peer default ip address

To specify an IP address, an address from a specific IP address pool, or an address from the Dynamic Host Configuration Protocol (DHCP) mechanism to be returned to a remote peer connecting to this interface, use the `peer default ip address` command in interface configuration mode. To disable a prior peer IP address pooling configuration on an interface, or to remove the default address from your configuration, use the `no` form of this command.

```
peer default ip address {ip-address | dhcp-pool | dhcp | pool [pool-name]}

no peer default ip address
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Specific IP address to be assigned to a remote peer dialing in to the interface. To prevent duplicate IP addresses from being assigned on more than one interface, this argument cannot be applied to a dialer rotary group nor to an ISDN interface.</td>
</tr>
<tr>
<td>dhcp-pool</td>
<td>Retrieves an IP address from an on-demand address pool. This option only supports remote access (PPP) sessions into MPLS VPNs.</td>
</tr>
<tr>
<td>dhcp</td>
<td>Retrieves an IP address from the DHCP server.</td>
</tr>
<tr>
<td>pool</td>
<td>Uses the global default mechanism as defined by the <code>ip address-pool</code> command unless the optional <code>pool-name</code> argument is supplied. This is the default.</td>
</tr>
<tr>
<td>pool-name</td>
<td>(Optional) Name of a local address pool created using the <code>ip local pool</code> command. DHCP retrieves an address from this pool regardless of the global default mechanism setting.</td>
</tr>
</tbody>
</table>

### Command Default

The default is `pool`.

### Command Modes

Interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(8)T</td>
<td>The <code>dhcp-pool</code> keyword was added.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command applies to point-to-point interfaces that support the PPP or Serial Line Internet Protocol (SLIP) encapsulation. This command sets the address used on the remote (PC) side.

### Note

This command replaces the `async default ip address` command.

This command allows an administrator to configure all possible address pooling mechanisms on an interface-by-interface basis.
The **peer default ip address** command can override the global default mechanism defined by the **ip address-pool** command on an interface-by-interface basis, as follows:

- For all interfaces not configured with a peer default IP address mechanism (equivalent to selecting the **peer default ip address pool** command), the router uses the global default mechanism that is defined by the **ip address-pool** command.

- If you select the **peer default ip address pool pool-name** form of this command, then the router uses the locally configured pool on this interface and does not follow the global default mechanism.

- If you select the **peer default ip address ip-address** form of this command, the specified IP address is assigned to any peer connecting to this interface and any global default mechanism is overridden for this interface.

- If you select the **peer default ip address dhcp** form of this command, the DHCP proxy-client mechanism is used by default on this interface and any global default mechanism is overridden for this interface.

- If you select the **peer default ip address dhcp-pool** form of this command, the DHCP on-demand address pooling mechanism is used by default on this interface and any global default mechanism is overridden for this interface.

### Examples

The following command specifies that this interface will use a local IP address pool named pool3:

```bash
peer default ip address pool pool3
```

The following command specifies that this interface will use the IP address 172.19.34.21:

```bash
peer default ip address 172.19.34.21
```

The following command reenables the global default mechanism to be used on this interface:

```bash
peer default ip address pool
```

The following example specifies address 192.168.7.51 for asynchronous interface 6:

```bash
line 20
  speed 115200
interface async 6
  peer default ip address 192.168.7.51
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>async dynamic</td>
<td>Specifies dynamic asynchronous addressing versus default addressing.</td>
</tr>
<tr>
<td>address</td>
<td></td>
</tr>
<tr>
<td>encapsulation</td>
<td>Enables SLIP encapsulation.</td>
</tr>
<tr>
<td>slip</td>
<td></td>
</tr>
<tr>
<td>exec</td>
<td>Allows an EXEC process on a line.</td>
</tr>
<tr>
<td>ip address-pool</td>
<td>Enables an address pooling mechanism used to supply IP addresses to dial in asynchronous, synchronous, or ISDN point-to-point interfaces.</td>
</tr>
<tr>
<td>ip dhcp-server</td>
<td>Specifies which DHCP servers to use on a network, and specifies the IP address of one or more DHCP servers available on the network.</td>
</tr>
<tr>
<td>ip local pool</td>
<td>Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.</td>
</tr>
<tr>
<td>ppp</td>
<td>Starts an asynchronous connection using PPP.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show cot dsp</td>
<td>Displays information about the COT DSP configuration or current status.</td>
</tr>
<tr>
<td>slip</td>
<td>Starts a serial connection to a remote host using SLIP.</td>
</tr>
</tbody>
</table>
peer ip address forced

To force the router to assign a peer the next available IP address in the pool for an interface, use the peer ip address forced command in interface configuration mode. To allow a peer to negotiate a specific IP address or to allow the router to attempt to assign a peer its previously assigned IP address, use the no form of this command.

peer ip address forced
no peer ip address forced

Syntax Description
This command has no arguments or keywords.

Command Default
When a network device dials in to a Cisco network access server (NAS) that is configured to assign an IP address to the network device, the NAS attempts to assign the device the address it was assigned previously. If that address is unavailable or if no address in the pool was assigned previously, the NAS then assigns the next available address in its pool.

Command Modes
Interface configuration

Command History
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
The peer ip address forced command is used for point-to-point interfaces that support a link framing protocol such as PPP where the NAS will assign a peer IP address from an address pool as a result of the following conditions:

• The NAS is configured with a pool of network addresses at the interface supporting the peers (configured by use of the ip local-pool command).

• The NAS is configured to assign IP addresses to peers from a pool. A pool of IP addresses can be configured and applied at the interface by use of the ip address-pool command and the peer default ip address pool command or as a RADIUS server directive.

• The peer is configured to request an IP address from the NAS server (for example, as configured by use of the ip address negotiated command).

To force the NAS to allocate the next available IP address from the pool for the interface, use the peer ip address forced command. Any attempts to allocate a previously held IP address or a specifically requested IP address are suppressed; instead, the NAS allocates the next available IP address from the specified pool. This feature can be used to prevent users from obtaining the same IP address for each dial-in session.
Examples

The following example specifies that the interface will allocate the next available address from the pool whenever an address is requested from a pool:

```
interface Virtual-template 1
peer default ip address pool poolA poolB
peer ip address forced
```

The following example specifies that the interface will allow a peer to negotiate an IP address or will attempt to assign a previously assigned address:

```
interface Virtual-template 1
peer default ip address pool poolA poolB
no peer ip address forced
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address negotiated</td>
<td>Specifies that the IP address for a particular interface is obtained via PPP IPCP address negotiation.</td>
</tr>
<tr>
<td>ip address-pool</td>
<td>Enables an address pooling mechanism used to supply IP addresses to dial-in asynchronous, synchronous, or ISDN point-to-point interfaces.</td>
</tr>
<tr>
<td>ip local-pool</td>
<td>Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.</td>
</tr>
<tr>
<td>peer default ip address</td>
<td>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.</td>
</tr>
<tr>
<td>ppp</td>
<td>Starts an asynchronous connection using PPP when you want to connect from a remote node computer to an EXEC session on the access server and want to connect from the access server to a device on the network.</td>
</tr>
</tbody>
</table>
peer match aaa-pools

To specify that any IP address pool name supplied by authentication, authorization, and accounting (AAA) servers must also be present in the list of pool names specified in the peer default ip address pool interface configuration command, use the peer match aaa-pools command in interface configuration mode. To configure the software to use any pool name supplied by the AAA server (default configuration), use the no form of this command.

peer match aaa-pools

no peer match aaa-pools

Syntax Description

This command has no arguments or keywords.

Command Default

Command is disabled.

Command Modes

Interface configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(6)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command provides the ability to control or restrict the use of pool names supplied by AAA to only those pool names that are configured on the router. This ability is useful in cases where the AAA server and the router and its local configuration are controlled by different administrators, as would be the case for a wholesale dial supplier where the AAA servers are owned by individual customers.

When the peer match aaa-pools command is configured on an interface, the IP address pool names used are those specified in the local configuration as part of the peer default ip address command and the pool names supplied by the AAA server.

When the no peer match aaa-pools command is used, pool name selection is controlled by the AAA server, as follows: When the AAA server supplies a pool name, that is the only pool used. If AAA does not supply a pool name, then the normal IP default pool name processing is used as described in the peer default ip address command page.

Examples

The following example shows how to configure pool name restrictions in a Resource Pool Management (RPM) customer profile template:

```
template Word
    multilink max-fragments
    peer match aaa-pools
    peer default ip address pool poolA poolB
    ppp ipcp dns 10.1.1.1
resource-pool profile customer WORD
    source template Word
    aaa group-configuration AAA-group1
```
```plaintext
template user_direct
peer default ip address pool mypool
ppp authentication chap isdn-users
ppp multilink
```

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip local pool</strong></td>
<td>Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.</td>
</tr>
<tr>
<td><strong>peer default ip address</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>peer pool backup</strong></td>
<td>Directs the pool software to use the local pool name configured with the peer default ip address interface configuration command to supplement the pool names supplied by AAA.</td>
</tr>
<tr>
<td><strong>peer pool static</strong></td>
<td>Suppresses an attempt to load all dynamic pools from the AAA server when a missing pool name is encountered.</td>
</tr>
</tbody>
</table>
peer pool backup

To provide backup IP address pool names supplied by authentication, authorization, and accounting (AAA) with local pool names, use the **peer pool backup** command in interface configuration mode. To disable the local pool name backup feature, use the **no** form of this command.

```
peer pool backup

no peer pool backup
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
No backup IP address pool names are configured.

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)B</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The **peer pool backup** command is useful in large-scale dial-out environments with a large number of independently controlled AAA servers. Difficulties arise when the network access server (NAS) must provide IP address pool name resolution when a new pool is introduced by one of the AAA servers before that pool is set up on the NAS, or when an existing local pool becomes exhausted but the AAA server actually has other pools that would be acceptable as IP address sources.

The **peer pool backup** command uses the local pool names configured with the **peer default ip address pool** interface configuration command to supplement the pool names supplied by AAA. The problems of pool name resolution and exhaustion can be solved by configuring backup pool names on a per-interface basis using both the **peer default ip address pool** and **peer pool backup** interface configuration commands.

