

# disconnect

To disconnect a line, use the **disconnect** command in EXEC mode.

**disconnect** [*connection*]

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <i>connection</i> (Optional) Number of the line or name of the active network connection to be disconnected. |
|---------------------------|--|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

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

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | Do not disconnect a line to end a session. Instead, log off the host, so that the Cisco IOS software can clear the connection. Then end the session. If you cannot log out of an active session, disconnect the line. |
|-------------------------|---|

|                 |  |
|-----------------|--|
| <b>Examples</b> | In the following example, the user disconnects from the device Slab to return to the router: |
|-----------------|--|

```
Slab% disconnect
Connection closed by remote host
```

|                         |                     |                                       |
|-------------------------|---------------------|---------------------------------------|
| <b>Related Commands</b> | <b>Command</b>      | <b>Description</b>                    |
|                         | <b>login (EXEC)</b> | Enables or changes a login user name. |

## dnis (VPDN)

To specify the Dialed Number Identification Service (DNIS) group name or DNIS number of users that are to be forwarded to a tunnel server using a virtual private dialup network (VPDN), use the **dnis** command in request dial-in VPDN subgroup configuration mode. To remove a DNIS group or number from a VPDN group, use the **no** form of this command.

```
dnis {dnis-group-name | dnis-number}
```

```
no dnis {dnis-group-name | dnis-number}
```

### Syntax Description

|                        |   |
|------------------------|---|
| <i>dnis-group-name</i> | DNIS group name used when resource pool management (RPM) is enabled and the VPDN group is configured under the incoming customer profile.                     |
| <i>dnis-number</i>     | DNIS group number used when RPM is disabled, or when a call is associated with a customer profile without any VPDN group configured for the customer profile. |

### Defaults

Disabled

### Command Modes

Request dial-in VPDN subgroup configuration

### Command History

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

### Usage Guidelines

You must specify a tunneling protocol using the **protocol** command in request dial-in VPDN subgroup configuration mode before issuing the **dnis** command. Removing or changing the **protocol** command configuration removes any existing **dnis** command configuration from the request dial-in VPDN subgroup.

You can configure a VPDN group to tunnel multiple DNIS group names and DNIS numbers by issuing multiple instances of the **dnis** command.

VPDN groups can also be configured to tunnel users based on domain name using the **domain** command.

### Examples

The following example configures a VPDN group to tunnel calls from multiple DNIS numbers and from the domain cisco.com to the tunnel server at 10.1.1.1 using the Layer 2 Forwarding (L2F) protocol:

```
Router(config)# vpdn-group users
Router(config-vpdn)# request dialin
Router(config-vpdn-req-in)# protocol l2f
Router(config-vpdn-req-in)# dnis 1234
Router(config-vpdn-req-in)# dnis 5678
Router(config-vpdn-req-in)# domain cisco.com
!
Router(config-vpdn)# initiate-to 10.1.1.1
```

| Related Commands | Command                  | Description   |
|------------------|--------------------------|---|
|                  | <b>dialer dnis group</b> | Creates a DNIS group.   |
|                  | <b>domain</b>            | Specifies the domain name of users that are to be forwarded to a tunnel server using VPDN.  |
|                  | <b>dnis group</b>        | Includes a group of DNIS numbers in a customer profile.   |
|                  | <b>protocol (VPDN)</b>   | Specifies the tunneling protocol that the VPDN subgroup will use.   |
|                  | <b>request-dialin</b>    | Creates a request dial-in VPDN subgroup that configures a NAS to request the establishment of a dial-in tunnel to a tunnel server, and enters request dial-in VPDN subgroup configuration mode. |

# dnis group

To include a group of Dialed Number Identification Service (DNIS) numbers in a customer profile, use the **dnis group** command in customer profile configuration mode. To remove a DNIS group from a customer profile, use the **no** form of this command.

```
dnis group { default | name dnis-group-name }
```

```
no dnis group { default | name dnis-group-name }
```

## Syntax Description

|                        |  |
|------------------------|--|
| <b>default</b>         | Allows a specified customer profile to accept all DNIS numbers coming into the access server. For example, a stray DNIS number not listed in any customer profile passes through this default DNIS group. Most customer profiles do not have this option configured. |
| <b>name</b>            | Assigns a name to a DNIS group.  |
| <i>dnis-group-name</i> | DNIS group name. It can have up to 23 characters.  |

## Defaults

No DNIS groups are associated with a customer profile.

