

# ppp pap wait

To configure the router to delay the Password Authentication Protocol (PAP) authentication until after the peer has authenticated itself to the router, use the **ppp pap wait** command in interface configuration mode. To allow the router to immediately send out its PAP request once the authentication phase starts, use the **no** form of this command.

**ppp pap wait**

**no ppp pap wait**

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

**Command Default** Immediate PAP request transmission enabled

**Command Modes** Interface configuration

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

**Usage Guidelines** This command is used only when the call direction is call-in. The **ppp pap wait** command specifies that the router will not authenticate to a peer requesting PAP authentication until the peer has authenticated itself to the router. The **no** form of this command specifies that the router will immediately send out its PAP request once the authentication phase starts.

**Examples** The following example specifies ISDN BRI number 0. The method of encapsulation on the interface is PPP. The following example disables the default, meaning that the router will immediately send out its PAP request once the authentication phase starts.

```
interface bri 0
 encapsulation ppp
 no ppp pap wait
```

| Related Commands | Command                       | Description   |
|------------------|-------------------------------|---|
|                  | <b>aaa authentication ppp</b> | Specifies one or more AAA authentication methods for use on serial interfaces running PPP.  |
|                  | <b>ppp authentication</b>     | Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.                     |
|                  | <b>ppp pap refuse</b>         | Refuses a peer request to authenticate remotely with PPP using PAP.   |
|                  | <b>ppp pap sent-username</b>  | Reenables remote PAP support for an interface and uses the sent username and password in the PAP authentication request packet to the peer. |

# ppp pfc local

To configure protocol field compression (PFC) in configuration requests, use the **ppp pfc local** command in interface configuration mode. To return the router to the default for PCF handling, use the **no** form of this command.

**ppp pfc local {forbid | request}**

**no ppp pfc local**

## Syntax Description

|                |   |
|----------------|---|
| <b>forbid</b>  | The PFC option is not sent in outbound configuration requests, and requests from a peer to add the PFC option are not accepted. |
| <b>request</b> | The PFC option is included in outbound configuration requests.  |

## Command Default

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

## Command Modes

Interface configuration

## Command History

| Release   | Modification  |
|-----------|---|
| 12.2(7)   | This command was introduced.                                  |
| 12.2(15)B | This command was integrated into Cisco IOS Release 12.2(15)B. |

## Usage Guidelines

When PFC is negotiated during PPP negotiation, Cisco routers may compress the PPP protocol field from two bytes to one byte. The **ppp pfc local** command configures how a router handles PFC in its outbound configuration request and allows PFC 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 pfc local** command, negotiation and use of PFC 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. The **ppp pfc local** command allows the system administrator to control when PPP negotiates the HDLC address and PFC options during initial LCP negotiations, and how the results of the PPP negotiation are applied.



### Note

Using PFC can result in minor gains in effective bandwidth because they reduce the amount of framing overhead for each packet. However, using PFC 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 PFC not be enabled without carefully considering the potential results.

**Examples**

The following example shows how to configure a router to exclude the PFC option from its outbound configuration requests:

```
ppp pfc local forbid
```

**Related Commands**

| Command                | Description  |
|------------------------|--|
| <b>ppp acfc remote</b> | Configures the ACFC options received from a remote peer.                         |
| <b>ppp acfc local</b>  | Configures the ACFC option in configuration requests.                            |
| <b>ppp pfc remote</b>  | Configures the PFC option in configuration requests received from a remote peer. |

## ppp pfc remote

To configure how the protocol field compression (PFC) option in configuration requests is received from a remote peer, use the **ppp pfc remote** command in interface configuration mode. To return to the default for PFC handling, use the **no** form of this command.

**ppp pfc remote** { **apply** | **ignore** | **reject** }

**no ppp pfc remote**

### Syntax Description

|               |   |
|---------------|---|
| <b>apply</b>  | PFC options are accepted and PFC may be performed on frames sent to the remote peer.  |
| <b>ignore</b> | PFC options are accepted, but PFC is not performed on frames sent to the remote peer. |
| <b>reject</b> | PFC options are explicitly rejected.  |

### Command Default

PFC 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 PFC options received from a remote peer and PFC may be performed on frames sent to the remote peer. For synchronous links, the router responds as if the **ignore** keyword were selected and PFC options are accepted but PFC is not performed on frames sent to the remote peer.

### Command Modes

Interface configuration

### Command History

| Release   | Modification  |
|-----------|---|
| 12.2(7)   | This command was introduced.                                  |
| 12.2(15)B | This command was integrated into Cisco IOS Release 12.2(15)B. |

### Usage Guidelines

When PFC is negotiated during PPP negotiation, Cisco routers may compress the PPP protocol field from two bytes to one byte. The **ppp pfc remote** command allows PFC 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 pfc remote** command, negotiation and use of PFC 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. The **ppp pfc remote** command allows the system administrator to control when PPP negotiates the HDLC address and PFC options during initial LCP negotiations, and how the results of the PPP negotiation are applied.



#### Note

Using PFC can result in minor gains in effective bandwidth because they reduce the amount of framing overhead for each packet. However, using PFC 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 PFC not be enabled without carefully considering the potential results.

**Examples**

The following example shows how to configure a router to explicitly reject PFC options from a remote peer:

```
ppp pfc remote reject
```

**Related Commands**

| Command                | Description   |
|------------------------|---|
| <b>ppp acfc local</b>  | Configures the ACFC option in configuration requests.                             |
| <b>ppp acfc remote</b> | Configures the ACFC option in configuration requests received from a remote peer. |
| <b>ppp pfc local</b>   | Configures the PFC option in configuration requests.                              |

# ppp quality

To enable Link Quality Monitoring (LQM) on a serial interface, use the **ppp quality** command in interface configuration mode. To disable LQM, use the **no** form of this command.

**ppp quality** *percentage*

**no ppp quality**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <i>percentage</i> Specifies the link quality threshold. Range is from 1 to 100. |
|---------------------------|---|

|                        |                      |
|------------------------|----------------------|
| <b>Command Default</b> | Command is disabled. |
|------------------------|----------------------|

|                      |                         |
|----------------------|-------------------------|
| <b>Command Modes</b> | Interface configuration |
|----------------------|-------------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 10.0           | This command was introduced. |

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | <p>The percentages are calculated for both incoming and outgoing directions. The outgoing quality is calculated by comparing the total number of packets and bytes sent to the total number of packets and bytes received by the destination node. The incoming quality is calculated by comparing the total number of packets and bytes received to the total number of packets and bytes sent by the destination node.</p> <p>If the link quality percentage is not maintained, the link is deemed to be of poor quality and is taken down. LQM implements a time lag so that the link does not bounce up and down.</p> |
|-------------------------|---|

|                 |  |
|-----------------|--|
| <b>Examples</b> | <p>The following example enables LQM on serial interface 2:</p> <pre>interface serial 2  encapsulation ppp  ppp quality 80</pre> |
|-----------------|--|

| <b>Related Commands</b> | <b>Command</b>   | <b>Description</b>                                 |
|-------------------------|------------------|--|
|                         | <b>exec</b>      | Allows an EXEC process on a line.                  |
|                         | <b>keepalive</b> | Sets the keepalive timer for a specific interface. |

# ppp reliable-link

To enable Link Access Procedure, Balanced (LAPB) Numbered Mode negotiation for a reliable serial link, use the **ppp reliable-link** command in interface configuration mode. To disable negotiation for a PPP reliable link on a specified interface, use the **no** form of the command.

**ppp reliable-link**

**no ppp reliable-link**

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

**Command Default** Command is disabled.

**Command Modes** Interface configuration

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 11.0    | This command was introduced. |

**Usage Guidelines** Enabling LAPB Numbered Mode negotiation as a means of providing a reliable link does not guarantee that all connections through the specified interface will in fact use a reliable link. It guarantees only that the router will attempt to negotiate reliable link on this interface.

PPP reliable link can be used with PPP compression over the link, but it does not require PPP compression.

PPP reliable link does not work with Multilink PPP.

You can use the **show interface** command to determine whether LAPB has been established on the link. You can troubleshoot PPP reliable link by using the **debug lapb** command and the **debug ppp negotiations**, **debug ppp errors**, and **debug ppp packets** commands.

**Examples** The following example enables PPP reliable link and predictor compression on BRI interface 0:

```
interface bri 0
description Enables predictor compression on BRI 0
ip address 172.16.1.1 255.255.255.0
encapsulation ppp
dialer map ip 172.16.1.2 name mymap 15550191357
compress predictor
ppp authentication chap
dialer-group 1
ppp reliable-link
```

| Related Commands | Command                | Description  |
|------------------|------------------------|--|
|                  | <b>compress</b>        | Configures compression for LAPB, PPP, and HDLC encapsulations.                         |
|                  | <b>debug lapb</b>      | Displays all traffic for interfaces using LAPB encapsulation.                          |
|                  | <b>debug ppp</b>       | Displays information on traffic and exchanges in an internetwork implementing the PPP. |
|                  | <b>show interfaces</b> | Displays statistics for all interfaces configured on the router or access server.      |

# ppp timeout aaa

To support the idle direction for the timeout value set by authentication, authorization, and accounting (AAA), use the **ppp timeout aaa** command in interface configuration mode. To remove this setting, use the **no** form of this command.

**ppp timeout aaa [inbound]**

**no ppp timeout aaa [inbound]**

|                           |  |  |
|---------------------------|--|--|
| <b>Syntax Description</b> | <b>inbound</b>   | (Optional) Specifies that the AAA server can set the PPP idle timeout parameters only for inbound traffic. |
| <b>Command Default</b>    | The command is disabled.   |  |
| <b>Command Modes</b>      | Interface configuration  |  |
| <b>Command History</b>    | <b>Release</b>   | <b>Modification</b>  |
|                           | 12.2T  | This command was introduced.   |
| <b>Usage Guidelines</b>   | Use this command to reset the idle timer based on inbound traffic only set by AAA, and to support the idle direction for the timeout value set by AAA.   |  |
| <b>Examples</b>           | The following example uses a virtual template to set the idle timer by AAA only when inbound traffic is detected:<br><br><pre>interface Virtual-Template1   ppp timeout idle 1800   timeout absolute 180   ppp timeout aaa inbound</pre> |  |
| <b>Related Commands</b>   | <b>Command</b>   | <b>Description</b>   |
|                           | <b>ppp timeout idle</b>  | Sets PPP idle timeout parameters, in seconds.  |

# ppp timeout authentication

To set the PPP authentication timeout value, use the **ppp timeout authentication** command in interface configuration mode. To restore the default value, use the **no** form of this command.