You may also configure local restrictions on the use of AAA-supplied pool names to a NAS-specified set by adding the **peer match aaa-pools** interface configuration command to the configuration. The **peer match aaa-pools** command specifies that any AAA-supplied pool name must match one of the pool names supplied with the **peer default ip address pool** command. See the “Examples” section for an example.
Examples

In the following example, the search order for backup pool names set by the `peer default ip address pool` command is pool1 then pool2. These pools will be used when the NAS cannot resolve a pool name or when an existing pool of IP addresses is exhausted.

```
interface Dialer1
  ip unnumbered FastEthernet0
  encapsulation ppp
dialer pool 1
dialer idle-timeout 3600
dialer-group 1
peer pool backup
peer default ip address pool pool1 pool2
no fair-queue
no cdp enable
ppp authentication chap
```

In the following example, assume that there is a AAA-supplied IP address pool named poolA. By adding the `peer match aaa-pools` command to the configuration, the AAA-supplied pool named poolA will not be used because it does not appear in the `peer default ip address pool` command; only the pools named pool1 and pool2 will be searched.

```
interface serial 1:23
  ip address 10.4.4.1 255.255.255.0
  encapsulation ppp
  ppp authentication chap
dialer-group 1
peer pool backup
peer match aaa-pools
peer default ip address pool pool1 pool2
isdn switch-type primary-5ess
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip local pool</code></td>
<td>Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.</td>
</tr>
<tr>
<td><code>peer default ip address</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>peer match aaa-pools</code></td>
<td>Specifies that any AAA-supplied pool name must match one of the pool names supplied with the <code>peer default ip address pool</code> command.</td>
</tr>
<tr>
<td><code>peer pool static</code></td>
<td>Suppresses an attempt to load all dynamic pools from a AAA server when a missing pool name is encountered.</td>
</tr>
</tbody>
</table>
peer pool static

To suppress an attempt to load all dynamic pools from an authentication, authorization, and accounting (AAA) server when a missing pool name is encountered, use the peer pool static command in interface configuration mode. To disable the suppression of dynamic pool loading and restore the normal dynamic pool loading behavior, use the no form of this command.

```plaintext
peer pool static
no peer pool static
```

### Syntax Description
This command has no arguments or keywords.

### Command Default
Dynamic pools are loaded.

### Command Modes
Interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)B</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This feature was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
The peer pool static command controls attempts by the pool software to load dynamic pools in response to a pool request from a specific interface. These dynamic pools are loaded at system startup and refreshed whenever a pool name not configured on the network access server (NAS) is specified for IP address allocation. Because the behavior of the NAS in response to a missing pool name can be changed using the peer pool backup interface configuration command, you may need to use the peer pool static command to control attempts to load all dynamic pools when the AAA-supplied pool name is not an existing local pool name. The peer pool static command provides a two-minute interval between attempts to download dynamic IP pools when a missing pool name is encountered.

### Examples
The following partial example shows how to disable loading dynamic pools using the peer pool static command:

```plaintext
aaa new-model
aaa authentication ppp default group radius
aaa authorization exec default group radius
aaa authorization network default group radius

! interface ATM0/0/0
no ip address
no ip directed-broadcast
no ip route-cache
no atm ilmi-keepalive
```
interface Virtual-Template1
  ip address 10.4.4.1 255.255.255.0
  encapsulation ppp
  ppp authentication chap
  no ip directed-broadcast
  peer pool static
  peer pool static
  peer default ip address pool pool3 pool4 pool5
  ip classless
  radius-server host 172.30.166.121
  radius-server key lab
  radius-server vsa send accounting
  radius-server vsa send authentication
  !
  ip local pool pool2 10.4.4.2
  ip local pool pool3 10.4.4.3
  ip local pool pool4 10.4.4.4
  ip local pool pool5 10.4.4.5

In this configuration, any attempt to load a dynamic pool name is suppressed; only the backup pool names defined by the **peer default ip address pool** command will be used.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip local pool</strong></td>
<td>Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.</td>
</tr>
<tr>
<td><strong>peer default ip address</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>peer pool backup</strong></td>
<td>Directs the pool software to use the local pool name configured with the <strong>peer default ip address pool</strong> interface configuration command to supplement the pool names supplied by AAA.</td>
</tr>
</tbody>
</table>
permission (dial peer voice)

To specify whether incoming or outgoing calls are permitted on the defined dial peer, use the permission command in dial peer voice configuration mode. To remove the specified permission, use the no form of this command.

    permission { orig | term | both | none }
    no permission { orig | term | both | none }

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>orig</th>
<th>This dial peer is permitted to originate calls. Thus, the access server can accept incoming calls from the dial peer.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>term</td>
<td>This dial peer is permitted to terminate calls. Thus, the access server can send outgoing calls to the dial peer.</td>
</tr>
<tr>
<td></td>
<td>both</td>
<td>This dial peer is permitted to originate and terminate calls. Both incoming and outgoing calls are permitted (default).</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td>No incoming or outgoing calls can be made to or from this dial peer.</td>
</tr>
</tbody>
</table>

Command Default
Both incoming and outgoing calls are permitted.

Command Modes
Dial peer voice configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(3)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
After a dial peer is associated with an incoming call, the permission is checked to determine whether incoming calls are permitted on the dial peer. If permission is not set to orig or both, the incoming call is blocked.

After a dial peer is matched for an outgoing call, the permission is checked to determine whether outgoing calls are permitted on the dial peer. If permission is not set to term or both, the outgoing call using this dial peer fails.

Note
The call may “rotary” to the next dial peer if the current dial peer does not have the huntstop command set.
Examples

The following example configures a dial peer and sets its permission to both originate and terminate calls:

dial-peer voice 526 pots
  answer-address 408526....
  corlist incoming list2
  direct-inward-dial
  permission both

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dial-peer voice</td>
<td>Enters dial-peer voice configuration mode and defines a remote VoIP dial peer.</td>
</tr>
</tbody>
</table>
pool-range

To assign a range of modems to a modem pool, use the **pool-range** command in modem-pool configuration mode. To remove the range of modems, use the **no** form of the command.

```
pool-range [tty] {modem1-modemN | x/y}

no pool-range [tty] {modem1-modemN | x/y}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tty</td>
<td>(Optional) Sets the range to terminal controller (TTY) lines.</td>
</tr>
<tr>
<td>modem1-modemN</td>
<td>Range of lines, which correspond to a range of modems or to a modem pool. A hyphen (-) is required between the two numbers. The range of modems you can choose from is equivalent to the number of modems in your access server that are not currently associated with another modem pool, up to a maximum of 48.</td>
</tr>
<tr>
<td>x/y</td>
<td>Slot/port numbers for an internal modem. A range of numbers is not accepted. The slash mark is required.</td>
</tr>
</tbody>
</table>

**Command Default**

Command is disabled. All modems are configured to be part of the system default modem pool.

**Command Modes**

Modem pool configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2P</td>
<td>This command was introduced on the Cisco AS5200 and Cisco AS5300.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For a complete description of modem pools and how they are configured on Cisco access servers, see the command page for the **modem-pool** command.

Replace the `modem1-modemN` arguments with the modem TTY line numbers that correspond with the range of modems you want in the modem pool. TTY line numbers start from 1, and they map to modem numbers that start from 0. For example, if you want to include modems 1/0 through 1/23 in a pool range, use the TTY line numbers 1 to 24. To verify the modem to TTY line numbering scheme, use the **show modem slot/port** command.

**Note**

MICA technologies modems and Microcom modems support incoming analog calls over ISDN PRI. However, only MICA modems support modem pooling for CT1 and CE1 configurations with channel-associated signaling.
Examples

The following example assigns modem TTY line numbers 30 to 50 to a modem pool. The Dialed Number Information Service (DNIS) number is set to 2000. The customers dialing 2000 are guaranteed access to 21 modems. The 22nd client to dial in is refused connectivity because the maximum number of allowable connections is exceeded.

```plaintext
modem-pool v90service
  pool-range 30-50
  called-number 2000 max-conn 21
  exit
```

The following configuration rejects the `pool-range 30` command, because modem TTY line 30 is already a member of the modem pool v90service, which was configured in the previous example. Each modem in the access server is automatically assigned to a unique TTY line. TTY line numbers are assigned according to your shelf, slot, or port hardware configuration.

```plaintext
modem-pool v34service
  pool-range tty 30

% TTY 30 is already in another pool.
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>called-number (modem pool)</td>
<td>Assigns a called party number to a pool of modems.</td>
</tr>
<tr>
<td>clear modempool-counters</td>
<td>Clears active or running counters associated with one or more modem pools.</td>
</tr>
<tr>
<td>modem-pool</td>
<td>Creates a new modem pool or specifies an existing modem pool, which allows you to physically or virtually partition your access server for dial-in and dial-out access.</td>
</tr>
<tr>
<td>show modem-pool</td>
<td>Displays the configuration and connection status for one or more modem pools.</td>
</tr>
</tbody>
</table>
port (global)

To enter the port configuration mode, use the port command in global configuration mode. To exit port configuration mode, use the no form of this command.

Cisco AS5400 with NextPort DFC

```plaintext
port {slot \ slot|port} [slot \ slot|port]
no port {slot \ slot|port} [slot \ slot|port]
```

Cisco AS5800 with Universal Port Card

```plaintext
port {shelf\slot \ shelf\slot|port} [shelf\slot \ shelf\slot|port]
no port {shelf\slot \ shelf\slot|port} [shelf\slot \ shelf\slot|port]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>slot</code></td>
<td>All ports on the specified slot. For the Cisco AS5400, slot values range from 0 to 7. Entering a second slot value will specify a range of slots.</td>
</tr>
<tr>
<td>`slot</td>
<td>port`</td>
</tr>
<tr>
<td>`shelf</td>
<td>slot`</td>
</tr>
<tr>
<td>`shelf</td>
<td>slot</td>
</tr>
</tbody>
</table>

### Command Default

Command is disabled.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(3)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `port` command helps you to enter the port configuration mode. The port configuration mode allows you to shut down or put individual ports or ranges of ports in busyout mode.
Examples

The following example shows how to enter port configuration mode on ports 1 to 18 to perform further tasks on the ports:

Router(config)# port 1/1 1/18
Router(config-port)# shutdown

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear port</td>
<td>Resets the port and clears any active calls to the port.</td>
</tr>
</tbody>
</table>
**port modem autotest**