## Command Modes

Customer profile configuration

## Command History

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

## Usage Guidelines

Use the **dnis group** customer profile configuration command to include a group of DNIS numbers in a customer profile or discriminator.

## Examples

The following example includes the DNIS group called customer1dnis in the customer1 customer profile:

```
resource-pool profile customer customer1
  dnis group customer1dnis
```

## Related Commands

| Command                               | Description                 |
|---------------------------------------|-----------------------------|
| <b>dialer dnis group</b>              | Creates a DNIS group.       |
| <b>resource-pool profile customer</b> | Creates a customer profile. |

# domain

To specify the domain name of users that are to be forwarded to a tunnel server using a virtual private dialup network (VPDN), use the **domain** command in request dial-in VPDN subgroup configuration mode. To remove a domain from a VPDN group or subgroup, use the **no** form of this command.

**domain** *domain-name*

**no domain** [*domain-name*]

## Syntax Description

*domain-name* Case-sensitive name of the domain that will be tunneled.

## Defaults

Disabled

## Command Modes

Request dial-in VPDN subgroup configuration

## Command History

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

## Usage Guidelines

You must specify a tunneling protocol using the **protocol** command in request dial-in VPDN subgroup configuration mode before issuing the **domain** command. Removing or changing the **protocol** command configuration removes any existing **domain** command configuration from the request dial-in VPDN subgroup.

You can configure a request dial-in VPDN subgroup to tunnel calls from multiple domain names by issuing multiple instances of the **domain** command.

VPDN groups can also be configured to tunnel users based on Dialed Number Identification Service (DNIS) group names or DNIS numbers using the **dnis** command.

## Examples

The following example configures VPDN group 1 to request a dial-in Layer 2 Tunnel Protocol (L2TP) tunnel to IP address 10.99.67.76 when it receives a PPP call from a username with the domain name cisco1.com, the domain name cisco2.com, or the DNIS number 4321:

```
Router(config)# vpdn-group 1
Router(config-vpdn)# request-dialin
Router(config-vpdn-req-in)# protocol l2tp
Router(config-vpdn-req-in)# domain cisco1.com
Router(config-vpdn-req-in)# domain cisco2.com
Router(config-vpdn-req-in)# dnis 4321
!
Router(config-vpdn)# initiate-to ip 10.99.67.76
```

**Related Commands**

| <b>Command</b>         | <b>Description</b>  |
|------------------------|---|
| <b>dnis</b>            | Specifies the DNIS group name or DNIS number of users that are to be forwarded to a tunnel server using VPDN.   |
| <b>protocol (VPDN)</b> | Specifies the tunneling protocol that the VPDN subgroup will use.   |
| <b>request-dialin</b>  | Creates a request dial-in VPDN subgroup that configures a NAS to request the establishment of a dial-in tunnel to a tunnel server, and enters request dial-in VPDN subgroup configuration mode. |

## ds0 busyout (channel)

To busyout one or more digital signal level 0s (DS0s), use the **ds0 busyout** command in controller configuration mode. To cancel busyout on a DS0, use the **no** form of this command.