**ppp timeout authentication** *seconds*

**no ppp timeout authentication**

|                           |                |   |
|---------------------------|----------------|---|
| <b>Syntax Description</b> | <i>seconds</i> | Maximum time, in seconds, to wait for a response to an authentication packet. Valid seconds are from 0 to 255 seconds. The default is 10 seconds. |
|---------------------------|----------------|---|

|                        |            |
|------------------------|------------|
| <b>Command Default</b> | 10 seconds |
|------------------------|------------|

|                      |                         |
|----------------------|-------------------------|
| <b>Command Modes</b> | Interface configuration |
|----------------------|-------------------------|

|                        |                |   |
|------------------------|----------------|---|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>   |
|                        | 11.3           | This command was introduced.                                    |
|                        | 12.2(31)SB2    | This command was integrated into Cisco IOS Release 12.2(31)SB2. |

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | <p><b>Cisco 10000 Series Router</b></p> <p>To keep an L2TP network server (LNS) from timing out a PPP authentication process, we recommend that you configure the PPP authentication timeout to 100 seconds.</p> |
|-------------------------|--|

|                 |  |
|-----------------|--|
| <b>Examples</b> | <p>The following example changes the time to wait for a response to an authentication packet to 15 seconds:</p> <pre>ppp timeout authentication 15</pre> |
|-----------------|--|

|                         |                          |                                    |
|-------------------------|--------------------------|------------------------------------|
| <b>Related Commands</b> | <b>Command</b>           | <b>Description</b>                 |
|                         | <b>ppp timeout retry</b> | Sets PPP timeout retry parameters. |

# ppp timeout idle

To set the PPP timeout idle parameter, use the **ppp timeout idle** command in interface configuration mode. To reset the timeout value, use the **no** form of this command.

**ppp timeout idle** *seconds*

**no ppp timeout idle** *seconds*

|                           |                |  |
|---------------------------|----------------|--|
| <b>Syntax Description</b> | <i>seconds</i> | Line idle time, in seconds, allowed before disconnecting the line. Acceptable range is platform dependent. |
|---------------------------|----------------|--|

|                        |                                       |
|------------------------|---------------------------------------|
| <b>Command Default</b> | No PPP timeout idle parameter is set. |
|------------------------|---------------------------------------|

|                      |                                     |
|----------------------|-------------------------------------|
| <b>Command Modes</b> | Interface configuration (config-if) |
|----------------------|-------------------------------------|

|                        |                |  |
|------------------------|----------------|--|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>  |
|                        | 11.3           | This command was introduced as <b>ppp idle-timeout</b> .                             |
|                        | 12.2           | This command was modified. The command name was changed to <b>ppp timeout idle</b> . |

**Usage Guidelines**

The **ppp timeout idle** command is used mainly on dialup interfaces and other temporary circuits to control how long the connection can be idle before it is terminated. All user traffic will reset the idle timer; however, nonnetwork traffic such as PPP control packets will not reset the timer. Also note that the dialer subsystem supports an alternate idle link detection mechanism that can be used instead of or with this PPP idle link detection mechanism.

The **ppp timeout idle** command name replaces the name **ppp idle-timeout**. The CLI will accept the **ppp timeout idle** name in Cisco IOS Release 12.2 and later releases.

**Examples**

The following example shows how to set the idle timer to 15 seconds:

```
ppp timeout idle 15
```

|                         |                                     |   |
|-------------------------|-------------------------------------|---|
| <b>Related Commands</b> | <b>Command</b>                      | <b>Description</b>  |
|                         | <b>absolute-timeout</b>             | Sets the interval for closing user connections on a specific line or port.  |
|                         | <b>dialer fast-idle (interface)</b> | Specifies the amount of time that a line for which there is contention will stay idle before it is disconnected and the competing call is placed. |

| Command                                | Description   |
|--|---|
| <b>dialer hold-queue</b>               | Allows interesting outgoing packets to be queued until a modem connection is established. |
| <b>dialer idle-timeout (interface)</b> | Specifies the idle time before the line is disconnected.                                  |

# ppp timeout idle (template)

To set PPP idle timeout parameters on a virtual template interface, use the **ppp timeout idle** command in interface configuration mode. To reset the time value, use the **no** form of this command.

**ppp timeout idle** *seconds*

**no ppp timeout idle** *seconds*

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <i>seconds</i> Line idle time, in seconds, allowed before disconnecting the line. |
|---------------------------|---|

|                        |                                |
|------------------------|--------------------------------|
| <b>Command Default</b> | No default behavior or values. |
|------------------------|--------------------------------|

|                      |                         |
|----------------------|-------------------------|
| <b>Command Modes</b> | Interface configuration |
|----------------------|-------------------------|

|                        |                |   |
|------------------------|----------------|---|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>   |
|                        | 12.2(4)T       | This command was introduced for virtual template interfaces.  |
|                        | 12.2(11)T      | This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300, Cisco AS5400 and Cisco AS5800. |

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | This version of the <b>ppp timeout idle</b> command is used on virtual template interfaces to control how long the connection can be idle before it is terminated. |
|-------------------------|--|

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example sets the PPP idle timeout to 45 seconds in virtual template interface 1: |
|-----------------|--|

```
interface Virtual-Template1
 ip unnumbered Loopback1
 peer default ip address pool local_pool
 ppp authentication chap callin
 ppp chap hostname name
 ppp timeout idle 45
 ip idle-group 101 in
 ip idle-group 102 in
 ppp multilink
```

|                         |   |   |
|-------------------------|---|---|
| <b>Related Commands</b> | <b>Command</b>                                    | <b>Description</b>  |
|                         | <b>absolute-timeout</b>                           | Sets the interval for closing user connections on a specific line or port.  |
|                         | <b>dialer fast-idle (interface configuration)</b> | Specifies the amount of time that a line for which there is contention will stay idle before it is disconnected and the competing call is placed. |

| <b>Command</b>                        | <b>Description</b>  |
|---------------------------------------|---|
| <b>dialer hold-queue</b>              | Allows interesting outgoing packets to be queued until a modem connection is established. |
| <b>dialer idle-timeout (template)</b> | Specifies the idle time on a virtual template interface before the line is disconnected.  |

# ppp timeout multilink link add

To limit the amount of time for which Multilink PPP (MLP) waits for a call to be established, use the **ppp timeout multilink link add** command in interface configuration mode. To remove the value, use the **no** form of this command.

**ppp timeout multilink link add** *seconds*

**no ppp timeout multilink link add**

## Syntax Description

|                |  |
|----------------|--|
| <i>seconds</i> | Wait period, in seconds, in the range from 1 to 65535 seconds. |
|----------------|--|

## Command Default

No default behavior or values.

## Command Modes

Interface configuration

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 11.3    | This command was introduced. |

## Usage Guidelines

When MLP needs to increase the bandwidth of a bundle, it attempts to bring up an additional link by requesting that the dialer system place a call to the peer system, or if the Bandwidth Allocation Protocol (BAP) is used, the call may also be done by requesting that the peer system make the call. BAP can be used to either make the call or request that the peer system make the call, depending upon the configuration. The time value specified with the **ppp timeout multilink link add** command determines how long MLP waits for that call to be established. If a new link does not join the bundle within the specified time, it is assumed that the call failed, and the call is attempted again.

If there are not enough links to carry the load, and the call succeeds in less than the time specified with the **ppp timeout multilink link add** command, MLP can immediately request another link. The time value specified with the **ppp timeout multilink link add** command prevents flooding the dialer system with call requests because not enough time was provided for prior requests to finish.

If the **ppp timeout multilink link add** command is not configured but the **dialer wait-for-carrier-time** command is, MLP will use the time value set with the **dialer wait-for-carrier-time** command. If neither command is configured, MLP uses a default value of 30 seconds.

This command is used with dynamic bandwidth (dial-on-demand) bundles.

## Examples

The following example sets the call timeout period to 45 seconds:

```
ppp timeout multilink link add 45
```

| Related Commands | Command   | Description  |
|------------------|---|--|
|                  | <b>dialer wait-for-carrier-time (interface)</b> | Specifies the length of time the interface waits for a carrier.  |
|                  | <b>ppp timeout multilink link remove</b>        | Sets a timer that determines how long MLP waits to drop a link when traffic load goes below the configured load threshold. |

# ppp timeout multilink link remove

To set a timer that determines how long Multilink PPP (MLP) waits to drop a link when traffic load goes below the configured load threshold, use the **ppp timeout multilink link remove** command in interface configuration mode. To remove the value, use the **no** form of this command.

**ppp timeout multilink link remove** *seconds*

**no ppp timeout multilink link remove**

|                           |                |  |
|---------------------------|----------------|--|
| <b>Syntax Description</b> | <i>seconds</i> | Threshold wait period, in seconds, in the range from 1 to 65535 seconds. |
|---------------------------|----------------|--|

|                        |                                |
|------------------------|--------------------------------|
| <b>Command Default</b> | No default behavior or values. |
|------------------------|--------------------------------|

|                      |                         |
|----------------------|-------------------------|
| <b>Command Modes</b> | Interface configuration |
|----------------------|-------------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 11.3           | This command was introduced. |

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | When traffic load goes below the threshold set with the <b>ppp multilink load-threshold</b> command, MLP waits for the time set with the <b>ppp timeout multilink link remove</b> command and, if the load still remains below that threshold, drops the link to reduce bandwidth. |
|-------------------------|--|

MLP will reduce bandwidth but never remove the last link in a bundle. The complete severing of a connection is controlled by the idle timer value specified in the **dialer idle-timeout** command; however, the idle timer has no effect on when MLP will drop excess links in a bundle.

If the **ppp timeout multilink link remove** command is not configured but the **dialer wait-for-carrier-time** command is, MLP will use the time value set with the **dialer wait-for-carrier-time** command. If neither command is configured, MLP uses a default value of 30 seconds.