To automatically and periodically perform a modem diagnostics test for modems inside the universal gateway or router, use the `port modem autotest` command in global configuration mode. To disable or turn off the modem autotest service, use the `no` form of this command.

```
port modem autotest [error threshold | minimum modems | time hh:mm [hours]]
```

```
no port modem autotest
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>error threshold</strong></td>
<td>Maximum modem error threshold. When the system detects this many errors with the modems, the modem diagnostics test is automatically triggered. Specify a threshold count from 3 to 50.</td>
</tr>
<tr>
<td><strong>minimum modems</strong></td>
<td>Minimum number of modems that will remain untested and available to accept calls during each test cycle. You can specify from 5 to 48 modems. The default is 6 modems on the Cisco AS5400. The range for the Cisco AS5800 is from 73 to 756.</td>
</tr>
<tr>
<td><strong>time hh:mm</strong></td>
<td>Time you want the modem autotest to begin. You must use the military time convention and a required colon (:) between the hours and minutes variables for this feature. For example, 1:30 p.m. is issued as 13:30.</td>
</tr>
<tr>
<td><strong>hours</strong></td>
<td>(Optional) Long-range time variable used to set the modem autotest more than one day in advance. The range of hours is from 1 hour to 168 hours. For example, if you want to run the test once per week, issue 168. There are 168 hours in one week.</td>
</tr>
</tbody>
</table>

**Command Default**

Modem diagnostics tests are disabled.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(1)XD</td>
<td>This command was introduced on the Cisco AS5400 as the <code>port modem autotest</code> command and replaced the <code>modem autotest</code> command for the NextPort dial feature card (DFC) only.</td>
</tr>
<tr>
<td>12.1(3)T</td>
<td>This command was implemented on the Cisco AS5400 and Cisco AS5800.</td>
</tr>
<tr>
<td>12.1(5)XM1</td>
<td>This command was implemented on the Cisco AS5350.</td>
</tr>
<tr>
<td>12.2(11)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.</td>
</tr>
</tbody>
</table>
Examples

The following example shows how to set the modem autotest to run once per week at 3:00 a.m. Additionally, the autotest activates if the system detects a modem error count higher than 40 errors.

Determine the current time set on the access server with the `show clock` EXEC command. In this example, the time and date set is 3:00 p.m., Monday, January 6, 2003:

```
Router# show clock
*15:00:01.031 EST Jan 06 2003
```

Enter global configuration mode and set the time you want the modem autotest to activate. In this example, the access server is configured to run the modem autotest at 3:00 a.m. and every 168 hours (week) thereafter:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# port modem autotest time 03:00 168
```

Configure the autotest to activate if the system detects a high modem error count. In this example, the autotest activates if the system detects a modem error count higher than 40 errors. For the list of modem errors that are monitored by the `modem autotest` command, see the `show modem call-stats` command.

```
Router(config)# port modem autotest error 40
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>modem autotest</strong></td>
<td>Automatically and periodically performs a modem diagnostics test for modems inside the access server or router.</td>
</tr>
<tr>
<td><strong>show clock</strong></td>
<td>Displays the system clock.</td>
</tr>
<tr>
<td><strong>show modem</strong></td>
<td>Displays a high-level performance report for all the modems or a single modem inside Cisco AS5200 and Cisco AS5300 access servers.</td>
</tr>
<tr>
<td><strong>show modem test</strong></td>
<td>Displays the modem test log.</td>
</tr>
</tbody>
</table>
To start an asynchronous connection using PPP, use the `ppp` command in EXEC mode.

```
ppp {/default | {remote-ip-address | remote-name} [@tacacs-server]} [/routing] negotiate
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/default</code></td>
<td>Makes a PPP connection when a default address has been configured. The slash mark is required.</td>
</tr>
<tr>
<td><code>remote-ip-address</code></td>
<td>IP address of the client workstation or PC. This parameter can be specified only if the line is set for dynamic addresses using the <code>async address dynamic</code> line configuration command.</td>
</tr>
<tr>
<td><code>remote-name</code></td>
<td>Name of the client workstation or PC. This parameter can be specified if the line is set for dynamic addresses using the <code>async address dynamic</code> line configuration command.</td>
</tr>
<tr>
<td><code>@tacacs-server</code></td>
<td>(Optional) IP address or IP host name of the TACACS server to which the user’s TACACS authentication request is sent. The at sign is required.</td>
</tr>
<tr>
<td><code>/routing</code></td>
<td>(Optional) Indicates that the remote system is a router and that routing messages should be exchanged over the link. The line must be configured for asynchronous routing using PPP encapsulation. The slash mark is required.</td>
</tr>
<tr>
<td><code>negotiate</code></td>
<td>Use PPP negotiated IP address.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you connect from a remote node computer to an EXEC session on the access server and want to connect from the access server to a device on the network, issue the `ppp` command.

If you specify an address for the TACACS server (either `/default` or `@tacacs-server`), the address must be the first parameter in the command after you type `ppp`. If you do not specify an address or enter the default keyword, you are prompted for an IP address or host name. You can enter the default keyword at this point.

To terminate a session, disconnect from the device on the network using the command specific to that device. Then, exit from the EXEC by using the `exit` command.

**Examples**

The following example shows a line that is in asynchronous mode using PPP encapsulation. The name of the computer (ntpc in this example) must be in the Domain Name System (DNS) so that it can be resolved to a real IP address. The computer must be running a terminal emulator program.

```
Router# ppp ntpc@server1
```
**ppp accm**

To specify the Asynchronous Control Character Map (ACCM) to be negotiated with a mobile station or sent to a peer in PPP outbound requests, use the *ppp accm* command in interface configuration mode. To restore the default state, use the *no* form of this command.

```
ppp accm hex-number
no ppp accm
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex-number</td>
<td>Specifies the initial value for the ACCM. The value must be a hexadecimal number in the range from 0x0 to 0xFFFFFFFF, where the bit positions from right to left correspond to the characters 0x00 through 0x1F. The default character map (0xA0000) escapes the characters represented by 0x11 (^Q, DC1, and X-on) and 0x13 (^S, DC3, and X-off).</td>
</tr>
</tbody>
</table>

**Note**

The leading 0x is not necessary when entering the *hex-number* argument, but is accepted by the software.

**Command Default**

0xA0000.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(3)XS</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2</td>
<td>This command was integrated into Cisco IOS Release 12.2.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The ACCM is a four octet hexadecimal number that is sent to a peer in a PPP outbound Config-Request packet, informing the peer of which characters need to be escaped during transmission of Asynchronous HDLC (AHDLC) frames containing control characters. The escaped characters set by the *ppp accm* command are useful for allowing data to pass uninterpreted through a network that would normally interpret the control sequences as a command.

For example, the ^Q and ^S characters are software flow control commands used by asynchronous modems to start and stop data transmissions. To allow these characters to be sent as part of a data stream and not be interpreted as control codes by intervening devices, the characters must be escaped, and the *ppp accm* command specifies which characters to use.

The TIA/EIA/IS-835-B requires that the PDSN propose an ACCM of 0x00000000. To be compliant with TIA/EIA/IS-835-B, *ppp accm 00000000* must be configured on the virtual template interface on Cisco PDSN.

The *ppp accm* command is meaningful only on asynchronous interfaces. If entered on other interface types, it will be ignored.
### Examples
In the following example, all characters can be transmitted intact to the receiver so that it is not necessary for the transmitter to escape anything:

```plaintext
interface async 0
capsulation ppp
ppp accm 0
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ppp authentication</strong></td>
<td>Specifies CHAP or PAP authentication.</td>
</tr>
</tbody>
</table>
**ppp acfc local**

To configure high-level data link control (HDLC) address and control field compression (ACFC) options in configuration requests, use the `ppp acfc local` command in interface configuration mode. To return the router to the default for ACFC handling, use the `no` form of this command.

```
ppp acfc local [request | forbid]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>request</td>
<td>The ACFC option is included in outbound configuration requests.</td>
</tr>
<tr>
<td>forbid</td>
<td>The ACFC option is not sent in outbound configuration requests, and requests from a peer to add the ACFC option are not accepted.</td>
</tr>
</tbody>
</table>

**Command Default**

ACFC handling is automatically selected based on the type of link, as follows: For asynchronous links, the router responds as if the `request` keyword were selected and the router includes the ACFC option in outbound configuration requests. For synchronous links, the router responds as if the `forbid` keyword were selected and the ACFC option is not sent out in configuration outbound requests and requests from a peer to add the ACFC option are not accepted.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(7)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)B</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)B.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command configures ACFC requests in outbound configuration requests. The `ppp acfc local` command allows ACFC handling to be disabled, thus allowing the HDLC framing and the protocol field to remain uncompressed.

Prior to the introduction of the `ppp acfc local` command, negotiation and use of ACFC was entirely dependent upon the link type (synchronous or asynchronous) and was not under the independent control of a system administrator, and this is still the default condition. The `ppp acfc local` command allows the system administrator to control over when PPP negotiates the HDLC ACFC options during initial LCP negotiations, and how the results of the PPP negotiation are applied.

**Note**

Using ACFC can result in minor gains in effective bandwidth because they reduce the amount of framing overhead for each packet. However, using ACFC changes the alignment of the network data in the frame, which in turn can impair the switching efficiency of the packets both at the local and remote ends of the connection. For these reasons, it is generally recommended that ACFC not be enabled without carefully considering the potential results.
The following example shows how to configure a router to exclude ACFC options from its configuration requests:

```sh
ppp acfc local forbid
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ppp acfc remote</code></td>
<td>Configures the ACFC option in configuration requests received from a remote peer.</td>
</tr>
<tr>
<td><code>ppp pfc remote</code></td>
<td>Configures the PFC option in configuration requests received from a remote peer.</td>
</tr>
<tr>
<td><code>ppp pfc local</code></td>
<td>Configures the PFC option in configuration requests.</td>
</tr>
</tbody>
</table>
ppp acfc remote

