to the chapter “Configuring Protocol Translation and Virtual Asynchronous Devices” in the *Cisco IOS Terminal Services Configuration Guide* and the “System Management” part of the *Cisco IOS Configuration Fundamentals Configuration Guide* for more information.

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

Examples

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

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

The following example configures a pool of 1024 IP addresses:

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

**Note**

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

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

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

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

```
ip local pool p1_g1 10.1.1.1 10.1.1.50 group grp1
ip local pool p2_g1 10.1.1.100 10.1.1.110 group grp1
ip local pool p1_g2 10.1.1.1 10.1.1.40 group grp2
ip local pool lp1 10.1.1.1 10.1.1.10
ip local pool p3_g1 10.1.2.1 10.1.2.30 group grp1
ip local pool p2_g2 10.1.1.50 10.1.1.70 group grp2
ip local pool lp2 10.1.2.1 10.1.2.10
```

In the example:

- Group grp1 consists of pools p1_g1, p2_g1, and p3_g1.
- Group grp2 consists of pools p1_g2 and p2_g2.
- Pools lp1 and lp2 are not associated with a group and are therefore members of the base system group.

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

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

```
ip local pool p1_vpn1 10.1.1.1 10.1.1.50 group vpn1
ip local pool p2_vpn1 10.1.1.100 10.1.1.110 group vpn1
ip local pool p1_vpn2 10.1.1.1 10.1.1.40 group vpn2
ip local pool lp1 10.1.1.1 10.1.1.10
ip local pool p3_vpn1 10.1.2.1 10.1.2.30 group vpn1
ip local pool p2_vpn2 10.1.1.50 10.1.1.70 group vpn2
ip local pool lp2 10.1.2.1 10.1.2.10
```

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

- Group vpn1 consists of pools p1_vpn1, p2_vpn1, and p3_vpn1.
- Group vpn2 consists of pools p1_vpn2 and p2_vpn2.
- Pools lp1 and lp2 are not associated with a group and are therefore members of the base system group.

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

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

In the example, a user in group `vpn1` is associated with some combination of the pools `p1_vpn1`, `p2_vpn1`, and `p3_vpn1`, and is allocated addresses from that address space. Addresses are returned to the same pool from which they were allocated.

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

ip 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 or VPDN template 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
VPDN template 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 VPDN tunnels to participate in path MTU discovery. |
| | vpdn-group | Creates a VPDN group and enters VPDN group configuration mode. |
| | vpdn-template | Creates a VPDN template and enters VPDN template configuration mode. |

ip pmtu

To enable the discovery of the path maximum transmission unit (MTU) for Layer 2 traffic, use the **ip pmtu** command in VPDN group, VPDN template, or pseudowire class configuration mode. To disable path MTU discovery, use the **no** form of this command.

ip pmtu

no ip pmtu

Syntax Description This command has no arguments or keywords.

Command Default Path MTU discovery is disabled.

Command Modes
 VPDN group configuration
 VPDN template configuration
 Pseudowire class configuration

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.2(4)T | This command was introduced. |
| | 12.2(11)T | This command was implemented on the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms. |
| | 12.0(23)S | This command was integrated into Cisco IOS Release 12.0(23)S and support was added for using this command in pseudowire class configuration mode. |
| | 12.3(2)T | Support was added for using this command in pseudowire class configuration mode. |

Usage Guidelines When the **ip pmtu** command is enabled, the Don't Fragment (DF) bit is copied from the inner IP header to the Layer 2 encapsulation header.

Enabling the **ip pmtu** command triggers Internet Control Message Protocol (ICMP) unreachable messages that indicate fragmentation errors in the IP backbone network carrying the tunneled traffic. If an IP packet is larger than the MTU of any interface it must pass through and the DF bit is set, the packet is dropped and an ICMP unreachable message is returned. The ICMP unreachable message indicates the MTU of the interface that was unable to forward the packet without fragmentation. This information allows the source host to reduce the size of the packet before retransmission, allowing it to fit through that interface.



Note

When path MTU discovery (PMTUD) is enabled, VPDN deployments are vulnerable to Denial of Service (DoS) attacks that use crafted Internet Control Message Protocol (ICMP) "fragmentation needed and Don't Fragment (DF) bit set" (code 4) messages, also known as PMTUD attacks.

Crafted code 4 ICMP messages can be used to set the path MTU to an impractically low value. This will

cause higher layer protocols to time out because of a very low throughput, even though the connection is still in the established state. This type of attack is classified as a throughput-reduction attack. When PMTUD is enabled, it is highly recommended that you use the **vpdn pmtu** command to configure a range of acceptable values for the path MTU to block PMTUD attacks.