**ds0 busyout** *ds0*

**no ds0 busyout** *ds0*

|                           |            |   |
|---------------------------|------------|---|
| <b>Syntax Description</b> | <i>ds0</i> | DS0 number listed as a single channel or channel range. The range of numbers can be from 1 to 24 for T1. For example, from 1 to 10, or from 10 to 24. |
|---------------------------|------------|---|

|                 |          |
|-----------------|----------|
| <b>Defaults</b> | Disabled |
|-----------------|----------|

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

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>  |
|------------------------|----------------|--|
|                        | 11.3(2)AA      | This command was introduced, and supported T1 and T3 only.   |
|                        | 12.0           | This command was integrated into Cisco IOS Release 12.0, and supported the E1 and DMM HMM (Double Modem Module [12] Hex Modem Module [6]). |

**Usage Guidelines**

Use the **ds0 busyout** command when you to busyout a one or more DS0s (channels). If there is an active call, the software waits until the call terminates by a disconnection; then the DS0 is busied out. First you must specify the T1 line (port) containing the 24 DS0s, using the **controller T1** command.

To busyout all DS0s on a trunk card or all modems on a modem card, use the **busyout** privileged EXEC command.

To display the busyout information, use the **show busyout** privileged EXEC command.



**Note**

The **ds0 busyout** command only applies to **cas-group** command configurations for channel-associated signaling. This command has no effect on **pri-group** command configurations.

**Examples**

In this example, the controller T1 is configured with cas-group (channel-associated signaling). The following example removes DS0s 1 through 10 from dialup services. These DS0s are assigned to the T1 port (line) in shelf 6, slot 0, port 0:

```
controller t1 6/0/0
 ds0 busyout 1-10
 exit
```

**Related Commands**

| <b>Command</b>                 | <b>Description</b>   |
|--------------------------------|--|
| <b>busyout</b>                 | Informs the central-office switch that a channel is out of service.  |
| <b>modem busyout</b>           | Disables a modem from dialing or answering calls whereby the disabling action is not executed until the active modem returns to an idle state. |
| <b>modem busyout-threshold</b> | Maintains a balance between the number of DS0s and modems.   |
| <b>modem shutdown</b>          | Abruptly shuts down an active or idle modem installed in an access server or router.   |
| <b>show busyout</b>            | Displays the busyout status for a card on the dial shelf.  |
| <b>show dial-shelf</b>         | Displays information about the dial shelf, including clocking information.   |

# ds0 busyout-threshold

To define a threshold to maintain a balance between the number of DS0s and modems, use the **ds0 busyout-threshold** command in global configuration mode. To remove the threshold, use the **no** form of this command.

## Cisco AS5300 and AS5800 Access Servers Only

**ds0 busyout-threshold** *threshold-number*

**no ds0 busyout-threshold** *threshold-number*



### Note

This command is the same as the **modem busyout-threshold** command for the Cisco AS5350 and AS5400 access servers.

### Syntax Description

|                         |  |
|-------------------------|--|
| <i>threshold-number</i> | Number of modems that are free when the router should enforce the stipulation that the number of free DS0 lines is less than or equal to the number of modems. |
|-------------------------|--|

### Command Modes

Global configuration

### Command History

| Release   | Modification   |
|-----------|--|
| 11.3(2)AA | This command was introduced as <b>modem busyout-threshold</b> .  |
| 12.2      | This command was changed to <b>ds0 busyout-threshold</b> for the Cisco AS5300 and AS5800 access servers. |

### Usage Guidelines

The **ds0 busyout-threshold** command functionality is also often termed **autobusyout**. This command applies to all DS0 lines coming into the router and counts all free modems in all pools.

The **ds0 busyout-threshold** command periodically checks to see if the number of free modems is less than the user specified threshold and if it is it ensures the number of free DS0 channels is less than or equal to the number of modems.

This command should only be used where excess calls to one router are forwarded by the exchange to an additional router on the same exchange group number.

Since the **ds0 busyout-threshold** command checks only periodically, the threshold should be greater than the number of calls the user expects to receive in 1 minute plus a safety margin. For example, if the user receives an average of 10 calls per minute, then a threshold of 20 would be advised. Very small thresholds should be avoided since they do not allow sufficient time for the exchange to respond to out-of-service notifications from the router, and callers may receive busy signals when free modems are all used.