To configure how high-level data link control (HDLC) address and control field compression (ACFC) options in configuration requests are received from a remote peer, use the `ppp acfc remote` command in interface configuration mode. To return the router to the default for ACFC handling, use the `no` form of this command.

```
ppp acfc remote {apply | reject | ignore}

no ppp acfc remote
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>apply</td>
<td>ACFC options are accepted and ACFC may be performed on frames sent to the remote peer.</td>
</tr>
<tr>
<td>reject</td>
<td>ACFC options are explicitly ignored.</td>
</tr>
<tr>
<td>ignore</td>
<td>ACFC options are accepted, but ACFC is not performed on frames sent to the remote peer.</td>
</tr>
</tbody>
</table>

**Command Default**

ACFC handling is automatically selected based on the type of link, as follows: For asynchronous links, the router responds as if the `apply` keyword were selected and the router accepts ACFC options received from a remote peer and may perform ACFC on frames sent to the peer. For synchronous links, the router responds as if the `ignore` keyword were selected and ACFC options received from a remote peer are accepted, but ACFC is not performed on frames sent to the remote peer.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(7)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)B</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)B.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If ACFC is negotiated during PPP negotiation, Cisco routers may omit the HDLC header on links using HDLC encapsulation. This command allows ACFC handling to be disabled during PPP negotiation, thus allowing the HDLC framing and the protocol field to remain uncompressed.

Prior to the introduction of the `ppp acfc remote` command, negotiation and use of ACFC was entirely dependent upon the link type (synchronous or asynchronous) and was not under the independent control of a system administrator, and this is still the default condition. The `ppp acfc remote` command allows the system administrator control over when PPP negotiates the HDLC ACFC options during initial LCP negotiations, and how the results of the PPP negotiation are applied.
Using ACFC can result in minor gains in effective bandwidth because they reduce the amount of framing overhead for each packet. However, using ACFC changes the alignment of the network data in the frame, which in turn can impair the switching efficiency of the packets both at the local and remote ends of the connection. For these reasons, it is generally recommended that ACFC not be enabled without carefully considering the potential results.

**Examples**

The following example configures ACFC options received from a remote peer to be rejected:

```
ppp acfc remote reject
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp acfc local</td>
<td>Configures the ACFC option in configuration requests.</td>
</tr>
<tr>
<td>ppp pfc remote</td>
<td>Configures the PFC option in configuration requests received from a remote peer.</td>
</tr>
<tr>
<td>ppp pfc local</td>
<td>Configures the PFC option in configuration requests.</td>
</tr>
</tbody>
</table>
ppp bap call

To set PPP Bandwidth Allocation Protocol (BAP) call parameters, use the `ppp bap call` command in interface configuration mode. To disable processing of a specific type of incoming connection, use the `no` form of this command.

```
ppp bap call {accept | request | timer seconds}

no ppp bap call {accept | request | timer}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept</td>
<td>Peer initiates link addition. This is the default.</td>
</tr>
<tr>
<td>request</td>
<td>Local side initiates link addition.</td>
</tr>
<tr>
<td>timer seconds</td>
<td>Number of seconds to wait between call requests the router sends, in the range from 2 to 120 seconds. No default value is set.</td>
</tr>
</tbody>
</table>

### Command Default

Peers can initiate the addition of links to a multilink bundle; the timer is disabled.

### Command Modes

Interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command can be included in a virtual interface template for configuring virtual interfaces or can be used to configure a dialer interface.

### Examples

The following example configures a dialer interface to accept calls. Accepting calls is the default, but the command is included for the sake of the example.

```
interface dialer 1
ip unnumbered ethernet 0
encapsulation ppp
ppp multilink bap
ppp bap call accept
ppp bap link types isdn analog
dialer load threshold 30
ppp bap timeout pending 60
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp bap callback</td>
<td>Enables PPP BAP callback and set callback parameters.</td>
</tr>
<tr>
<td>ppp bap drop</td>
<td>Sets parameters for removing links from a multilink bundle.</td>
</tr>
<tr>
<td>ppp bap link types</td>
<td>Specifies the types of links that can be included in a specific multilink bundle.</td>
</tr>
</tbody>
</table>
ppp bap callback

To enable PPP Bandwidth Allocation Protocol (BAP) callback and set callback parameters, use the `ppp bap callback` command in interface configuration mode. To remove the PPP BAP callback configuration, use the `no` form of this command.

```
ppp bap callback {accept | request | timer seconds}

no ppp bap callback {accept | request | timer}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept</td>
<td>Local router initiates link addition upon peer notification.</td>
</tr>
<tr>
<td>request</td>
<td>Local router requests that a peer initiate link addition.</td>
</tr>
<tr>
<td>timer seconds</td>
<td>Number of seconds to wait between callback requests the router sends, in the range from 2 to 120 seconds. Disabled by default.</td>
</tr>
</tbody>
</table>

**Command Default**

Callback is disabled, and no callback parameters are set. The timer is disabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example configures a BRI interface for active mode BAP:

```
interface bri 0
   ip unnumbered ethernet 0
dialer load-threshold 10 either
dialer map ip 172.21.13.101 name bap-peer 14085778899
capsulation ppp
   ppp multilink bap
   ppp bap call request
   ppp bap callback accept
   no ppp bap call accept
   no ppp bap drop accept
   ppp bap pending timeout 30
   ppp bap number default 5664567
   ppp bap number secondary 5664568
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp bap drop</td>
<td>Sets parameters for removing links from a multilink bundle.</td>
</tr>
<tr>
<td>ppp bap link types</td>
<td>Specifies the types of links that can be included in a specific multilink bundle.</td>
</tr>
<tr>
<td>show ppp bap</td>
<td>Displays the configuration settings and run-time status for a multilink bundle.</td>
</tr>
</tbody>
</table>
**ppp bap drop**

To set parameters for removing links from a multilink bundle, use the `ppp bap drop` command in interface configuration mode. To disable a specific type of default processing, use the `no` form of this command.

```
ppp bap drop {accept | after-retries | request | timer seconds}
no ppp bap drop {accept | after-retries | request | timer}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept</td>
<td>Peer can initiate link removal. Enabled by default.</td>
</tr>
<tr>
<td>after-retries</td>
<td>Local router can remove the link without Bandwidth Allocation Protocol (BAP) negotiation when no response to the drop requests arrives.</td>
</tr>
<tr>
<td>request</td>
<td>Local router can initiate removal of a link. Enabled by default.</td>
</tr>
<tr>
<td>timer seconds</td>
<td>Number of seconds to wait between drop requests sent.</td>
</tr>
</tbody>
</table>

**Command Default**

- **accept, request**: Peers can initiate link removal and this router also can initiate link removal.
- **no ppp bap drop after-retries**: The link is not dropped when there is no response to drop requests.
- **timer**: Disabled, no default value is defined.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `no ppp bap drop accept` command disables the router’s ability to respond favorably to link drop requests from a peer. However, the router can still remove the link when it receives such requests.

The `no ppp bap drop after-retries` command is the default behavior; the `ppp bap drop after-retries` command must be entered explicitly to be effective.

The `no ppp bap drop request` command disables the router’s ability to send link drop requests to a peer. However, the peer can still remove the link on its own behalf; for example, when there is too little traffic to justify keeping the link up.

The `ppp bap max` command specifies the maximum number of requests and retries.

**Examples**

The following partial example sets a 60-second wait between drop requests:

```
ppp bap drop timer 60
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp bap max</td>
<td>Sets upper limits on the number of retransmissions for PPP BAP.</td>
</tr>
</tbody>
</table>
**ppp bap link types**

To specify the types of links that can be included in a specific multilink bundle, use the **ppp bap link types** command in interface configuration mode. To remove a type of interface that was previously allowed to be added, use the **no** form of this command.

```
ppp bap link types [isdn] [analog]
no ppp bap link types [isdn] [analog]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>isdn</th>
<th>(Optional) ISDN interfaces can be added to a multilink bundle. This is the default.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>analog</td>
<td>(Optional) Asynchronous serial interfaces can be added to a multilink bundle.</td>
</tr>
</tbody>
</table>

**Command Default**

ISDN interfaces are added to the multilink bundle (**isdn** keyword).

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The choice of keywords must suit the interfaces configured for Multilink PPP. For example, if you have configured a dialer rotary with only ISDN interfaces, only the **isdn** keyword would be appropriate. If the configuration allows both ISDN and asynchronous interfaces, both **isdn** and **analog** keywords could be used; the multilink bundle could then consist of both ISDN and asynchronous links. Bandwidth Allocation Protocol (BAP) dynamically determines which interfaces are applicable.

**Examples**

The following example configures a dialer interface for passive mode BAP and for both ISDN and asynchronous serial links:

```
interface dialer 1
  ip unnumbered ethernet 0
  encapsulation ppp
  ppp multilink bap
  ppp bap call accept
  ppp bap link types isdn analog
  dialer load threshold 30
  ppp bap timeout pending 60
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp bap callback</td>
<td>Enables PPP BAP callback and set callback parameters.</td>
</tr>
<tr>
<td>show ppp bap</td>
<td>Displays the configuration settings and run-time status for a multilink bundle.</td>
</tr>
</tbody>
</table>
**ppp bap max**

To set upper limits on the number of retransmissions for PPP Bandwidth Allocation Protocol (BAP), use the **ppp bap max** command in interface configuration mode. To remove any retry limit, use the **no** form of this command.

```
ppp bap max {dial-attempts number | ind-retries number | req-retries number | dialers number}
```

```
no ppp bap max {dial-attempts | ind-retries | req-retries | dialers number}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>dial-attempts</strong> <em>number</em></td>
<td>Maximum number of dial attempts to any destination number, in the range from 1 to 3. The default is one dial attempt.</td>
</tr>
<tr>
<td><strong>ind-retries</strong> <em>number</em></td>
<td>Maximum number of retries of a call status indication message, in the range from 1 to 10. The default is three indication retries.</td>
</tr>
<tr>
<td><strong>req-retries</strong> <em>number</em></td>
<td>Maximum number of retries for a particular request, in the range from 1 to 5. The default is three request retries.</td>
</tr>
<tr>
<td><strong>dialers</strong> <em>number</em></td>
<td>Maximum number of free dialers logged, in the range from 1 to 10. The default is five free dialers.</td>
</tr>
</tbody>
</table>

**Command Default**

1 dial attempt
3 indication retries
3 request retries
5 searches for free dialers

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

In compliance with RFC 2125, the **no** form of this command explicitly removes any status indication retry limit and is displayed in the router configuration.

The **ppp bap max dialers** command works in conjunction with the **dialer rotor** and **dialer priority** interface commands, which can be used to determine free dialers based upon the priority or the best available. Dialers include all interfaces that are configured under the dialer group leader (the dialer interface itself). The dialer group leader is displayed as the Master Interface in the **show ppp bap group** output.

BAP bases its link type and phone number decisions upon the ordering of the interfaces. This decision is suited to a mixed media environment of both ISDN and analog interfaces, where it may be desirable to choose the ISDN link over the asynchronous or vice versa.

Note that this decision also will limit the number of potential phone numbers that can be included in a CallResponse or CallbackRequest; the maximum number is limited to 20. For example, ten BRI interfaces with two numbers per interface.
**Examples**

The following partial example accepts the default number of attempts to dial a number and the default number of indication retries, but configures a limit of four times to send requests:

```
ppp bap max req-retries 4
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dialer priority</td>
<td>Sets the priority of an interface in a dialer rotary group.</td>
</tr>
<tr>
<td>dialer rotor</td>
<td>Specifies the method for identifying the outbound line to be used for ISDN or asynchronous DDR calls.</td>
</tr>
<tr>
<td>ppp bap drop</td>
<td>Sets parameters for removing links from a multilink bundle.</td>
</tr>
<tr>
<td>ppp bap monitor load</td>
<td>Validates peer requests to add or remove links against the current bundle load and the defined dialer load threshold.</td>
</tr>
<tr>
<td>ppp bap timeout</td>
<td>Specifies nondefault timeout values for PPP BAP pending actions and responses.</td>
</tr>
<tr>
<td>show ppp bap group</td>
<td>Displays the configuration settings and run-time status for a multilink bundle.</td>
</tr>
</tbody>
</table>
**ppp bap monitor load**

To validate peer requests to add or remove links against the current bundle load and the defined dialer load threshold, use the `ppp bap monitor load` command in interface configuration mode. To specify that incoming link addition requests are not to be subject to the bundle load threshold, use the `no` form of this command.

```
ppp bap monitor load
no ppp bap monitor load
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Command is enabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the load is being monitored and the incoming peer requests that a link be dropped when the current traffic load is above the dialer load (that is, there is enough traffic to justify the current number of links), the router will not drop the link. In addition, when the traffic falls below the threshold, Bandwidth Allocation Protocol (BAP) tries to drop a link.

The `no` form of this command indicates that incoming peer requests to add a link are not subject to the bundle load threshold. However, other criteria must be met before a favorable response is sent.

**Examples**

The following partial example configures BAP not to validate peer requests against the current bundle load and the configured dialer load threshold:

```
no ppp bap monitor load
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dialer load-threshold</code></td>
<td>Configures bandwidth on demand by setting the maximum load before the dialer places another call to a destination.</td>
</tr>
</tbody>
</table>
ppp bap number

To specify a local telephone number that peers can dial to establish a multilink bundle, use the **ppp bap number** command in interface configuration mode. To remove a previously configured number, use the **no** form of this command.

```
ppp bap number { default phone-number | secondary phone-number | prefix prefix-number | format { national | subscriber } }

no ppp bap number { default phone-number | prefix prefix-number | format { national | subscriber } }
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>default phone-number</strong></td>
<td>Primary (base) phone number for the interface and the number that can be used for incoming dial calls.</td>
</tr>
<tr>
<td><strong>secondary phone-number</strong></td>
<td>Telephone number for the second B channel. Applies only to BRI interfaces that have a different number for each B channel or to dialer interfaces that are BRIs.</td>
</tr>
<tr>
<td><strong>prefix prefix-number</strong></td>
<td>Prefix number for the PPP phone number.</td>
</tr>
<tr>
<td>**format national</td>
<td>subscriber**</td>
</tr>
<tr>
<td></td>
<td>• Ten-digit number for a national format.</td>
</tr>
<tr>
<td></td>
<td>• Seven-digit number for a subscriber format.</td>
</tr>
</tbody>
</table>

### Command Default

No base number is provided.

### Command Modes

Interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.3T</td>
<td>The <strong>prefix</strong> and <strong>format</strong> keywords were added.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to supply a local default number to be exchanged between peers in order to establish a multilink bundle.

This command is applicable on both the dialer interface and the individual physical interfaces.

If a peer requests that a number be supplied and no PPP Bandwidth Allocation Protocol (BAP) default number is defined, it might not be possible for the peer to access the interface. However, the peer can access the interface if it has the number already or the number it dialed originally is the same as the number for establishing a Multilink PPP (MLP) bundle.
During BAP negotiations between peers, the called party indicates the number to call for BAP if it is different from the number the peer originally dialed. The called party responds with information about the phone number *delta* (the changes to be made in the right-most digits dialed). This information indicates the number of digits that are different from the number originally dialed and what those digits should be.

For example, if the remote peer dialed 5550159876, and the **ppp bap number** command had the default number 5550159912, the local router would respond “3 | 912.” In the response, a vertical bar (|) is used to divide the number of digits to change from the number sequence to use instead. In the “3 | 912” response, the local router instructs the calling interface to replace the right-most three digits with “912” for BAP.

This command is used by the client side for dialing instructions when communicating with the server. Use the **prefix** keyword on the Always On/Dynamic ISDN (AO/DI) client side to specify what will precede any number dialed to a multilink peer. For example, the client issues a call request to the server whereby the server issues a call response that includes the dialing number the client should use and the format this number should be in (national or subscriber). The client then dials the number supplied by the server, preceded by any prefix information contained in the **ppp bap number prefix** command. Figure 1 shows an overview about the information exchange between the client and the server.

**Figure 1**  
*Client and Server Response Sequence*

Use the **format** keyword on the AO/DI server side to specify how many digits should be returned by BAP. BAP will return the numbers based on either a national or subscriber format. The value that is returned is preceded by the prefix before dialing occurs. For example, if the **format national** keywords are configured, then the national format (which is equivalent to ten digits) is returned (during BAP negotiation) from the server.

The **ppp bap number prefix** and **ppp bap number format** keyword options cannot be combined to a single-string command line; they must be entered in two separate command strings.

**Examples**

In the following example, the AO/DI client uses a **ppp bap prefix** value of 9, which indicates that the dialed number of 5550134 will be preceded by a 9. The number that is actually dialed is 95550134. The AO/DI server uses a subscriber format, which indicates that when the client asks the server for the numbers to dial, BAP will return seven digits.
Client Router
interface dialer1
ppp bap number prefix 9

Server Router
interface dialer1
ppp bap number format subscriber
ppp bap number default 5550134

In the following example, the AO/DI client uses a **ppp bap prefix** value of 1, which indicates that the dialed number of 5550178 will be preceded by a 1. The number that is actually dialed is 19195550178 because the server is using a national format, and BAP therefore, returns ten digits.

Client Router
interface dialer1
ppp bap number prefix 1

Server Router
interface dialer1
ppp bap number format national
ppp bap number default 9195550178

The following example configures a physical interface with both a default number and a secondary number:

```
interface bri 0
ip unnumbered ethernet 0
dialer load-threshold 10 either
dialer map ip 172.21.13.101 name bap-peer 14085550199
encapsulation ppp
ppp multilink bap
ppp bap call request
ppp bap callback accept
no ppp bap call accept
no ppp bap drop accept
ppp bap pending timeout 30
ppp bap number default 5550167
ppp bap number secondary 5550168
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ppp bap callback</strong></td>
<td>Enables PPP BAP callback and set callback parameters.</td>
</tr>
<tr>
<td><strong>show ppp bap</strong></td>
<td>Displays the configuration settings and run-time status for a multilink bundle.</td>
</tr>
</tbody>
</table>
To specify nondefault timeout values for PPP Bandwidth Allocation Protocol (BAP) pending actions and responses, use the `ppp bap timeout` command in interface configuration mode. To reset the response timeout to the default value, or to remove a pending timeout entirely, use the `no` form of this command.

```
ppp bap timeout {pending seconds | response seconds}
no ppp bap timeout {pending | response}
```

**Syntax Description**

- `pending seconds`: Number of seconds to wait before timing out pending actions, in the range from 2 to 180 seconds. The default is 20 seconds.
- `response seconds`: Number of seconds to wait for a response before timing out, in the range from 2 to 120 seconds. The default is 3 seconds.

**Command Default**

- Enabled
  - `pending`: 20 seconds
  - `response`: 3 seconds

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `no ppp bap timeout response` command resets the timer to the default value. The `no ppp bap timeout pending` command removes the pending-action timeout entirely (in compliance with the BAP specification).

**Examples**

The following example configures BAP to wait 45 seconds before timing out pending actions:

```
interface dialer 1
  ip unnumbered ethernet 0
  encapsulation ppp
  ppp multilink bap
  ppp bap call accept
  ppp bap link types isdn analog
  dialer load threshold 30
  ppp bap timeout pending 45
```
ppp bap timeout

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ppp bap callback</strong></td>
<td>Enables PPP BAP callback and set callback parameters.</td>
</tr>
<tr>
<td><strong>ppp bap drop</strong></td>
<td>Sets parameters for removing links from a multilink bundle.</td>
</tr>
<tr>
<td><strong>ppp bap max</strong></td>
<td>Sets upper limits on the number of retransmission for PPP BAP.</td>
</tr>
<tr>
<td><strong>show ppp bap</strong></td>
<td>Displays the configuration settings and run-time status for a multilink bundle.</td>
</tr>
</tbody>
</table>
**ppp bridge appletalk**

To enable half-bridging of AppleTalk packets across a serial interface, use the `ppp bridge appletalk` command in interface configuration mode. To disable AppleTalk packet half-bridging, use the `no` form of this command.

```
ppp bridge appletalk

no ppp bridge appletalk
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Command is disabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you configure a serial or ISDN interface for half-bridging, you configure it to function as a node on an Ethernet subnetwork. It communicates with a bridge on the subnetwork by sending and receiving bridge packets. The serial or ISDN interface converts bridge packets to routed packets and forwards them, as needed.

The serial interface must be configured with an AppleTalk address for communication on the Ethernet subnetwork, and the AppleTalk address must have the same AppleTalk cable range as the bridge.

You cannot configure a serial interface for both half-bridging and for transparent bridging. No more than one half-bridge should be on any subnetwork.

**Examples**

The following example configures serial interface 0 for half-bridging of AppleTalk. The remote bridge and other Ethernet nodes must be on the same network.