This command is used with dynamic bandwidth (dial-on-demand) bundles.

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example sets the low traffic load threshold wait period to 45 seconds: |
|-----------------|--|

```
ppp timeout multilink link remove 45
```

**Related Commands**

| <b>Command</b>                                  | <b>Description</b>  |
|---|---|
| <b>dialer fast-idle (interface)</b>             | Specifies the idle time before the line is disconnected.                    |
| <b>dialer wait-for-carrier-time (interface)</b> | Specifies the length of time the interface waits for a carrier.             |
| <b>ppp timeout multilink link add</b>           | Limits the amount of time for which MLP waits for a call to be established. |

# ppp timeout multilink lost-fragment

To set a timer that determines how long Multilink PPP waits for an expected fragment to arrive before declaring it lost, use the **ppp timeout multilink lost-fragment** command in interface configuration mode. To reset the default value, use the **no** form of this command.

**ppp timeout multilink lost-fragment** *seconds* [*milliseconds*]

**no ppp timeout multilink lost-fragment**

## Syntax Description

|                     |  |
|---------------------|--|
| <i>seconds</i>      | Wait period, in seconds, in the range from 1 to 255 seconds.   |
|                     | <b>Note</b> If the desired delay should be in milliseconds, set the <i>seconds</i> argument to 0 and enter a value for the <i>milliseconds</i> argument. |
| <i>milliseconds</i> | (Optional) Wait period, in milliseconds, in the range from 1 to 999 milliseconds.  |

## Command Default

The default value is 1 second.

## Command Modes

Interface configuration

## Command History

| Release     | Modification   |
|-------------|--|
| 11.3        | This command was introduced.   |
| 12.4(6)T    | The optional <i>milliseconds</i> argument was added for a more precise setting and the command was integrated into Cisco IOS Release 12.4(6)T. |
| 12.2(31)SB2 | The command was integrated into Cisco IOS Release 12.2(31)SB2.   |

## Examples

The following example sets a 5-second wait period for receiving expected fragments before declaring the fragments lost:

```
ppp timeout multilink lost-fragment 5
```

The following example sets a 300-millisecond wait period for receiving expected fragments before declaring the fragments lost:

```
ppp timeout multilink lost-fragment 0 300
```

The following example configures a wait period of 500 milliseconds (1/2 second):

```
ppp timeout multilink lost-fragment 0 500
```

## Related Commands

| Command                  | Description   |
|--------------------------|---|
| <b>ppp link reorders</b> | Sets an advisory flag that indicates that the serial interface may receive packets in a different order than a peer system sent them. |

# ppp timeout ncp

To set a time limit for the successful negotiation of at least one network layer protocol after a PPP connection is established, use the **ppp timeout ncp** command in interface configuration mode. To reset the default condition, use the **no** form of this command.

**ppp timeout ncp** *seconds*

**no ppp timeout ncp**

## Syntax Description

|                |  |
|----------------|--|
| <i>seconds</i> | Maximum time, in seconds, PPP should wait for negotiation of a network layer protocol. If no network protocol is negotiated in the given time, the connection is disconnected. |
|----------------|--|

## Command Default

No time limit is imposed (**no ppp timeout ncp**).

## Command Modes

Interface configuration

## Command History

| Release | Modification   |
|---------|--|
| 11.3    | This command was introduced as <b>ppp negotiation-timeout</b> .  |
| 12.2    | This command was changed to <b>ppp timeout ncp</b> . The <b>ppp negotiation-timeout</b> command was accepted by the command line interpreter through Cisco IOS Release 12.2. |

## Usage Guidelines

The **ppp timeout ncp** command protects against the establishment of links that are physically up and carrying traffic at the link level, but are unusable for carrying data traffic due to failure to negotiate the capability to transport any network level data. This command is particularly useful for dialed connections, where it is usually undesirable to leave a telephone circuit active when it cannot carry network traffic.

## Examples

The following example sets the Network Control Protocol (NCP) timer to 8 seconds:

```
ppp timeout ncp 8
```

## Related Commands

| Command                                | Description  |
|--|--|
| <b>absolute-timeout</b>                | Sets the interval for closing user connections on a specific line or port. |
| <b>dialer idle-timeout (interface)</b> | Specifies the idle time before the line is disconnected.                   |

# ppp timeout retry

To set the maximum waiting period for a response during PPP negotiation, use the **ppp timeout retry** command in interface configuration mode. To reset the time value to the default settings, use the **no** form of this command.

**ppp timeout retry** *seconds*

**no ppp timeout retry**

## Cisco IOS Release 12.2(33)SRD

**ppp timeout retry** *seconds* [*milliseconds*]

**no ppp timeout retry**

### Syntax Description

|                     |   |
|---------------------|---|
| <i>seconds</i>      | Maximum time, in seconds, to wait for a response during PPP negotiation. Valid values for the <i>seconds</i> argument range from 0 to 255. The default value is 2 seconds.                      |
| <i>milliseconds</i> | (Optional) Maximum time, in milliseconds (ms), to wait for a response during PPP negotiation. Valid values for the <i>milliseconds</i> argument range from 0 to 999. The default value is 0 ms. |

### Command Default

The default value waiting period for a response during PPP negotiation is 2 seconds.

### Command Modes

Interface configuration

### Command History

| Release     | Modification  |
|-------------|---|
| 11.3        | This command was introduced.  |
| 12.2        | This command was integrated into Cisco IOS Release 12.2.  |
| 12.2(33)SRD | This command was integrated into Cisco IOS Release 12.2(33)SRD. The <i>milliseconds</i> argument was added. |

### Usage Guidelines

The **ppp timeout retry** command is useful for setting a maximum amount of time PPP should wait for a response to any control packet it sends.

### Examples

The following example sets the retry timer to 100 seconds and 200 ms:

```
interface serial 2/0
encapsulation ppp
ppp timeout retry 100 200
```

■ **ppp timeout retry**

| <b>Related Commands</b> | <b>Command</b>                    | <b>Description</b>                          |
|-------------------------|-----------------------------------|---|
|                         | <b>ppp timeout authentication</b> | Sets PPP authentication timeout parameters. |
|                         | <b>ppp timeout idle</b>           | Sets PPP idle timeout parameters.           |

# pri-group timeslots

To specify an ISDN PRI group on a channelized T1 or E1 controller, and to release the ISDN PRI signaling time slot, use the **pri-group timeslots** command in controller configuration mode. To remove or change the ISDN PRI configuration, use the **no** form of this command.

```
pri-group timeslots timeslot-range [nfas_d { backup nfas_int number nfas_group number | none nfas_int number nfas_group number [service mgcp] | primary nfas_int number nfas_group number [iua as-name | rlm-group number | service mgcp]} | service mgcp]
```

```
no pri-group timeslots timeslot-range [nfas_d { backup nfas_int number nfas_group number | none nfas_int number nfas_group number [service mgcp] | primary nfas_int number nfas_group number [iua as-name | rlm-group number | service mgcp]} | service mgcp]
```

## Syntax Description

|                          |  |
|--------------------------|--|
| <i>timeslot-range</i>    | A value or range of values for time slots on a T1 or E1 controller that consists of an ISDN PRI group. Use a hyphen to indicate a range.<br><br><b>Note</b> Groups of time slot ranges separated by commas (1-4,8-23 for example) are also accepted. |
| <b>nfas_d</b>            | (Optional) Configures the operation of the ISDN PRI D channel.   |
| <b>backup</b>            | The D-channel time slot is used as the Non-Facility Associated Signaling (NFAS) D backup.  |
| <b>none</b>              | The D-channel time slot is used as an additional B channel.  |
| <b>primary</b>           | The D-channel time slot is used as the NFAS D primary.   |
| <b>nfas_int number</b>   | Specifies the provisioned NFAS interface as a value. Valid values for the NFAS interface range from 0 to 44.   |
| <b>nfas_group number</b> | Specifies the NFAS group. Valid values for the NFAS group number range from 0 to 31.   |
| <b>iua as-name</b>       | (Optional) Configures the ISDN User Adaptation Layer (IUA) application server (AS) name.   |
| <b>rlm-group number</b>  | (Optional) Specifies the Redundant Link Manager (RLM) group and release the ISDN PRI signaling channel. Valid values for the RLM group number range from 0 to 255.   |
| <b>service mgcp</b>      | (Optional) Configures the service type as Media Gateway Control Protocol (MGCP) service.   |

## Command Default

No ISDN PRI group is configured. The switch type is automatically set to the National ISDN switch type (**primary-ni** keyword) when the **pri-group timeslots** command is configured with the **rlm-group** subkeyword.

## Command Modes

Controller configuration

**Command History**

| <b>Release</b> | <b>Modification</b>   |
|----------------|---|
| 11.0           | This command was introduced.  |
| 11.3           | This command was enhanced to support NFAS.  |
| 12.0(2)T       | This command was implemented on the Cisco MC3810 multiservice concentrator.   |
| 12.0(7)XK      | This command was implemented on the Cisco 2600 and Cisco 3600 series routers.   |
| 12.1(2)T       | The modifications in Cisco IOS Release 12.0(7)XK were integrated into Cisco IOS Release 12.1(2)T.                     |
| 12.2(8)B       | This command was modified with the <b>rlm-group</b> subkeyword to support release of the ISDN PRI signaling channels. |
| 12.2(15)T      | The modifications in Cisco IOS Release 12.2(8)B were integrated into Cisco IOS Release 12.2(15)T.                     |

**Usage Guidelines**

The **pri-group** command supports the use of DS0 time slots for Signaling System 7 (SS7) links, and therefore the coexistence of SS7 links and PRI voice and data bearer channels on the same T1 or E1 span. In these configurations, the command applies to voice applications.

In SS7-enabled Voice over IP (VoIP) configurations when an RLM group is configured, High-Level Data Link Control (HDLC) resources allocated for ISDN signaling on a digital subscriber line (DSL) interface are released and the signaling slot is converted to a bearer channel (B24). The D channel will be running on IP. The chosen D-channel time slot can still be used as a B channel by using the **isdn rlm-group** interface configuration command to configure the NFAS groups.