**Caution**

The number of DS0 lines in normal operating conditions should be approximately equal to the number of modems (for example, within 30). If it is not, this will cause a lot of messaging traffic to the exchange and may cause active calls to be dropped. This is not a concern for short periods, that is, when modem cards are replaced.

On T3 controllers, any contained T1 controllers that are not in use should be undeclared to remove them from the **autobusyout** list.

**Examples**

The following example shows how you might configure the **ds0 busyout-threshold** command:

```
ds0 busyout-threshold 30
```

**Related Commands**

| Command                      | Description  |
|------------------------------|--|
| <b>busyout</b>               | Informs the central-office switch that a channel is out-of-service.  |
| <b>ds0 busyout (channel)</b> | Forces a DS0 timeslot on a controller into the busyout state.  |
| <b>modem busyout</b>         | Disables a modem from dialing or answering calls whereby the disabling action is not executed until the active modem returns to an idle state. |
| <b>modem shutdown</b>        | Abruptly shuts down an active or idle modem installed in an access server or router.   |

## ds0-group (controller e1)

To define E1 channels for compressed voice calls and the channel-associated signaling (CAS) method by which the router connects to the PBX or PSTN, enter the **ds0-group** command in controller configuration mode. To remove the group and signaling setting, use the **no** form of this command.

**ds0-group** *channel* **timeslots** *range* **type** *signal*

**no ds0-group** *channel* **timeslots** *range* **type** *signal*

### Syntax Description

|                               |   |
|-------------------------------|---|
| <i>channel</i>                | Specifies a single channel group number. Replace the <i>channel</i> variable with a number from 0 through 30.   |
| <b>timeslots</b> <i>range</i> | Specifies a time-slot range, which can be from 1 through 31. You can specify a time-slot range (for example, 1-31), individual time-slots separated by commas (for example 1, 3, 5), or a combination of the two (for example 1-14, 15, 17-31). The sixteenth time slot is reserved for out-of-band signaling.  |
| <b>type</b> <i>signal</i>     | Specifies the type of channel-associated signaling. Configure the signal type that your central office uses. Replace the <i>signal</i> argument with one of the following signal types: <ul style="list-style-type: none"> <li>• <b>r2-analog</b> [<b>r2-compelled</b> [ani]   <b>r2-non-compelled</b> [ani]   <b>r2-semi-compelled</b> [ani]]</li> <li>• <b>r2-digital</b> [<b>r2-compelled</b> [ani]   <b>r2-non-compelled</b> [ani]   <b>r2-semi-compelled</b> [ani]]</li> <li>• <b>r2-pulse</b> [<b>r2-compelled</b> [ani]   <b>r2-non-compelled</b> [ani]   <b>r2-semi-compelled</b> [ani]]</li> </ul> |

The following descriptions are provided for the previous three R2 syntax bullets:

**r2-analog**—Specifies R2 ITU Q411 analog line signaling, which reflects the on/off switching of a tone in frequency-division multiplexing circuits (before TDM circuits were created). The tone is used for line signaling.

**r2-digital**—Specifies R2 ITU Q421 digital line signaling, which is the most common signaling configuration. The A and B bits are used for line signaling.

**r2-pulse**—Specifies R2 ITU supplement 7 pulse line signaling, which is a transmitted pulse that indicates a change in the line state.

**r2-compelled** [ani]—Specifies R2 compelled register signaling. You can also specify provisioning the ANI address option.

**r2-non-compelled** [ani]—Specifies R2 noncompelled register signaling.

**r2-semi-compelled** [ani]—Specifies R2 semicompelled register signaling.

### Defaults

No channel-associated signaling is configured on the controller. All R2 signaling types have DNIS turned on by default.