```
interface serial 0
ppp bridge appletalk
appletalk cable-range 301-301
appletalk zone remote-lan
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>appletalk cable-range</td>
<td>Enables an extended AppleTalk network.</td>
</tr>
<tr>
<td>appletalk zone</td>
<td>Sets the zone name for the connected AppleTalk network.</td>
</tr>
<tr>
<td>ppp bridge ip</td>
<td>Enables half-bridging of IP packets across a serial interface.</td>
</tr>
<tr>
<td>ppp bridge ipx</td>
<td>Enables half-bridging of IPX packets across a serial interface.</td>
</tr>
</tbody>
</table>
**ppp bridge ip**

To enable half-bridging of IP packets across a serial interface, use the **ppp bridge ip** command in interface configuration mode. To disable IP packet half-bridging, use the **no** form of this command.

```
ppp bridge ip
no ppp bridge ip
```

**Syntax Description** This command has no arguments or keywords.

**Command Default** Command is disabled.

**Command Modes** Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines** When you configure a serial or ISDN interface for half-bridging, you configure it to function as a node on an Ethernet subnetwork. It communicates with a bridge on the subnetwork by sending and receiving bridge packets. The serial interface converts bridge packets to routed packets and forwards them, as needed.

The interface must be configured with an IP address for communication on the Ethernet subnetwork, and the IP address must be on the same subnetwork as the bridge.

You cannot configure a serial interface for both half-bridging and for transparent bridging.

No more than one half-bridge should be on any subnetwork.

**Examples**

The following example configures serial interface 0 for half-bridging of IP. The remote bridge and other Ethernet nodes must be on the same subnetwork.

```
interface serial 0
ip address 172.19.5.8
ppp bridge ip
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Sets a primary or secondary IP address for an interface.</td>
</tr>
<tr>
<td>ppp bridge appletalk</td>
<td>Enables half-bridging of AppleTalk packets across a serial interfaces.</td>
</tr>
<tr>
<td>ppp bridge ipx</td>
<td>Enables half-bridging of IPX packets across a serial interfaces.</td>
</tr>
</tbody>
</table>
**ppp bridge ipx**

To enable half-bridging of Internetwork Packet Exchange (IPX) packets across a serial interface, use the `ppp bridge ipx` command in interface configuration mode. To return to the default Novell Ethernet_802.3 encapsulation, use the `no` form of this command.

```
ppp bridge ipx [novell-ether | arpa | sap | snap]
no ppp bridge ipx
```

**Syntax Description**

- `novell-ether` (Optional) Novell Ethernet_802.3 encapsulation. This is the default.
- `arpa` (Optional) Novell Ethernet_II encapsulation.
- `sap` (Optional) Novell Ethernet_802.2 encapsulation.
- `snap` (Optional) Novell Ethernet_Snap encapsulation.

**Command Default**
The default encapsulation is `novell-ether`.

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you configure a serial interface for half-bridging, you configure it to function as a node on an Ethernet subnetwork. It communicates with a bridge on the subnetwork by sending and receiving bridge packets. The serial interface converts bridge packets to routed packets and forwards them, as needed.

The serial interface must be configured with an IPX address for communication on the Ethernet subnetwork, and the IPX address must be on the same subnetwork as the bridge.

You cannot configure a serial interface for both half-bridging and for transparent bridging.

No more than one half-bridge should be on any subnetwork.

**Examples**

The following example configures serial interface 0 for half-bridging of IPX. The remote bridge and other Ethernet nodes must be on the same subnetwork.

```
interface serial 0
ppp bridge ipx
ipx network 1800
```
### Dial Commands

**ppp bridge ipx**

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>ipx network</strong></td>
<td>Enables IPX routing on a particular interface and optionally selects the type of encapsulation (framing).</td>
</tr>
<tr>
<td></td>
<td><strong>ppp bridge appletalk</strong></td>
<td>Enables half-bridging of AppleTalk packets across a serial interfaces.</td>
</tr>
<tr>
<td></td>
<td><strong>ppp bridge ip</strong></td>
<td>Enables half-bridging of IP packets across a serial interfaces.</td>
</tr>
</tbody>
</table>
ppp callback (DDR)

To enable a dialer interface to function either as a callback client that requests callback or as a callback server that accepts callback requests, use the **ppp callback** command in interface configuration mode. To disable a function, use the **no** form of this command.

```
ppp callback {accept | permit | request}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>accept</th>
<th>Dialer interface accepts PPP callback requests (and functions as the PPP callback server).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax Description</td>
<td>permit</td>
<td>Dialer interface permits PPP callback (and functions as the PPP callback client).</td>
</tr>
<tr>
<td>Syntax Description</td>
<td>request</td>
<td>Dialer interface requests PPP callback (and functions as the PPP callback client).</td>
</tr>
</tbody>
</table>

**Command Default**
Callback requests are neither accepted nor requested.

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
An interface can request PPP callback only if the interface is configured for PPP authentication with Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).

If an interface of the callback server is configured with **ppp callback accept** and the client attempts to cancel the callback and connect, Cisco IOS software will refuse the request and disconnect the client.

If a client is allowed to cancel callbacks and connects, the **ppp callback permit** command must be used instead of the **ppp callback accept** command on the callback server interface.

**Examples**
The following example configures a previously defined dialer interface to accept PPP callback requests:

```
ppp callback accept
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>dialer callback-secure</strong></td>
<td>Enables callback security.</td>
</tr>
<tr>
<td><strong>map-class dialer</strong></td>
<td>Defines a class of shared configuration parameters associated with the <strong>dialer map</strong> command for outgoing calls from an ISDN interface and for PPP callback.</td>
</tr>
<tr>
<td><strong>ppp callback (PPP client)</strong></td>
<td>Enables a PPP client to dial in to an asynchronous interface and request a callback.</td>
</tr>
</tbody>
</table>
ppp callback (PPP client)

To enable a PPP client to dial in to an asynchronous interface and request a callback, use the `ppp callback` command in interface configuration mode. To disable callback acceptance, use the `no` form of this command.

```
ppp callback {accept | initiate}
```

```
o ppp callback
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>accept</code></td>
<td>Accept callback requests from RFC 1570-compliant PPP clients on the interface.</td>
</tr>
<tr>
<td><code>initiate</code></td>
<td>Initiate a callback to non-RFC 1570-compliant PPP clients dialing in to an asynchronous interface.</td>
</tr>
</tbody>
</table>

**Command Default**

Callback requests are not accepted on asynchronous interfaces.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

PPP callback can be initiated only if the interface is configured for authentication using CHAP or PAP.

**Examples**

The following example accepts a callback request from an RFC-compliant PPP client:

```
ppp callback accept
```

The following example accepts a callback request from a non-RFC-compliant PPP client:

```
ppp callback initiate
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>arap callback</code></td>
<td>Enables an ARA client to request a callback from an ARA client.</td>
</tr>
<tr>
<td><code>autoselect ppp</code></td>
<td>Configures a line to start a SLIP session.</td>
</tr>
<tr>
<td><code>call progress tone country</code></td>
<td>Forces the Cisco IOS software to wait before initiating a callback to a requesting client.</td>
</tr>
<tr>
<td><code>ppp authentication</code></td>
<td>Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ppp callback (DDR)</td>
<td>Enables a dialer interface to function either as a callback client that</td>
</tr>
<tr>
<td></td>
<td>requests callback or as a callback server that accepts callback requests.</td>
</tr>
<tr>
<td>username</td>
<td>Establishes a username-based authentication system, such as PPP CHAP and</td>
</tr>
<tr>
<td></td>
<td>PAP.</td>
</tr>
</tbody>
</table>
**ppp caller name**

To set the caller option when no Calling Line Identification (CLID) is available, use the **`ppp caller name`** command in interface configuration mode. To remove the name, use the **`no`** form of this command.

```
ppp caller name name
no ppp caller name name
```

**Syntax Description**

| `name` | Username string for this call. |

**Command Default**

Command is disabled by default.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command sets the username used when the CLID is not available. This username is used only in the case where the **`ppp dnis`** command is configured and the CLID is not available.

**Examples**

The following example shows how to configure a call to user1:

```
interface Serial0:15
description "PRI D channel"
ip unnumbered Loopback0
encapsulation ppp
no keepalive
dialer pool-member 1 max-link 1
isdn switch-type primary-net5
isdn incoming-voice modem
no fair-queue
no cdp enable
ppp caller name user1
ppp authentication pap chap callin USERS&TUNNELS
ppp chap hostname osh
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong><code>ppp dnis</code></strong></td>
<td>Sets the DNIS string for a PPP call.</td>
</tr>
</tbody>
</table>
**ppp direction**

To override the default direction of a PPP connection, use the `ppp direction` command in interface configuration mode. To disable an override setting, use the `no` form of this command.

```
ppp direction {callin | callout | dedicated}

no ppp direction {callin | callout | dedicated}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>callin</td>
<td>Treat the connection as a received call.</td>
</tr>
<tr>
<td>callout</td>
<td>Treat the connection as an initiated call.</td>
</tr>
<tr>
<td>dedicated</td>
<td>Treat the connection as a dedicated call.</td>
</tr>
</tbody>
</table>

**Defaults**

Disabled (no direction configured)

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ppp direction` command is useful when a router is connected to an interface type where there is either no inherent call direction, such as with a back-to-back or leased-line connection, or where an external dial device such as a CSU/DSU or an ISDN terminal adapter is connected to the interface.

The configured call direction will always override the automatically detected direction, even on dial interfaces where the true direction is known.

The call direction is used mainly internally by PPP authentication, as follows:

- If doing bidirectional authentication, PPP will wait to send its authentication credentials to the peer if the direction is call-in, and the `no ppp chap wait`, `no ppp pap wait`, or `no ppp eap wait` commands are not configured.
- PPP uses the call direction internally to detect spoofed Challenge Handshake Authentication Protocol (CHAP) sessions.
- If the direction is call-in, PPP requires that the remote names used in a peer’s CHAP challenge and CHAP response be the same.

The call direction is also used for callback processing.

Typically, you will not need to configure this command. If you do, you should configure the opposite of the command on the other side of the link, so one side is call-out and one side is call-in.
Examples

The following example determines the call direction on a back-to-back serial connection:

```
interface Serial2/0
ip address 192.168.1.131 255.255.255.0
encapsulation ppp
peer default ip address pool local local_pool
serial restart-delay 0
ppp authentication chap
ppp direction callin
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp chap wait</td>
<td>Configures the router to delay the CHAP authentication until after the peer has authenticated itself to the router.</td>
</tr>
<tr>
<td>ppp eap wait</td>
<td>Configures the router to delay the EAP authentication until after the peer has authenticated itself to the server.</td>
</tr>
<tr>
<td>ppp pap wait</td>
<td>Configures the router to delay the PAP authentication until after the peer has authenticated itself to the router.</td>
</tr>
</tbody>
</table>
ppp dnis

To configure a set of dialed number identification service (DNIS) numbers to check an incoming call against to automatically authenticate and authorize a user, use the `ppp dnis` command in interface configuration mode. To remove the numbers, use the `no` form of this command.

```
ppp dnis DNIS-number [DNIS-number] [DNIS-number...]
```

- **Syntax Description**
  - `DNIS-number` Specifies the DNIS number that will be checked when a call comes in. Multiple DNIS numbers can be entered separated by spaces.