NFAS allows a single D channel to control multiple PRI interfaces. Use of a single D channel to control multiple PRI interfaces frees one B channel on each interface to carry other traffic. A backup D channel can also be configured for use when the primary NFAS D channel fails. When a backup D channel is configured, any hard system failure causes a switchover to the backup D channel and currently connected calls remain connected.

NFAS is supported only with a channelized T1 controller and, as a result, must be ISDN PRI capable. Once the channelized T1 controllers are configured for ISDN PRI, only the NFAS primary D channel must be configured; its configuration is distributed to all members of the associated NFAS group. Any configuration changes made to the primary D channel will be propagated to all NFAS group members. The primary D channel interface is the only interface shown after the configuration is written to memory.

The channelized T1 controllers on the router must also be configured for ISDN. The router must connect to either an AT&T 4ESS, Northern Telecom DMS-100 or DMS-250, or National ISDN switch type.

The ISDN switch must be provisioned for NFAS. The primary and backup D channels should be configured on separate T1 controllers. The primary, backup, and B-channel members on the respective controllers should be the same configuration as that configured on the router and ISDN switch. The interface ID assigned to the controllers must match that of the ISDN switch.

You can disable a specified channel or an entire PRI interface, thereby taking it out of service or placing it into one of the other states that is passed in to the switch using the **isdn service** interface configuration command.

In the event that a controller belonging to an NFAS group is shut down, all active calls on the controller that is shut down will be cleared (regardless of whether the controller is set to primary, backup, or none), and one of the following events will occur:

- If the controller that is shut down is configured as the primary and no backup is configured, all active calls on the group are cleared.
- If the controller that is shut down is configured as the primary, and the active (In service) D channel is the primary and a backup is configured, then the active D channel changes to the backup controller.
- If the controller that is shut down is configured as the primary, and the active D channel is the backup, then the active D channel remains as backup controller.
- If the controller that is shut down is configured as the backup, and the active D channel is the backup, then the active D channel changes to the primary controller.

The expected behavior in NFAS when an ISDN D channel (serial interface) is shut down is that ISDN Layer 2 should go down but keep ISDN Layer 1 up, and that the entire interface will go down after the amount of seconds specified for timer T309.



#### Note

The active D channel changeover between primary and backup controllers happens only when one of the link fails and not when the link comes up. The T309 timer is triggered when the changeover takes place.

#### Examples

The following example configures T1 controller 1/0 for PRI and for the NFAS primary D channel. This primary D channel controls all the B channels in NFAS group 1.

```
controller t1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 nfas_d primary nfas_int 0 nfas_group 1
```

The following example specifies ISDN PRI on T1 slot 1, port 0, and configures voice and data bearer capability on time slots 2 through 6:

```
isdn switch-type primary-4ess
controller t1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 2-6
```

The following example configures a standard ISDN PRI interface:

```
! Standard PRI configuration:
controller t1 1
 pri-group timeslots 1-23 nfas_d primary nfas_int 0 nfas_group 0
 exit

! Standard ISDN serial configuration:
interface serial1:23
! Set ISDN parameters:
 isdn T309 4000
 exit
```

The following example configures a dedicated T1 link for SS7-enabled VoIP:

```
controller T1 1
 pri-group timeslots 1-23 nfas_d primary nfas_int 0 nfas_group 0
 exit
```

```

! In a dedicated configuration, we assume the 24th timeslot will be used by ISDN.
! Serial interface 0:23 is created for configuring ISDN parameters.
interface Serial:24
! The D channel is on the RLM.
 isdn rlm 0
 isdn T309 4000
exit

```

The following example configures a shared T1 link for SS7-enabled VoIP. The **rlm-group 0** portion of the **pri-group timeslots** command releases the ISDN PRI signaling channel.

```

controller T1 1
 pri-group timeslots 1-3 nfas_d primary nfas_int 0 nfas_group 0 rlm-group 0
 channel group 23 timeslot 24
end

! D-channel interface is created for configuration of ISDN parameters:
interface Dchannel1
 isdn T309 4000
end

```

### Related Commands

| Command                     | Description  |
|-----------------------------|--|
| <b>controller</b>           | Configures a T1 or E1 controller and enters controller configuration mode.   |
| <b>interface Dchannel</b>   | Specifies an ISDN D-channel interface for VoIP applications that require release of the ISDN PRI signaling time slot for RLM configurations.   |
| <b>interface serial</b>     | Specifies a serial interface created on a channelized E1 or channelized T1 controller for ISDN PRI signaling.  |
| <b>isdn rlm-group</b>       | Specifies the RLM group number that ISDN will start using.   |
| <b>isdn switch-type</b>     | Specifies the central office switch type on the ISDN PRI interface.  |
| <b>isdn timer t309</b>      | Changes the value of the T309 timer to clear network connections and release the B channels when there is no signaling channel active, that is, when the D channel has failed and cannot recover by switching to an alternate D channel. Calls remain active and able to transfer data when the D channel fails until the T309 timer expires. The T309 timer is canceled when D-channel failover succeeds. |
| <b>show isdn nfas group</b> | Displays all the members of a specified NFAS group or all NFAS groups.   |

# profile incoming

To define a template formed by directives guiding the Call Service Module (CSM) to process the digit sequence for a signaling class, use the **profile incoming** command in global configuration mode.

## **profile incoming** *template*

|                           |                 |  |
|---------------------------|-----------------|--|
| <b>Syntax Description</b> | <i>template</i> | String of special characters that are arranged in a certain order to process the digit sequence for the signaling class. Choose from the following list: <ul style="list-style-type: none"> <li>• <b>S</b>—Starts the state machine.</li> <li>• <b>&lt;*</b>—Waits for the digit <i>*</i> to be detected. The digit to be detected is the next character in the template. If any other digit is detected, then that is a failure. If the digit is detected, then go to the next directive.</li> <li>• <b>a</b>—Digits are collected as the ANI until the first nondigit or a timeout occurs.</li> <li>• <b>d</b>—Digits are collected as the DNIS until the first nondigit or a timeout occurs.</li> <li>• <b>n</b>—Notifies the CSM of the collected ANI and DNIS.</li> </ul> |
|---------------------------|-----------------|--|

|                        |                               |
|------------------------|-------------------------------|
| <b>Command Default</b> | No default behavior or values |
|------------------------|-------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 12.1(1)T       | This command was introduced. |

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | Arrange the directive special characters in the order necessary to process the digit sequence for your signaling class. |
|-------------------------|---|

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example enables the <b>profile incoming</b> command: |
|-----------------|--|

```
signaling-class cas test
profile incoming S<*a<*d<*n
```

| <b>Related Commands</b> | <b>Command</b>             | <b>Description</b>  |
|-------------------------|----------------------------|---|
|                         | <b>class (controller)</b>  | Activates the <b>signaling-class cas</b> command.   |
|                         | <b>signaling-class cas</b> | Defines a signaling class with a template formed by directives guiding the CSM to process the digit sequence. |

# range

To associate a range of modems or other physical resources with a resource group, use the **range** command in resource group configuration mode. To remove a range of modems or other physical resources, use the **no** form of this command.

```
range { limit number | port slot [slot] }
```

```
no range { limit number | port slot [slot] }
```

## Cisco AS5200 and AS5300 Series Routers

```
range { limit number | port slot/port [slot/port] }
```

```
no range { limit number | port slot/port [slot/port] }
```

### Syntax Description

|   |  |
|---|--|
| <b>limit</b> <i>number</i>                        | Maximum number of simultaneous connections supported by the resource group. Replace the <i>number</i> argument with the session limit you want to assign. Your access server hardware configuration determines the maximum value of this limit. Applicable to ISDN B channels or HDLC controllers. |
| <b>port</b> <i>slot</i> [ <i>slot</i> ]           | Slot or range of slots to use in the resource group.   |
| <b>port</b> <i>slot/port</i> [ <i>slot/port</i> ] | Specific port or range of ports to use in the resource group. A forward slash must be used to separate the slot and port numbers.  |

### Command Default

No range is configured.

### Command Modes

Resource group configuration

### Command History

| Release   | Modification                 |
|-----------|------------------------------|
| 12.0(4)XI | This command was introduced. |

### Usage Guidelines

Use the **range** resource group configuration command to associate a range of modems or other physical resources with a resource group.

Specify the range for port-based resources by using the resource's physical location. Do not identify non-port-based resource ranges by using a location. Rather, specify the size of the resource group with a single integer limit.

Specify noncontiguous ranges by using multiple **range port** commands within the same resource group. Do not configure the same ports in more than one resource group and do not overlap multiple port ranges.

For resources that are not pooled and have a one-to-one correspondence between DS0s, B channels, and HDLC framers, use the **range limit** *number* command. Circuit-switched data calls and V.120 calls use these kinds of resources.

**Note**

---

Do not put heterogeneous resources in the same group. Do not put MICA modems in the same group as Microcom modems. Do not put modems and HDLC controllers in the same resource group.

Do not configure “port” and “limit” parameters in the same resource group.

---

**Examples**

The following example shows the range limit set for 48 simultaneous connections being supported by the resource group:

```
resource-pool group resource hdlc1
  range limit 48
```

The following example shows the ports set for modem 1 ranging from port 0 to port 47:

```
resource-pool group modem1
  range port 1/0 1/47
```

# rcapi number

To enable the Cisco 800 series router to distinguish between incoming CAPI calls and incoming non-CAPI calls such as POTS, PPP, and X.25, use the **rcapi number** command in global configuration mode. To release the specified directory number from the RCAPi interface, use the **no** form of this command.

**rcapi number** *directory-number*[:*subaddress*]

**no rcapi number**

| Syntax Description      |  |
|-------------------------|--|
| <i>directory-number</i> | ISDN directory number.                                       |
| <i>:subaddress</i>      | (Optional) Subaddress of the router preceded by a colon (:). |

**Command Default** No directory number is set for the RCAPi interface.

**Command Modes** Global configuration

| Command History | Release   | Modification  |
|-----------------|-----------|---|
|                 | 12.0(7)XV | The commands <b>rcapi number</b> and <b>no rcapi number</b> were introduced on the Cisco 800 series router. |

**Usage Guidelines** The **rcapi number** command allows the Cisco 800 series router to reserve directory numbers exclusively for incoming calls.

The *directory-number* argument is the number assigned by the ISDN provider for the PC on which RCAPi is configured. The directory number should not be set to any other interfaces such as POTS and DOV. This command works only with the Net3 switch type.