**Command Modes** Controller configuration

| Command History | Release                | Modification  |
|-----------------|------------------------|---|
|                 | 11.3 MA                | The command was introduced as the <b>voice-group</b> command on the Cisco MC3810 concentrator.                            |
|                 | 12.0(5)XK and 12.0(7)T | The command was implemented on the Cisco 2600 and Cisco 3600 series with a different name and some keyword modifications. |
|                 | 12.1(2)XH and 12.1(3)T | The command was modified for E1 R2 signaling.   |

**Usage Guidelines** Use this command to configure support for incoming and outgoing call signals (such as on-hook and off-hook) on each E1 controller.

If you specify the time-slot range 1-31, the system software automatically uses the sixteenth time slot to transmit the channel-associated signaling.

The signaling you configure on the access server must match the signaling used by the central office. For example, if the central office switch is forwarding R2 analog signaling to a Cisco 2600 or 3600 series router, the E1 controller on the router must also be configured for R2 analog signaling (**r2-analog**).

All R2 signaling options have DNIS support turned on by default. If you enable the **ani** option, the collection of DNIS information is still performed. Specifying the **ani** option does not disable DNIS. DNIS is the number being called. ANI is the caller's number. For example, if you are configuring router A to call router B, the DNIS number is router B and the ANI number is router A. ANI is very similar to Caller ID.

To customize the R2 signaling parameters, refer to the **cas-custom** controller configuration command. When you enable the **ds0-group** command, the **cas-custom** command is automatically set up to be polled for configuration information. However, unless you enable or turn on specific features with the **ds0-custom** command, the cas-custom feature has an empty set of signaling parameters.

DNIS is automatically collected for modem pools and R2 tone signaling. You do not need to specify the collection of DNIS information with the **ds0-group** command. However, if you are using non-R2 tone signaling, the system must be manually configured to collect DNIS information. For non-R2 CAS signaling, DNIS collection is done only for E&M-fgb.

**Examples** In most cases, you will configure the same channel-associated signaling on each E1 controller. The following examples configure signaling and customized parameters on controller E1 2 using the **ds0-group** and **cas-custom** controller configuration commands.

The actual channel-associated signaling is configured on the sixteenth time slot, which is the reason why this time slot does not come up in the following output.

```
Router(config)# controller e1 2
Router(config-controller)# ds0-group 1 timeslots 1-31 type r2-digital r2-compelled ani
Router(config-controller)#

%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 1 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 2 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 3 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 4 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 5 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 6 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 7 is up
```

```

%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 8 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 9 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 10 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 11 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 12 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 13 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 14 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 15 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 17 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 18 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 19 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 20 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 21 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 22 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 23 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 24 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 25 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 26 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 27 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 28 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 29 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 30 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 31 is up

```

The following example shows all the supported E1 signaling types on a Cisco 2600 or 3600 series router.

```
Router(config-controller)# ds0-group 1 timeslots 1-31 type ?
```

```

e&m-fgb          E & M Type II FGB
e&m-fgd          E & M Type II FGD
e&m-immediate-start E & M Immediate Start
fxs-ground-start FXS Ground Start
fxs-loop-start   FXS Loop Start
p7              P7 Switch
r2-analog       R2 ITU Q411
r2-digital      R2 ITU Q421
r2-pulse        R2 ITU Supplement 7
sas-ground-start SAS Ground Start
sas-loop-start  SAS Loop Start

```

```
Router(config-controller)# cas-group 1 timeslots 1-31 type r2-analog ?
```

```

r2-compelled      R2 Compelled Register Signalling
r2-non-compelled  R2 Non Compelled Register Signalling
r2-semi-compelled R2 Semi Compelled Register Signalling
<cr>

```

R2 signaling parameters can be customized with the **cas-custom** controller configuration command:

```
Router(config-controller)# cas-custom 1
```

```
Router(config-ctrl-cas)# ?
```

CAS custom commands:

```

caller-digits  Digits to be collected before requesting CallerID
category       Category signal
country        Country Name
default        Set a command to its defaults
exit           Exit from cas custom mode
invert-abcd    invert the ABCD bits before tx and after rx
metering       R2 network is sending metering signal
nc-congestion  Non Compelled Congestion signal
no             Negate a command or set its defaults

```

# encapsulation cpp



## Note

Effective with release 12.3(4)T, the **encapsulation cpp** command is no longer available in Cisco IOS software.