- **Command Default**
  - This command is disabled by default.

- **Command Modes**
  - Interface configuration

- **Command History**
  - Release Modification
    - 12.2T This command was introduced.

- **Usage Guidelines**
  - This command enables a method of authenticating and authorizing a user based on the DNIS. The DNIS is the number dialed by the user. If the dialed number for this session matches one of the numbers configured in the `ppp dnis` command, the user is automatically authenticated and authorized for the session. Any other configured PPP authentication is not performed. In the case of DNIS authentication, the Calling Line Identification (CLID) is used as the username. If the CLID is unavailable, the username is the name configured with the `ppp caller name` command. If neither the CLID nor a caller name is configured, the username will automatically be set to "no-clid."

- **Examples**
  - The following example shows how to set the DNIS for a call:
    ```
    interface Serial0:15
    description "PRI D channel"
    ip unnumbered Loopback0
    encapsulation ppp
    no keepalive
    dialer pool-member 1 max-link 1
    isdn switch-type primary-net5
    isdn incoming-voice modem
    no fair-queue
    no cdp enable
    ppp dnis 13693 132
    ppp authentication pap chap callin USERS&TUNNELS
    ppp chap hostname osh
    ```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ppp caller name</code></td>
<td>Sets the caller option when no CLID is available.</td>
</tr>
</tbody>
</table>
**ppp encrypt mppe**

To enable Microsoft Point-to-Point Encryption (MPPE) on the virtual template, use the **ppp encrypt mppe** command in interface configuration mode. To disable MPPE, use the **no** form of this command.

```
ppp encrypt mppe [auto | 40 | 128] [passive | required] [stateful]
```

```
no ppp encrypt mppe
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>auto</th>
<th>All available encryption strengths are allowed.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>40</td>
<td>Only 40-bit encryption is allowed.</td>
</tr>
<tr>
<td></td>
<td>128</td>
<td>Only 128-bit encryption is allowed.</td>
</tr>
<tr>
<td>passive</td>
<td></td>
<td>(Optional) MPPE will not offer encryption, but will negotiate if the other tunnel endpoint requests encryption.</td>
</tr>
<tr>
<td>required</td>
<td></td>
<td>(Optional) MPPE must be negotiated, or the connection will be terminated.</td>
</tr>
<tr>
<td>stateful</td>
<td></td>
<td>(Optional) MPPE will negotiate only stateful encryption. If the stateful keyword is not used, MPPE will first attempt to negotiate stateless encryption, but will allow stateful mode if the other tunnel endpoint requests it.</td>
</tr>
</tbody>
</table>

**Command Default**

MPPE encryption is disabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)XE5</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(5)T</td>
<td>This command was integrated into Cisco IOS Release 12.1(5)T.</td>
</tr>
<tr>
<td>12.4(5)</td>
<td>This command was modified to explicitly disallow interleaving.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

PPP encapsulation must be enabled before you can use the **ppp encrypt mppe** command.

All of the configurable MPPE options must be identical on both tunnel endpoints.

The **auto** keyword is offered only on 128-bit images.

**Note**

The **ppp authentication ms-chap** command must be added to the interface that will carry Point-to-Point Tunnel Protocol (PPTP)-MPPE traffic. All Windows clients using MPPE need the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) application. This is a Microsoft design requirement.

Stateful encryption is not appropriate for links that have high loss rates because the state information is updated with each packet received, but cannot be updated correctly for packets that are not received. Losing a packet means loss of state (transmissions are no longer synchronous). Losing state triggers expensive resynchronization mechanisms, and more packets will be lost during the recovery period. Any link that experiences more than the occasional random drop is therefore unsuitable for stateful
encryption mechanisms. The same is also true for stateful compressions. For this reason, stateful encryption may not be appropriate for lossy network environments such as Layer 2 tunnels on the Internet.

The interleaving of packets among fragments of larger packets on a Multilink PPP (MLP) bundle (enabled with the `ppp multilink interleave` command) is not supported with this command.

**Examples**

The following example shows a virtual template configured to perform 40-bit MPPE encryption:

```plaintext
interface Virtual-Template1
  ip unnumbered FastEthernet0/0
  no ip directed-broadcast
  ip mroute-cache
  no keepalive
  ppp encrypt mppe 40
  ppp authentication ms-chap
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>encryption mppe</code></td>
<td>Enables MPPE encryption on the ISA card.</td>
</tr>
<tr>
<td><code>interface virtual-template</code></td>
<td>Creates a virtual template interface.</td>
</tr>
<tr>
<td><code>ppp authentication</code></td>
<td>Enables CHAP, PAP, MS-CHAP, or a combination of methods and specifies the order in which the authentication methods are selected on the interface.</td>
</tr>
<tr>
<td><code>ppp multilink interleave</code></td>
<td>Enables interleaving of packets among the fragments of larger packets on an MLP bundle.</td>
</tr>
</tbody>
</table>
ppp hold-queue

To specify the maximum number of packets to be queued to the PPP process across all interfaces, use the `ppp hold-queue` command in global configuration mode. To restore the default values, use the `no` form of this command.

`ppp hold-queue length`

`no ppp hold-queue`

Syntax Description

<table>
<thead>
<tr>
<th>Command Default</th>
<th>The number of packets to be queued. Values are from 1 to 1000000.</th>
</tr>
</thead>
</table>

Command Default

The default length depends on the platform. That is, the default length is twice the maximum number of PPP-supported interfaces on that platform.

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(15)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The exact value of the packets queued depends on the number of PPP sessions supported. The default value works in most cases. It is not recommended to set a different value unless your Cisco technical support representative directs you to do so for deployment-specific tuning purposes.

The command specifies that only packets that are actually queued are counted; packets that are discarded at interrupt because they do not pass various checks are not counted. Preprocessed packets are also not counted. Any type of packet queued to the PPP process is counted.

Examples

The following example shows how to specify the maximum number of packets to be queued to the PPP process:

```
Router(config)# ppp hold-queue 64000
```
ppp ipcp

To configure PPP IP Control Protocol (IPCP) features such as the ability to provide primary and secondary Domain Name Server (DNS) and Windows Internet Naming Service (WINS) server addresses, and the ability to accept any address requested by a peer, use the `ppp ipcp` command in template or interface configuration mode. To disable a `ppp ipcp` feature, use the `no` form of this command.

```
ppp ipcp {accept-address | address {accept | required | unique} | dns {primary-ip-address [secondary-ip-address] [aaa] [accept] [reject] [request [accept]]} | header-compression ack | ignore-map | mask {subnet-mask | reject | request} | username unique | wins {primary-ip-address [secondary-ip-address] [aaa] [accept] [reject] [request | reject | request [accept]]} }

no ppp ipcp {accept-address | address {accept | required | unique} | dns | header-compression ack | ignore-map | mask | predictive | username unique | wins}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>accept-address</strong></td>
<td>Accepts any nonzero IP address from the peer.</td>
</tr>
<tr>
<td><strong>address</strong></td>
<td>Specifies IPCP IP address options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>accept</strong>—Accepts any nonzero IP address from the peer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>required</strong>—Disconnects the peer if no IP address is negotiated.</td>
</tr>
<tr>
<td></td>
<td>• <strong>unique</strong>—Disconnects the peer if the IP address is already in use.</td>
</tr>
<tr>
<td><strong>dns</strong></td>
<td>Specifies DNS options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>primary-ip-address</strong>—IP address of the primary DNS server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>secondary-ip-address</strong>—(Optional) IP address of the secondary DNS server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>aaa</strong>—(Optional) Use DNS data from the AAA server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>accept</strong>—(Optional) Specifies that any nonzero DNS address will be accepted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>accept</strong>—Specifies that any nonzero DNS address will be accepted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>reject</strong>—Reject the IPCP option if received from the peer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>request</strong>—Request the DNS address from the peer.</td>
</tr>
<tr>
<td><strong>header-compression ack</strong></td>
<td>Enables IPCP header compression.</td>
</tr>
<tr>
<td><strong>ignore-map</strong></td>
<td>Ignores dialer map when negotiating peer IP address.</td>
</tr>
<tr>
<td><strong>mask</strong></td>
<td>Specifies IP address mask options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>subnet-mask</strong>—Specifies the subnet mask to offer the peer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>reject</strong>—Reject subnet mask negotiations.</td>
</tr>
<tr>
<td></td>
<td>• <strong>request</strong>—Request the subnet mask from the peer.</td>
</tr>
</tbody>
</table>
### username unique
Ignored a common username when providing an IP address to the peer.

### wins
Specifies WINS options:
- **primary-ip-address**—IP address of the primary WINS server.
- **secondary-ip-address**—(Optional) IP address of the secondary WINS server.
- **aaa**—(Optional) Use WINS data from the AAA server.
- **accept**—(Optional) Specifies that any nonzero WINS address will be accepted.
- **accept**—Specifies that any nonzero WINS address will be accepted.
- **reject**—Reject the IPCP option if received from the peer.
- **request**—Request the WINS address from the peer.

### Command Default
No servers are configured, and no address request is made.

### Command Modes
- Template configuration
- Interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(6)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(5)T</td>
<td>The <strong>reject</strong> and <strong>accept</strong> keywords were added.</td>
</tr>
</tbody>
</table>

### Examples
The following examples show use of the **ppp ipcp** command:

```plaintext
ppp ipcp accept-address
ppp ipcp dns 10.1.1.3
ppp ipcp dns 10.1.1.3 10.1.1.4
ppp ipcp dns 10.1.1.1 10.1.1.2 accept
ppp ipcp dns accept
ppp ipcp dns reject
ppp ipcp ignore-map
ppp ipcp username unique
ppp ipcp wins 10.1.1.1 10.1.1.2
ppp ipcp wins accept
```

The following examples show how to use the **no** form of the **ppp ipcp** command:

```plaintext
no ppp ipcp wins
no ppp ipcp ignore-map
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ppp</code></td>
<td>Displays information on traffic and exchanges in an internetwork implementing the PPP.</td>
</tr>
<tr>
<td><code>show interfaces</code></td>
<td>Displays statistics for all interfaces configured on the router or access server.</td>
</tr>
<tr>
<td><code>show ip interfaces</code></td>
<td>Displays the usability status of interfaces configured for IP.</td>
</tr>
</tbody>
</table>
ppp ipcp default route