**Examples** The following example sets the router to recognize an ISDN number rather than a subaddress:

```
rcapi number 12345
```

| Related Commands | Command                   | Description  |
|------------------|---------------------------|--|
|                  | <b>debug rcapi events</b> | Displays diagnostic DCP and driver messages.   |
|                  | <b>rcapi server</b>       | Enables the RCAPi server on the 800 series router and, optionally, sets the TCP port number. |
|                  | <b>show rcapi status</b>  | Display statistics and details about RCAPi server operation.                                 |

# rcapi server

To enable the RAPI server on the 800 series router or to set the TCP port number, use the **rcapi server** command in global configuration mode. To disable the RAPI server on the 800 series router, use the **no** form of this command.

**rcapi server** [*port number*]

**no rcapi server**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>port number</b> (Optional) TCP port number. |
|---------------------------|--|

|                        |  |
|------------------------|--|
| <b>Command Default</b> | If the router is configured for basic Net3 ISDN switch type, by default RAPI is enabled, and the port number is set to 2578. |
|------------------------|--|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

|                        |                |   |
|------------------------|----------------|---|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>   |
|                        | 12.0(7)XV      | This command was introduced on the Cisco 800 series router. |

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | This command works only with the Net3 switch type. The same port number must be configured on both the router and client PC. |
|-------------------------|--|

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example set the TCP port number to 2000:<br><pre>rcapi server port 2000</pre> |
|-----------------|---|

|                         |                           |   |
|-------------------------|---------------------------|---|
| <b>Related Commands</b> | <b>Command</b>            | <b>Description</b>  |
|                         | <b>debug rcapi events</b> | Displays diagnostic DCP and driver messages.  |
|                         | <b>rcapi number</b>       | Enables the Cisco 800 series router to distinguish between incoming CAPI calls and incoming non-CAPI calls such as POTS, PPP, and X.25. |
|                         | <b>show rcapi status</b>  | Display statistics and details about RAPI server operation.   |

# redundancy

To enter redundancy configuration mode, use the **redundancy** command in global configuration mode.

**redundancy**

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

**Command Default** None

**Command Modes** Global configuration (config)

| Command History | Release      | Modification  |
|-----------------|--------------|---|
|                 | 12.1(5)XV1   | This command was introduced on the Cisco AS5800 universal access server.                                      |
|                 | 12.2(4)XF    | This command was introduced for the Cisco uBR10012 router.  |
|                 | 12.2(11)T    | This command was integrated into Cisco IOS Release 12.2(11)T.   |
|                 | 12.0(9)SL    | This command was integrated into Cisco IOS Release 12.0(9)SL.   |
|                 | 12.0(16)ST   | This command was implemented on the Cisco 7500 series Internet routers.                                       |
|                 | 12.2(14)S    | This command was integrated into Cisco IOS Release 12.2(14)S.   |
|                 | 12.2(14)SX   | Support for this command was added for the Supervisor Engine 720.   |
|                 | 12.2(18)S    | This command was implemented on the Cisco 7500 series Internet routers.                                       |
|                 | 12.2(20)S    | This command was implemented on the Cisco 7304 router.  |
|                 | 12.2(17d)SXB | Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.                     |
|                 | 12.3(7)T     | This command was implemented on the Cisco 7500 series Internet routers.                                       |
|                 | 12.2(8)MC2   | This command was implemented on the MWR 1900 Mobile Wireless Edge Router (MWR).                               |
|                 | 12.3(11)T    | This command was implemented on the MWR 1900 MWR.   |
|                 | 12.3BC       | This command was integrated into Cisco IOS Release 12.3BC.  |
|                 | 12.0(22)S    | This command was implemented on the Cisco 10000 series Internet routers.                                      |
|                 | 12.2(18)SXE2 | This command was integrated into Cisco IOS Release 12.2(18)SXE2.  |
|                 | 12.2(28)SB   | This command was integrated into Cisco IOS Release 12.2(28)SB.  |
|                 | 12.2(33)SRA  | This command was integrated into Cisco IOS Release 12.2(33)SRA.   |
|                 | 12.2(44)SQ   | This command was integrated into Cisco IOS Release 12.2(44)SQ. Support for the Cisco RF Gateway 10 was added. |
|                 | 12.2(33) SRE | This command was modified. The interchassis subconfiguration mode was added.                                  |

**Usage Guidelines** Use the **redundancy** command to enter redundancy configuration mode, where you can define aspects of redundancy such as shelf redundancy for the Cisco AS5800 universal access server.

### Cisco 10000 Series Router

Before configuring line card redundancy, install the Y-cables. Before deconfiguring redundancy, remove the Y-cables.

The following restrictions apply to line card redundancy on the Cisco 10000 series router:

- Port-level redundancy is not supported.
- Redundant cards must occupy the two subslots within the same physical line card slot.
- The line card that will act as the primary line card must be the first line card configured, and it must occupy subslot 1.

### Cisco 7600 Series Router

From redundancy configuration mode, you can enter the main CPU submode to manually synchronize the configurations that are used by the two supervisor engines.

From the main CPU submode, you can use the **auto-sync** command to use all of the redundancy commands that are applicable to the main CPU.

To select the type of redundancy mode, use the **mode** command.

Nonstop forwarding (NSF) with stateful switchover (SSO) redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, Internetwork Packet Exchange (IPX), and Multiprotocol Label Switching (MPLS).

After you enter redundancy configuration mode, you can use the **interchassis** command to specify the redundancy group number and enter interchassis redundancy mode. In the interchassis redundancy configuration mode, you can do the following:

- Specify a backbone interface for the redundancy group using the **backbone** command.
- Exit from interchassis configuration mode using the **exit** command.
- Specify the IP address of the remote redundancy group member using the **member ip** command.
- Specify the Multichassis LACP (mLACP) node ID, system MAC address, and system priority using the **node-id**, **system-mac**, and **system-priority** commands.
- Define the peer monitoring method using the **monitor** command.

### Cisco uBR10012 Universal Broadband Router

After you enter redundancy configuration mode, you can use the **main-cpu** command to enter main-CPU redundancy configuration mode, which allows you to specify which files are synchronized between the active and standby Performance Routing Engine (PRE) modules.

### Cisco RF Gateway 10

At the redundancy configuration mode, you can do the following:

- Set a command to its default mode using the **default** command.
- Exit from a redundancy configuration using the **exit** command.
- Enter the line card group redundancy configuration using the **linecard-group** command.
- Enter main-CPU redundancy configuration mode using the **main-cpu** command, which allows you to specify which files are synchronized between the active and standby Supervisor cards.
- Configure the redundancy mode for the chassis using the **mode** command.
- Enforce a redundancy policy using the **policy** command.

**Examples**

The following example shows how to enable redundancy mode:

```
Router(config)# redundancy
Router(config-red)#
```

The following example shows how to assign the configured router shelf to the redundancy pair designated as 25. This command must be issued on both router shelves in the redundant router-shelf pair:

```
Router(config)# redundancy
Router(config-red)# failover group-number 25
```

**Cisco 10000 Series Router**

The following example shows how to configure two 4-port channelized T3 half eight line cards that are installed in line card slot 2 for one-to-one redundancy:

```
Router(config)# redundancy
Router(config-r)# linecard-group 1 y-cable
Router(config-r-lc)# member subslot 2/1 primary
Router(config-r-lc)# member subslot 2/0 secondary
```

**Cisco 7600 Series Router**

The following example shows how to enter the main CPU submode:

```
Router(config)# redundancy
Router(config-r)# main-cpu
Router(config-r-mc)#
```

**Cisco uBR10012 Universal Broadband Router**

The following example shows how to enter redundancy configuration mode and display the commands that are available in that mode on the Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# redundancy
Router(config-r)# ?
```

```
Redundancy configuration commands:
  associate  Associate redundant slots
  exit      Exit from redundancy configuration mode
  main-cpu  Enter main-cpu mode
  no       Negate a command or set its defaults
```

The following example shows how to enter redundancy configuration mode and displays its associated commands on the Cisco RFGW-10 chassis:

```
Router# configure terminal
Router(config)# redundancy
Router(config-r)#?
```

```
Redundancy configuration commands:
  default  Set a command to its defaults
  exit    Exit from redundancy configuration mode
  linecard-group  Enter linecard redundancy submode
  main-cpu  Enter main-cpu mode
  mode    redundancy mode for this chassis
  no     Negate a command or set its defaults
  policy  redundancy policy enforcement
```

The following example shows how to enter redundancy configuration mode and its associated commands in the interchassis mode:

```
Router# configure terminal
Router(config)# redundancy
Router(config-r)# ?

Redundancy configuration commands:
  exit          Exit from redundancy configuration mode
  interchassis  Enter interchassis mode
  no            Negate a command or set its defaults

Router(config-r)# interchassis group 100
R1(config-r-ic)# ?