Enabling PMTUD will decrease switching performance.

When issued in VPDN group configuration mode, the **ip pmtu** command enables any tunnel associated with the specified virtual private dialup network (VPDN) group to participate in path MTU discovery.

When issued in VPDN template configuration mode, the **ip pmtu** command enables any tunnel associated with the specified VPDN template to participate in path MTU discovery.

When issued in pseudowire class configuration mode, the **ip pmtu** command enables any Layer 2 Tunnel Protocol Version 3 (L2TPv3) session derived from the specified pseudowire class configuration to participate in path MTU discovery.

Examples

The following example configures a VPDN group named dial-in on a Layer 2 Tunnel Protocol (L2TP) tunnel server and uses the **ip pmtu** command to specify that tunnels associated with this VPDN group will participate in path MTU discovery. The **vpdn pmtu** command is used to configure the device to accept only path MTU values ranging from 576 to 1460 bytes. The device will ignore code 4 ICMP messages that specify a path MTU outside of this range.

```
Router(config)# vpdn-group dial-in
Router(config-vpdn)# request-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 1
!
Router(config-vpdn)# l2tp security crypto-profile l2tp
Router(config-vpdn)# no l2tp tunnel authentication
Router(config-vpdn)# lcp renegotiation on-mismatch
Router(config-vpdn)# ip pmtu
!
Router(config)# vpdn pmtu maximum 1460
Router(config)# vpdn pmtu minimum 576
```

The following example shows how to enable the discovery of the path MTU for pseudowires that are created from the pseudowire class named ether-pw. The **vpdn pmtu** command is used to configure the device to accept only path MTU values ranging from 576 to 1460 bytes. The device will ignore code 4 ICMP messages that specify a path MTU outside of this range.

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# ip pmtu
!
Router(config)# vpdn pmtu maximum 1460
Router(config)# vpdn pmtu minimum 576
```

Related Commands

| Command | Description |
|-------------------------|--|
| ip dfbit set | Enables the DF bit in the outer L2TPv3 tunnel header. |
| ip mtu | Sets the MTU size of IP packets sent on an interface. |
| ip mtu adjust | Enables automatic adjustment of the IP MTU on a virtual access interface. |
| pseudowire-class | Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode. |

| Command | Description |
|----------------------|---|
| vpdn pmtu | Manually configures a range of allowed path MTU sizes for an L2TP VPDN. |
| vpdn-group | Creates a VPDN group and enters VPDN group configuration mode. |
| vpdn-template | Creates a VPDN template and enters VPDN template configuration mode. |

ip precedence (VPDN)

To set the precedence value in the virtual private dialup network (VPDN) Layer 2 encapsulation header, use the **ip precedence** command in VPDN group or VPDN template configuration mode. To remove a precedence value setting, use the **no** form of this command.

ip precedence {*number* | *name*}

no ip precedence {*number* | *name*}

Syntax Description

| | |
|-----------------------------|--|
| <i>number</i> <i>name</i> | A number or name that defines the setting for the precedence bits in the IP header. The values for the <i>number</i> argument and the corresponding <i>name</i> argument are listed in Table 9 , from least to most important. |
|-----------------------------|--|

Command Default

The IP precedence value of the Layer 2 encapsulation header is set to zero.

Command Modes

VPDN group configuration
VPDN template 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 9](#) 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 9 *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 queuing (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 enters VPDN group configuration mode. |
| vpdn-template | Creates a VPDN template and enters VPDN template 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

| | |
|-------------------------|---|
| <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: 10.1.1.1. |
| <i>interface</i> | Network interface name and number to use. |
| <i>distance</i> | (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 <i>name</i> | (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 | | |
|--------------------|--------------------------|---|
| | <i>lowest-udp-port</i> | Lowest UDP port number to which the packets are sent. |
| | <i>range-of-ports</i> | Number, which when 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 | 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 least 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. |
| <i>seconds</i> | Number of seconds to delay the TCP closure. Possible values: 0 to 360. |
| <i>number-of-characters</i> | Number of characters to be saved in the device buffer before sending an RFC 2217 SUSPEND message. |
| <i>window-size</i> | 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 communication, 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 | <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:

```
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

| | |
|--------------------------|---|
| <i>tos-bit-value</i> | A value (number) from 0 to 15 that sets the ToS bits in the IP header. See Table 10 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 10 shows the format of the four ToS bits in binary form.

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

| | |
|-----------------|--|
| 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. |
|--------------------|----------------------------------|---|
| | <i>loopback-interface-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
  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). |