To configure a default route through a PPP virtual access interface, use the **ppp ipcp default route** command in interface configuration mode. To disable a default route for a PPP virtual access interface, use the **no** form of this command.

```
ppp ipcp default route

no ppp ipcp default route
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
No default route

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>T2.3(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command allows a PPP virtual template to dynamically add a default route pointing to the virtual access interface created by the virtual template.

A customer premises equipment (CPE) router with PPP over an ATM or Frame Relay connection can access the Internet without turning on any other routing.

**Examples**
The following example shows how to configure the PPP default route on the virtual access interface:

```
interface virtual-template 1
ip address negotiated
ppp ipcp default route
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>debug ppp negotiation</strong></td>
<td>Displays information on traffic and exchanges in an internetwork implementing PPP.</td>
</tr>
</tbody>
</table>
**ppp ipcp predictive**

To set the PPP Internet Protocol Control Protocol (IPCP) to a predictive state that reduces negotiation time by predicting responses from peers and sending expected reply and request packets in advance, use the **ppp ipcp predictive** command in interface configuration mode. To disable the IPCP predictive state, use the **no** form of this command.

```
ppp ipcp predictive
no ppp ipcp predictive
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
The PPP IPCP is not set to a predictive state.

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(11)T</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The **ppp ipcp predictive** command is useful in networks that accept connections from devices that require a reduction in the IPCP negotiation cycle time. This command reduces the amount of time needed for PPP to negotiate with the peer so that connections can be made in an acceptable amount of time. The following changes to the IPCP negotiation strategy make this time reduction possible:

- Send an IPCP Configure-Ack packet after sending an IPCP Configure-Nak packet.
- Send IPCP Configure-Nak and Configure-Ack packets after rejecting certain configuration options.

These changes can reduce connection delay by approximately 40 percent.

**Note**
Any Configure-Request packet received in the Open state is ignored until the software receives Configure-Request packets with identifying numbers greater than what was last acknowledged, in which case the software disables the predictive mode and processes the Configure-Request packet using normal IPCP negotiation operations.

The **ppp ipcp predictive** command is configured on group asynchronous and dialer interfaces running PPP or Multilink PPP.
Examples

The following example sets the link control protocol (LCP) and IPCP to predictive states on a group asynchronous interface:

```conf
interface group-async 1
  ip unnumbered loopback 0
  encapsulation ppp
  no ip mroute-cache
dialer in-band
dialer pool-member 1
async dynamic address
async dynamic routing
async mode dedicated
no fair-queue
ppp lcp predictive
ppp ipcp predictive
group-range 1 48
hold-queue 75 in
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface dialer</td>
<td>Defines a dialer rotary group.</td>
</tr>
<tr>
<td>interface group-async</td>
<td>Creates a group interface that will serve as master, to which asynchronous interfaces can be associated as members.</td>
</tr>
<tr>
<td>ppp lcp predictive</td>
<td>Sets LCP to a predictive state that reduces negotiation time by predicting responses from peers and sending expected reply and request packets in advance.</td>
</tr>
</tbody>
</table>
**ppp iphc max-header**

To set the maximum size of the largest IP header that may be compressed when configuring Internet Protocol Header Compression (IPHC) control options over PPP, use the `ppp iphc max-header` command in interface configuration mode. To change the configuration, use the `no` form of this command.

```
ppp iphc max-header bytes
no ppp iphc max-header bytes
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Command Modes</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes</td>
<td>Interface configuration</td>
<td>Release</td>
</tr>
<tr>
<td>168 bytes</td>
<td></td>
<td>11.3</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

There are two types of IP header compression used over PPP: Van Jacobsen header compression defined in RFC 1332 and enabled with the `ip tcp header-compression` command, and IPHC defined in RFC 2509 and enabled with the `ip rtp header-compression` command. The `ppp iphc` set of commands controls parameters that pertain to the form of IPHC described in RFC 2509.

The IPHC specification allows low speed links to run more efficiently by reducing the size of the IP headers as transmitted on the link. IPHC supports compressed Real-Time Transport Protocol (cRTP), compressed User Datagram Protocol (cUDP), and compressed Transaction Control Protocol (cTCP).

An IPHC-enabled interface sends only changes to the header instead of sending the entire header with every packet. At the beginning of a transmission, the transmitting end (the compressor) sends a full header packet to the receiving end (the decompressor). After the initial packet is sent, the compressor sends all other packets with headers that contain only the differences between them and the original full header. The decompressor maintains a copy of the original full header and reconstructs all the other packet headers by adding the changes to them.

The header data that is different with each packet is referred to as the session state, and is identified by a session ID or connection ID.

When the decompressor receives a compressed packet, it reconstructs the packet header by adding the difference to the saved uncompressed header. Typically, IPHC enables the header to be compressed to two bytes (four bytes if UDP checksums are used).
The following fields in a packet header usually remain the same throughout a transmission:

- IP source and destination addresses
- UDP and TCP source and destination ports
- RTP synchronization source (SSRC) fields

The following fields in a packet header usually change during a transmission:

- IP packet ID
- Checksum
- Sequence number
- RTP time stamp
- The RTP marker bit

**Examples**

The following example shows how to change the maximum size of the largest IP header that may be compressed from the default of 168 bytes to 114 bytes:

```plaintext
interface Multilink1
ip address 10.100.253.1 255.255.255.0
no ip directed-broadcast
no ip route-cache
ip tcp header-compression iphc-format
no ip mroute-cache
fair-queue 64 256 1000
no cdp enable
ppp multilink
ppp multilink fragment-delay 20
ppp multilink interleave
multilink-group 1
ip rtp header-compression iphc-format
ip rtp priority 16384 50 64
ppp iphc max-header 114
ppp iphc max-time 10
ppp iphc max-period 512
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip rtp header-compression</td>
<td>Enables TCP, UDP, and RTP (RFC 2509) header compression.</td>
</tr>
<tr>
<td>ip tcp header-compression</td>
<td>Enables TCP (RFC 1332) header compression.</td>
</tr>
<tr>
<td>ppp iphc max-period</td>
<td>Sets the maximum number of compressed packets that can be sent before a full header when configuring IPHC control options over PPP.</td>
</tr>
<tr>
<td>ppp iphc max-time</td>
<td>Sets the maximum time allowed between full headers when configuring IPHC control options over PPP.</td>
</tr>
</tbody>
</table>
**ppp lcp delay**

To configure the link control protocol (LCP) delay timer for initiating LCP negotiations after a link connects and to configure the router to discard incoming setup requests until the LCP delay timer expires, use the `ppp lcp delay` command in interface configuration mode. To disable the LCP delay timer, use the `no` form of this command.

```
ppp lcp delay seconds [milliseconds] [random max-delay-seconds] [discard]

no ppp lcp delay
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seconds</code></td>
<td>Delay, in seconds, before initiating LCP negotiations. Valid values for the <code>seconds</code> argument range from 0 to 255. The default value is 2 seconds.</td>
</tr>
<tr>
<td><code>milliseconds</code></td>
<td>(Optional) Delay, in milliseconds (ms), before initiating LCP negotiations. Valid values for the <code>milliseconds</code> argument range from 0 to 999. The default value is 0 ms.</td>
</tr>
<tr>
<td><code>random max-delay-seconds</code></td>
<td>(Optional) Specifies that a random amount of additional time will be added to the configured LCP delay timer. The additional amount of time will not exceed the number of seconds specified with the <code>max-delay-seconds</code> argument. Valid values for <code>max-delay-seconds</code> range from 1 to 255. Random delay is disabled by default.</td>
</tr>
<tr>
<td><code>discard</code></td>
<td>(Optional) Specifies that incoming configuration requests (CONFREQs) will be discarded until the LCP delay timer has expired. CONFREQs are not discarded by default.</td>
</tr>
</tbody>
</table>

**Command Default**

No LCP delay timer is configured.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T. The <code>milliseconds</code> argument was added.</td>
</tr>
<tr>
<td>12.3(11)YS</td>
<td>This command was integrated into Cisco IOS Release 12.3(11)YS. The <code>random max-delay-seconds</code> and <code>discard</code> keywords and argument were added.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Configure an LCP delay timer to allow the peer device a short amount of time to send the first packet after the PPP link comes up. If the LCP delay timer expires before a CONFREQ is received from the peer, the router can initiate LCP negotiations.
The LCP delay timer is applied only to incoming connections. PPP does not delay for outbound connections or connections where PPP cannot determine a direction.

Use the `random max-delay-seconds` keyword and argument combination to add a random amount of time to the LCP delay timer. Setting a random delay on the initiation of LCP negotiations prevents overload when many PPP links come up at the same time.

Use the `discard` keyword to specify that incoming CONFREQs should be discarded until the configured delay has expired. LCP negotiations will not be initiated until the LCP delay timer has expired.

**Examples**

The following example shows how to configure an LCP delay timer of 4 seconds. If a CONFREQ is not received before the LCP delay timer expires, LCP negotiations can be initiated by either peer.

```
Router(config-if)# ppp lcp delay 4
```

The following example shows how to configure an LCP delay timer that will expire at a random time between 5 and 15 seconds after the link comes up. If a CONFREQ is not received before the LCP delay timer expires, LCP negotiations can be initiated by either peer.

```
Router(config-if)# ppp lcp delay 5 random 10
```

The following example shows how to configure an LCP delay timer of 3.25 seconds and specifies that incoming CONFREQs will be discarded until the LCP delay timer has expired. After 3.25 seconds, LCP negotiations can be initiated by either peer.

```
Router(config-if)# ppp lcp delay 3 250 discard
```

The following example shows how to configure an LCP delay timer that will expire at a random time between 10 and 15 seconds after the link comes up, and specifies that incoming CONFREQs will be discarded until the LCP delay timer has expired. After the LCP delay timer expires, negotiations can be initiated by either peer.

```
Router(config-if)# ppp lcp delay 10 random 5 discard
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ppp multilink negotiation</code></td>
<td>Displays information about events affecting multilink groups controlled by BACP.</td>
</tr>
<tr>
<td><code>show ppp multilink</code></td>
<td>Displays bundle information for MLP bundles.</td>
</tr>
</tbody>
</table>
ppp lcp delay