Interchassis redundancy configuration commands:
  backbone      specify a backbone interface for the redundancy group
  exit          Exit from interchassis configuration mode
  member        specify a redundancy group member
  mlacp         mLAGP interchassis redundancy group subcommands
  monitor       define the peer monitoring method
  no            Negate a command or set its defaults
```

### Related Commands

| Command                            | Description  |
|------------------------------------|--|
| <b>associate slot</b>              | Logically associates slots for APS processor redundancy.   |
| <b>auto-sync</b>                   | Enables automatic synchronization of the configuration files in NVRAM.   |
| <b>clear redundancy history</b>    | Clears the redundancy event history log.   |
| <b>linecard-group y-cable</b>      | Creates a line card group for one-to-one line card redundancy.   |
| <b>main-cpu</b>                    | Enters main-CPU redundancy configuration mode for synchronization of the active and standby PRE modules or Supervisor cards.   |
| <b>member subslot</b>              | Configures the redundancy role of a line card.   |
| <b>mode (redundancy)</b>           | Configures the redundancy mode of operation.   |
| <b>redundancy force-switchover</b> | Switches control of a router from the active RP to the standby RP.   |
| <b>show redundancy</b>             | Displays information about the current redundant configuration and recent changes in states or displays current or historical status and related information on planned or logged handovers. |

# reload components

To request that the dial shelf controller (DSC) (or DSCs in a redundant configuration) be reloaded at the same time as a reload on the Router Shelf on the Cisco AS5800, use the **reload components** command in EXEC mode. To cancel a reload, use the **reload components cancel** command.

**reload components** { **all** | *description-line* | **at** *hh:mm* | **in** [*hhh:mmmm*] }

**reload components cancel**

## Syntax Description

|                               |  |
|-------------------------------|--|
| <b>all</b>                    | Reloads all attached components.   |
| <i>description-line</i>       | Displays reason for the reload, 1 to 255 characters in length.   |
| <b>at</b> <i>hh:mm</i>        | Schedules when the software reload takes place using a 24-hour clock. If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within approximately 24 days. |
| <b>in</b> [ <i>hhh:mmmm</i> ] | Schedule a reload of the software to take effect in the specified minutes or (optionally) hours and minutes. The reload must take place within approximately 24 days.  |
| <b>cancel</b>                 | Cancels a scheduled reload.  |

## Command History

| Release  | Modification                 |
|----------|------------------------------|
| 12.1(3)T | This command was introduced. |

## Command Modes

EXEC

## Usage Guidelines

On the Cisco AS5800 only, to request that the DSC (or DSCs in a redundant configuration) be reloaded at the same time as a reload on the Router Shelf, use the **reload components all** command.

You cannot reload from a virtual terminal if the system is not set up for automatic booting. This prevents the system from dropping to the ROM monitor and thereby taking the system out of remote user control.

If you modify your configuration file, the system prompts you to save the configuration. During a save operation, the system asks you if you want to proceed with the save if the CONFIG\_FILE environment variable points to a startup configuration file that no longer exists. If you say “yes” in this situation, the system goes to setup mode upon reload.

When you schedule a reload to occur at a later time, it must take place within approximately 24 days.

The **at** keyword can only be used if the system clock has been set on the router (either through Network Time Protocol (NTP), the hardware calendar, or manually). The time is relative to the configured time zone on the router. To schedule reloads across several routers to occur simultaneously, the time on each router must be synchronized with NTP.

To display information about a scheduled reload, use the **show reload** command.

---

**Examples**

The following example reloads all components on a Cisco AS5800:

```
Router# reload components all
```

---

**Related Commands**

| Command                  | Description                               |
|--------------------------|---|
| <code>show reload</code> | Displays the reload status on the router. |

---

# resource

To assign resources and supported call-types to a customer profile, use the **resource** command in customer profile configuration mode. To disable this function, use the **no** form of this command.

**resource** *name* { **digital** | **speech** | **v110** | **v120** } [*service name*]

**no resource** *name* { **digital** | **speech** | **v110** | **v120** } [*service name*]

## Syntax Description

|                     |  |
|---------------------|--|
| <i>name</i>         | Name for a group of physical resources inside the access server. This name can have up to 23 characters.   |
| <b>digital</b>      | Accepts digital calls. Specifies circuit-switched data calls that terminate on a HDLC framer (unlike asynchronous analog modem call that use start and stop bits). |
| <b>speech</b>       | Accepts speech calls. Specifies normal voice calls, such as calls started by analog modems and standard telephones.  |
| <b>v110</b>         | Accepts V.110 calls.   |
| <b>v120</b>         | Accepts V.120 calls. By specifying this keyword, the access server begins counting the number of v120 software encapsulations occurring in the system.             |
| <b>service name</b> | (Optional) Name for a service profile. This option is not supported for digital or V.120 calls.  |

## Command Default

No resources are assigned to the customer profile by default.

## Command Modes

Customer profile configuration

## Command History

| Release   | Modification                 |
|-----------|------------------------------|
| 12.0(4)XI | This command was introduced. |

## Usage Guidelines

Use the **resource** customer profile configuration command to assign resources and supported call-types to a customer profile. This command specifies a group of physical resources to be used in answering an incoming call of a particular type for a particular customer profile. For example, calls started by analog modems are reciprocated with the **speech** keyword.

## Examples

The following example shows a physical resource group called “modem1”. Forty-eight integrated modems are then assigned to modem1, which is linked to the customer profile called “customer1\_isp”:

```
resource-pool group resource modem1
  range port 1/0 1/47
!
resource-pool profile customer customer1_isp
  resource modem1 speech
```

**Related Commands**

| <b>Command</b>                        | <b>Description</b>          |
|---------------------------------------|-----------------------------|
| <b>resource-pool profile customer</b> | Creates a customer profile. |

# resource-pool

To enable or disable resource pool management, use the **resource-pool** command in global configuration mode.

```
resource-pool { enable | disable }
```

## Syntax Description

|                |                                    |
|----------------|------------------------------------|
| <b>enable</b>  | Enables resource pool management.  |
| <b>disable</b> | Disables resource pool management. |

## Command Default

Resource management is disabled.

## Command Modes

Global configuration

## Command History

| Release   | Modification                 |
|-----------|------------------------------|
| 12.0(4)XI | This command was introduced. |

## Usage Guidelines

Use the **resource-pool** global configuration command to enable and disable the resource pool management feature.

## Examples

The following example shows how to enable RPM:

```
resource-pool enable
```

# resource-pool aaa accounting ppp

To include enhanced start/stop resource manager records to authorization, authentication, and accounting (AAA) accounting, use the **resource-pool aaa accounting ppp** command in global configuration mode. To disable this feature, use the **no** form of this command.

**resource-pool aaa accounting ppp**

**no resource-pool aaa accounting ppp**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled. The default of the **resource-pool enable** command is to *not* enable these new accounting records.

## Command Modes

Global configuration

## Command History

| Release   | Modification                 |
|-----------|------------------------------|
| 12.0(4)XI | This command was introduced. |

## Usage Guidelines

Use the **resource-pool aaa accounting ppp** global configuration command to include enhanced start/stop resource manager records to AAA accounting. The **resource-pool aaa accounting ppp** command adds new resource pool management fields to the AAA accounting start/stop records. The new attributes in the start records are also in the stop records—in addition to those new attributes added exclusively for the stop records.

If you have configured your regular AAA accounting, this command directs additional information from the resource manager into your accounting records.



### Note

If you configure only this command and do not configure AAA accounting, nothing happens. The default functionality for the resource-pool enable command does not include this functionality.

Table 18 shows the new fields that have been added to the start and stop records.

**Table 18 Start and Stop Resource Manager Records**

| New Start Record Fields                | New Stop Record Fields           |
|--|----------------------------------|
| Call-type                              | ModemSpeed-receive               |
| Customer-profile-name                  | ModemSpeed-transmit              |
| Customer-profile-active-sessions       | MLP-session-ID (multilink users) |
| MLP-session-ID (multilink users)       |                                  |
| Resource-group-name                    |                                  |
| Overflow-flag                          |                                  |
| VPDN-tunnel-ID (VPDN users)            |                                  |
| VPDN-homegateway (VPDN users)          |                                  |
| VPDN-domain-name (VPDN users)          |                                  |
| VPDN-group-active-session (VPDN users) |                                  |



**Caution**

This list of newly supported start and stop fields is not exhaustive. Cisco reserves the right to enhance this list of records at any time. Use the **show accounting** command to see the contents of each active session.



**Note**

Cisco recommends that you *thoroughly* understand how these new start/stop records affect your current accounting structure *before* you enter this command.

**Examples**

The following example shows the new AAA accounting start/stop records inserted into an existing AAA accounting infrastructure:

```
resource-pool aaa accounting ppp
```

**Related Commands**

| Command                | Description  |
|------------------------|--|
| <b>show accounting</b> | Allows display of the active accountable events on the network and helps collect information in the event of a data loss on the accounting server. |

# resource-pool aaa protocol

To specify which protocol to use for resource management, use the **resource-pool aaa protocol** command in global configuration mode. To disable this feature and go to local, use the **no** form of this command.

```
resource-pool aaa protocol {local | group name}
```

```
no resource-pool aaa protocol
```

## Syntax Description

|                   |  |
|-------------------|--|
| <b>local</b>      | Local authorization.   |
| <b>group name</b> | Use an external authorization, authentication, and accounting (AAA) server group. The Resource Pool Management Server (RPMS) is defined in a AAA server group. |

## Command Default

Default is set to local authorization.

## Command Modes

Global configuration

## Command History

| Release   | Modification                 |
|-----------|------------------------------|
| 12.0(4)XI | This command was introduced. |

## Usage Guidelines

Use the **resource-pool aaa protocol** global configuration command to specify which protocol to use for resource management. The AAA server group is most useful when you want to have multiple RPMSs configured as a fall-back mechanism.

## Examples

The following example shows how to specify local authorization protocol:

```
resource-pool aaa protocol local
```

# resource-pool call treatment

To set up the signal sent back to the telco switch in response to incoming calls, use the **resource-pool call treatment** command in global configuration mode. To disable this function, use the **no** form of this command.

```
resource-pool call treatment {profile {busy | no-answer} | resource {busy |
channel-not-available}}
```

```
no resource-pool call treatment {profile {busy | no-answer} | resource {busy |
channel-not-available}}
```

## Syntax Description

|                              |   |
|------------------------------|---|
| <b>profile</b>               | Call treatment when profile authorization fails.  |
| <b>busy</b>                  | Answers the call, then sends a busy signal when profile authorization or resource allocation fails. |
| <b>no-answer</b>             | Does not answer the call when profile authorization fails.  |
| <b>resource</b>              | Call treatment when resource allocation fails.  |
| <b>channel-not-available</b> | Sends channel not available (CNA) code when resource allocation fails.                              |

## Command Default

No answer for a customer profile; CNA for a resource.

## Command Modes

Global configuration

## Command History

| Release   | Modification                 |
|-----------|------------------------------|
| 12.0(4)XI | This command was introduced. |

## Usage Guidelines

Use the **resource-pool call treatment** global configuration command to set up the signal sent back to the telco switch in response to incoming calls.

## Examples

The following example configures the device to answer the call and send a busy signal when profile authorization or resource allocation fails:

```
resource-pool call treatment profile busy
```

# resource-pool call treatment discriminator

To modify the signal (ISDN cause code) sent to the switch when a discriminator rejects a call, enter the **resource-pool call treatment discriminator** command in global configuration mode. To disable this function, use the **no** form of this command.

```
resource-pool call treatment discriminator { busy | no-answer | channel-not-available }
```

```
no resource-pool call treatment discriminator { busy | no-answer | channel-not-available }
```

## Syntax Description

|                              |   |
|------------------------------|---|
| <b>busy</b>                  | Answers the call, then sends a busy signal when profile authorization or resource allocation fails. |
| <b>no-answer</b>             | Does not answer the call when profile authorization fails.  |
| <b>channel-not-available</b> | Sends channel not available (CNA) code when resource allocation fails.                              |

## Command Default

No answer for a customer profile; CNA for a resource.

## Command Modes

Global configuration

## Command History

| Release  | Modification                 |
|----------|------------------------------|
| 12.1(5)T | This command was introduced. |

## Usage Guidelines

Use the **resource-pool call treatment discriminator** global configuration command to set up the signal sent back to the telco switch in response to incoming calls.

## Examples

Use the following command to answer the call, but send a busy signal to the switch when profile authorization or resource allocation fails:

```
resource-pool call treatment discriminator busy
```

Use the following command to prevent the call from being answered when profile authorization fails and the discriminator rejects a call:

```
resource-pool call treatment discriminator no-answer
```

# resource-pool group resource

To create a resource group for resource management, use the **resource-pool group resource** command in global configuration mode. To remove a resource group from the running configuration, use the **no** form of this command.

**resource-pool group resource** *name*

**no resource-pool group resource** *name*

## Syntax Description

|             |  |
|-------------|--|
| <i>name</i> | Name for the group of physical resources inside the access server. This name can have up to 23 characters. |
|-------------|--|

## Command Default

No resource groups are set up.

## Command Modes

Global configuration

## Command History

| Release   | Modification                 |
|-----------|------------------------------|
| 12.0(4)XI | This command was introduced. |

## Usage Guidelines

Use the **resource-pool group resource** global configuration command to create a resource group for resource management. When calls come into the access server, they are allocated physical resources as specified within resource groups and customer profiles.

See the **range** command for more information.

If some physical resources are not included in any resource groups, then these remaining resources are not used and are considered to be part of the default resource group. These resources can be used in certain cases to answer calls before profile allocation occurs, but the resources are not used other than in the connection phase.



### Note

For standalone network access server environments, configure resource groups before using them in customer profiles. For external RPMS environments, configure resource groups on the network access server before defining them on external RPMS servers.

When enabling RPM for SS7 signaling, like resources in the network access server (NAS) must be in a single group:

- All modems must be in one group.
- All High-Level Data Link Control (HDLC) controllers must be in a different group.
- All V.110 ASICs must be put into another group.
- All V.120 resources must be in a separate group.

All resource group types must have the same number of resources and that number must equal the number of interface channels available from the public network switch. This grouping scheme prevents the CNA signal from being sent to the signaling point. For SS7 signaling, Microcom and MICA technologies modems must be in the *same* group. If SS7 signaling is not used, Cisco recommends assigning Microcom and MICA modems to separate groups to avoid introducing errors in RPM statistics.

### Examples

The following example shows the configuration options within a resource group:

```
Router(config)# resource-pool group resource modem1
?
Resource Group Configuration Commands:
  default  Set a command to its defaults
  exit     Exit from resource-manager configuration mode
  help     Description of the interactive help system
  no       Negate a command or set its defaults
  range    Configure range for resource

Router(config-resource)# range ?
  limit    Configure the maximum limit
  port     Configure the resource ports

Router(config-resource)# range limit ?
  <1-192>  Maximum number of connections allowed

Router(config-resource)# range port ?
  <0-246>  First Modem TTY Number
  x/y     Slot/Port for Internal Modems
```

### Related Commands

| Command      | Description   |
|--------------|---|
| <b>range</b> | Associates a range of modems or other physical resources with a resource group. |

# resource-pool profile customer

To create a customer profile and to enter customer profile configuration mode, use the **resource-pool profile customer** command in global configuration mode. To delete a customer profile from the running configuration, use the **no** form of this command.

**resource-pool profile customer** *name*

**no resource-pool profile customer** *name*

## Syntax Description

*name* Customer profile name. This name can have up to 23 characters.

## Command Default

No customer profiles are set up.

## Command Modes

Global configuration

## Command History

| Release   | Modification   |
|-----------|--|
| 12.0(4)XI | This command was introduced.   |
| 12.0(5)T  | Support for this command was integrated into Cisco IOS Release 12.0(5)T. |

## Usage Guidelines

Use the **resource-pool profile customer** command to create a customer profile and enter customer profile configuration mode.

VPDN groups can be associated with a customer profile by issuing the **vpdn group** command in customer profile configuration mode.

A VPDN profile can be associated with a customer profile by issuing the **vpdn profile** command in customer profile configuration mode.

VPDN session limits for the VPDN groups associated with a customer profile can be configured in customer profile configuration mode using the **limit base-size** command.

## Examples

The following example shows how to create two VPDN groups, configure the VPDN groups under a VPDN profile named profile1, then associate the VPDN profile with a customer profile named customer12:

```
Router(config)# vpdn-group 1
Router(config-vpdn)#
!
Router(config)# vpdn-group 2
Router(config-vpdn)#
!
Router(config)# resource-pool profile vpdn profile1
Router(config-vpdn-profile)# vpdn group 1
Router(config-vpdn-profile)# vpdn group 2
!
```

```
Router(config)# resource-pool profile customer customer12
Router(config-vpn-customer)# vpn profile profile1
```

**Related Commands**

| <b>Command</b>                      | <b>Description</b>   |
|-------------------------------------|--|
| <b>dnis group</b>                   | Includes a group of DNIS numbers in a customer profile.  |
| <b>limit base-size</b>              | Defines the base number of simultaneous connections that can be done in a single customer or VPDN profile. |
| <b>limit overflow-size</b>          | Defines the number of overflow calls granted to one customer or VPDN profile.                              |
| <b>resource</b>                     | Assigns resources and supported call types to a customer profile.  |
| <b>resource-pool group resource</b> | Creates a resource group for resource management.  |
| <b>vpn group</b>                    | Associates a VPDN group with a customer or VPDN profile.   |
| <b>vpn-group</b>                    | Creates a VPDN group and enters VPDN group configuration mode.   |
| <b>vpn profile</b>                  | Associates a VPDN profile with a customer profile.   |

# resource-pool profile discriminator

To create a call discrimination profile and assign it a name, use the **resource-pool profile discriminator** command in global configuration mode. To remove a call discrimination profile from the running configuration, use the **no** form of this command.

**resource-pool profile discriminator** *name*

**no resource-pool profile discriminator** *name*

## Syntax Description

|             |   |
|-------------|---|
| <i>name</i> | Name of the call discrimination profile created. This name can have up to 23 characters. You can add a calling line ID (CLID) or DNIS group to the discriminator profile created. |
|-------------|---|

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release   | Modification  |
|-----------|---|
| 12.0(4)XI | This command was introduced.  |
| 12.1(5)T  | This command was enhanced to add CLID groups and dialed number identification service (DNIS) groups to a discriminator. |

## Usage Guidelines

Discriminator profiles enable you to process calls differently based on the call type and DNIS or CLID combination. Use the **resource-pool profile discriminator** command to create a call discrimination profile, and then use the **clid group** command to add a CLID group to a discriminator.

To create a call discrimination profile, you must specify both the call type and CLID group. Once a CLID group is associated with a call type in a discriminator, it cannot be used in any other discriminator.

## Examples

The following example shows a call discriminator named `clid1` created and configured to block digital calls from the CLID group named `clid3`:

```
resource-pool profile discriminator clid1
  call-type digital
  clid group clid3
```

## Related Commands

| Command           | Description                                 |
|-------------------|---|
| <b>clid group</b> | Configures a CLID group in a discriminator. |
| <b>dnis group</b> | Configures a DNIS group in a discriminator. |

# resource-pool profile service

To set up the service profile configuration, use the **resource-pool profile service** command in global configuration mode. To disable this function, use the **no** form of this command.

**resource-pool profile service** *name*

**no resource-pool profile service** *name*

---

**Syntax Description**

|             |   |
|-------------|---|
| <i>name</i> | Service profile name. This name can have up to 23 characters. |
|-------------|---|

---

---

**Command Default**

No service profiles are set up.

---

**Command Modes**

Global configuration

---

**Command History**

| Release   | Modification                 |
|-----------|------------------------------|
| 12.0(4)XI | This command was introduced. |

---

---

**Usage Guidelines**

Use the **resource-pool profile service** global configuration command to set up the service profile configuration.

---

**Examples**

The following example shows the creation of a service profile called user1:

```
resource-pool profile service user1
```

# resource-pool profile vpdn

To create a virtual private dialup network (VPDN) profile and to enter VPDN profile configuration mode, use the **resource-pool profile vpdn** command in global configuration mode. To disable this function, use the **no** form of this command.

**resource-pool profile vpdn** *name*

**no resource-pool profile vpdn** *name*

|                           |             |                    |
|---------------------------|-------------|--------------------|
| <b>Syntax Description</b> | <i>name</i> | VPDN profile name. |
|---------------------------|-------------|--------------------|

|                        |                              |
|------------------------|------------------------------|
| <b>Command Default</b> | No VPDN profiles are set up. |
|------------------------|------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

| <b>Command History</b> | <b>Release</b>   | <b>Modification</b>          |
|------------------------|--|------------------------------|
|                        | 12.0(4)XI  | This command was introduced. |
| 12.0(5)T               | Support for this command was integrated into Cisco IOS Release 12.0(5)T. |                              |

**Usage Guidelines**

Use the **resource-pool profile vpdn** command to create a VPDN profile and enter VPDN profile configuration mode, or to enter VPDN profile configuration mode for a VPDN profile that already exists. VPDN groups can be associated with a VPDN profile using the **vpdn group** command in VPDN profile configuration mode. A VPDN profile will count VPDN sessions across all associated VPDN groups. VPDN session limits for the VPDN groups associated with a VPDN profile can be configured in VPDN profile configuration mode using the **limit base-size** command.

**Examples**

The following example creates the VPDN groups named l2tp and l2f, and associates both VPDN groups with the VPDN profile named profile32:

```
Router(config)# vpdn-group l2tp
Router(config-vpdn)#
!
Router(config)# vpdn-group l2f
Router(config-vpdn)#
!
Router(config)# resource-pool profile vpdn profile32
Router(config-vpdn-profile)# vpdn group l2tp
Router(config-vpdn-profile)# vpdn group l2f
```

**Related Commands**

| <b>Command</b>             | <b>Description</b>   |
|----------------------------|--|
| <b>limit base-size</b>     | Defines the base number of simultaneous connections that can be done in a single customer or VPDN profile. |
| <b>limit overflow-size</b> | Defines the number of overflow calls granted to one customer or VPDN profile.                              |
| <b>vpdn group</b>          | Associates a VPDN group with a customer or VPDN profile.   |
| <b>vpdn-group</b>          | Creates a VPDN group and enters VPDN group configuration mode.   |
| <b>vpdn profile</b>        | Associates a VPDN profile with a customer profile.   |

# retry keepalive

To enable Redundant Link Manager (RLM) keepalive retries, use the **retry keepalive** command in RLM configuration mode. To disable this function, use the **no** form of this command.

**retry keepalive** *number-of-times*

**no retry keepalive** *number-of-times*

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <i>number-of-times</i> Number of keepalive failures allowed before the link is declared down, from 1 to 100. |
|---------------------------|--|

|                        |                       |
|------------------------|-----------------------|
| <b>Command Default</b> | Default retries is 3. |
|------------------------|-----------------------|

|                      |                   |
|----------------------|-------------------|
| <b>Command Modes</b> | RLM configuration |
|----------------------|-------------------|

|                        |                |                              |
|------------------------|----------------|------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|                        | 11.3(7)        | This command was introduced. |

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | RLM allows keepalive failures in consecutive certain amounts of time configured using the command line interface (CLI) before it declares the link is down. |
|-------------------------|---|

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example sets RLM keepalive retries to 88:<br><pre>retry keepalive 88</pre> |
|-----------------|--|

|                         |                                       |  |
|-------------------------|---------------------------------------|--|
| <b>Related Commands</b> | <b>Command</b>                        | <b>Description</b>   |
|                         | <b>clear interface virtual-access</b> | Resets the hardware logic on an interface.   |
|                         | <b>clear rlm group</b>                | Clears all RLM group time stamps to zero.  |
|                         | <b>interface</b>                      | Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode. |
|                         | <b>link (RLM)</b>                     | Specifies the link preference.   |
|                         | <b>protocol rlm port</b>              | Reconfigures the port number for the basic RLM connection for the whole rlm-group.                             |
|                         | <b>server (RLM)</b>                   | Defines the IP addresses of the server.  |
|                         | <b>show rlm group statistics</b>      | Displays the network latency of the RLM group.   |
|                         | <b>show rlm group status</b>          | Displays the status of the RLM group.  |
|                         | <b>show rlm group timer</b>           | Displays the current RLM group timer values.   |

| <b>Command</b>        | <b>Description</b>                                |
|-----------------------|---|
| <b>shutdown (RLM)</b> | Shuts down all of the links under the RLM group.  |
| <b>timer</b>          | Overwrites the default setting of timeout values. |

# rotary

To define a group of lines consisting of one or more virtual terminal lines or one auxiliary port line, use the **rotary** command in line configuration mode. To remove a group of lines from a rotary group, use the **no** form of this command.

```
rotary group [queued [by-role]] [round-robin]
```

```
no rotary group [queued [by-role]] [round-robin]
```

## Syntax Description

|                    |   |
|--------------------|---|
| <i>group</i>       | Rotary group number.  |
| <b>queued</b>      | (Optional) Specifies queueing a connection request to a rotary group.   |
| <b>by-role</b>     | (Optional) Enables priority users to move to the head of the queue.   |
| <b>round-robin</b> | (Optional) Selects a round-robin port selection algorithm instead of the default linear port selection algorithm. |

## Command Default

No group of lines is defined.

## Command Modes

Line configuration

## Command History

| Release   | Modification                              |
|-----------|---|
| 10.0      | This command was introduced.              |
| 12.1(1)T  | The <b>queued</b> keyword was added.      |
| 12.1(2)T  | The <b>round-robin</b> keyword was added. |
| 12.2(15)T | The <b>by-role</b> keyword was added.     |

## Usage Guidelines

Connections to a rotary group can take advantage of the following features:

- Clear To Send (CTS)—If a line in a rotary group is configured to require CTS, the Cisco IOS software ignores that line when CTS from the attached device is low. This feature enables the software to avoid inactive host ports automatically. To enable this feature, use the **modem bad** line configuration command.
- EIA/TIA-232 handshaking—Rotary groups are often associated with large terminal switches that require an EIA/TIA-232 handshake before forming a connection. In this case, use the **modem callout** line configuration command to configure the lines in the group. If the EIA/TIA-232 handshake fails on a line, the Cisco IOS software steps to the next free line in the rotary group and restarts the negotiation.
- Access control—You can use access lists for groups of virtual terminal lines.
- Session timeout—Use the **session-timeout** line configuration command to set an interval for a line so that if no activity occurs on a remotely initiated connection for that interval, the Cisco IOS software closes the connection. The software assumes that the host has crashed or is otherwise inaccessible.

Typically, rotary groups are used on devices with multiple modem connections to allow connection to the next free line in a hunt group. In the event that there are no free asynchronous ports, the **queued** keyword enables outgoing connection requests to be queued until a port becomes available. Periodic messages are sent to users to update them on the status of their connection request.

For a nonqueued connection request, the remote host must specify a particular TCP port on the router to connect to a rotary group with connections to an individual line. The available services are the same, but the TCP port numbers are different. Table 19 lists the services and port numbers for both rotary groups and individual lines.

**Table 19 Services and Port Numbers for Rotary Groups and Lines**

| Services Provided                     | Base TCP Port for Rotaries | Base TCP Port for Individual Lines |
|---------------------------------------|----------------------------|------------------------------------|
| Telnet protocol                       | 3000                       | 2000                               |
| Raw TCP protocol (no Telnet protocol) | 5000                       | 4000                               |
| Telnet protocol, binary mode          | 7000                       | 6000                               |
| XRemote protocol                      | 10000                      | 9000                               |

For example, if Telnet protocols are required, the remote host connects to the TCP port numbered 3000 (decimal) plus the rotary group number. If the rotary group identifier is 13, the corresponding TCP port is 3013.

If a raw TCP stream is required, the port is 5000 (decimal) plus the rotary group number. If rotary group 5 includes a raw TCP (printer) line, the user connects to port 5005 and is connected to one of the raw printers in the group.

If Telnet binary mode is required, the port is 7000 (decimal) plus the rotary group number.

The **by-role** keyword enables priority users to bypass the queue and access the first available line.



**Note**

Priority users must have the privilege level of administrator(PRIV\_ROOT) to take advantage of this option.

The round-robin selection algorithm enabled by the **round-robin** keyword improves the utilization of tty ports. When looking for the next available port, the default linear hunting algorithm will not roll over to the next port if the first port it finds is bad. This failure to roll over to the next port results in an inequitable utilization of the tty ports on a router. The round-robin hunting algorithm will roll over bad ports instead of retrying them.



**Note**

The **round-robin** option must be configured for all the lines in a rotary group.

**Examples**

The following example establishes a rotary group consisting of virtual terminal lines 2 through 4 and defines a password on those lines. By using Telnet to connect to TCP port 3001, the user gets the next free line in the rotary group. The user need not remember the range of line numbers associated with the password.

```
line vty 2 4
 rotary 1
```

```
password letmein
login
```

The following example enables asynchronous rotary line queuing:

```
line 1 2
 rotary 1 queued
```

The following example enables asynchronous rotary line queuing using the round-robin algorithm:

```
line 1 2
 rotary 1 queued round-robin
```

#### Related Commands

| Command                | Description  |
|------------------------|--|
| <b>login (line)</b>    | Enables password checking at login and defines the method (local or TACACS+).                    |
| <b>modem bad</b>       | Removes an integrated modem from service and indicates it as suspect or proven to be inoperable. |
| <b>modem callout</b>   | Configures a line for reverse connections.   |
| <b>modem dialin</b>    | Configures a line to enable a modem attached to the router to accept incoming calls only.        |
| <b>session-timeout</b> | Sets the interval for closing the connection when there is no input or output traffic.           |

# rotary-group

To assign a request-dialout virtual private dialup network (VPDN) subgroup to a dialer rotary group, use the **rotary-group** command in request-dialout configuration mode. To remove the request-dialout VPDN subgroup from the dialer rotary group, use the **no** form of this command.

**rotary-group** *group-number*

**no rotary-group** [*group-number*]

## Syntax Description

*group-number* The dialer rotary group that this VPDN group belongs to.

## Command Default

Disabled

## Command Modes

Request-dialout configuration

## Command History

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

## Usage Guidelines

If the dialer pool or dialer rotary group that the VPDN group is in contains physical interfaces, the physical interfaces will be used before the VPDN group.

You must first enable the **protocol l2tp** command on the request-dialout VPDN subgroup before you can enable the **rotary-group** command. Removing the **protocol l2tp** command will remove the **rotary-group** command from the request-dialout subgroup.

You can only configure one dialer profile pool (using the **pool-member** command) or dialer rotary group (using the **rotary-group** command). If you attempt to configure a second dialer resource, you will replace the first dialer resource in the configuration.

## Examples

The following example configures VPDN group 1 to request Layer 2 Tunnel Protocol (L2TP) dial-out to IP address 172.16.4.6 using dialer profile pool 1 and identifying itself using the local name router32.

```
vpdn-group 1
 request-dialout
  protocol l2tp
  rotary-group 1
 initiate-to ip 172.16.4.6
 local name router32
```

| Related Commands | Command                | Description  |
|------------------|------------------------|--|
|                  | <b>initiate-to</b>     | Specifies the IP address that will be tunneled to.           |
|                  | <b>pool-member</b>     | Assigns a request-dialout VPDN subgroup to a dialer pool.    |
|                  | <b>protocol (VPDN)</b> | Specifies the L2TP that the VPDN subgroup will use.          |
|                  | <b>request-dialout</b> | Enables an LNS to request VPDN dial-out calls by using L2TP. |