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

**encapsulation cpp**

**no encapsulation cpp**

## Syntax Description

This command has no arguments or keywords.

## Defaults

CPP encapsulation disabled.

## Command Modes

Interface configuration

## Command History

| Release  | Modification   |
|----------|--|
| 11.2     | This command was introduced.   |
| 12.3(4)T | This command was removed and is no longer available in Cisco IOS software. |

## Usage Guidelines

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

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

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

This command is supported on ISDN BRIs and PRIs only.

## Examples

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

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

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

```
controller t1 1/1
  framing esf
  linecode b8zs
  pri-group timeslots 1-23
  isdn switchtype primary-4ess
!
interface Serial1/1:23
  encapsulation cpp
  cpp callback accept
  cpp authentication
```

---

**Related Commands**

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

---

# encryption mppe

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

**encryption mppe**

**no encryption mppe**

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

**Command Default** IPSec is the default encryption type.

**Command Modes** Controller configuration

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

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

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

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

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

| Related Commands | Command                | Description                                      |
|------------------|------------------------|--|
|                  | <b>debug ppp mppe</b>  | Displays debug messages for MPPE events.         |
|                  | <b>encryption mppe</b> | Enables MPPE encryption on the virtual template. |
|                  | <b>show ppp mppe</b>   | Displays MPPE information for an interface.      |

# failover group-number

To configure shelf redundancy for Cisco AS5800 universal access servers, use the **failover group-number** command in redundancy configuration mode. To disable redundancy, use the **no** form of this command.

**failover group-number** *group-code*

**no failover group-number** *group-code*

## Syntax Description

|                   |   |
|-------------------|---|
| <i>group-code</i> | The failover group code. An integer that identifies a redundant pair of router shelves. Each member of the pair must be configured with the same group code. When failover mode is enabled, this group code is sent in place of the router MAC address. |
|-------------------|---|

## Defaults

Redundancy is not enabled.

## Command Modes

Redundancy configuration

## Command History

| Release    | Modification  |
|------------|---|
| 12.1(5)XV1 | This command was introduced.                                  |
| 12.2(11)T  | This command was integrated into Cisco IOS Release 12.2(11)T. |

## Usage Guidelines

This command must be configured on both router shelves. The *group-code* argument is used by the system controller and must be the same for both router shelves forming the redundant pair.

For successful failover to occur, both router-shelf configurations must be synchronized. Configure each router shelf separately, as active and backup respectively, with the same configuration except for the IP address on egress interfaces.



### Note

Test the backup router shelf configuration before deployment in a production environment.

## Examples

The following example assigns the configured router shelf to the redundancy pair designated as 25. These commands must be issued on both router shelves in the redundant router-shelf pair:

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

**Related Commands**

| <b>Command</b>         | <b>Purpose</b>  |
|------------------------|---|
| <b>redundancy</b>      | Enters redundancy mode for further configuration.   |
| <b>show redundancy</b> | Displays current or historical status and related information and displays shelf-redundancy status. |

# firmware location

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

**firmware location** [*IFS*:[*/*]]*filename*

**no firmware location**

## Syntax Description

|                 |  |
|-----------------|--|
| <i>IFS</i> :    | (Optional) IOS file specification (IFS), which can be any valid IFS on any local file system. Examples of legal specifications include: <ul style="list-style-type: none"> <li>• <b>bootflash:</b>—Loads the firmware from a separate Flash memory device.</li> <li>• <b>flash:</b>—Loads the firmware from the Flash NVRAM located within the router.</li> <li>• <b>system:/</b>—Loads the firmware from a built-in file within the Cisco IOS image. The optional forward slash (<i>/</i>) and system path must be entered with this specification.</li> </ul> <p>Use the <b>dir all-file systems</b> EXEC command to display legal IFSs.</p> |
| <i>filename</i> | The firmware filename. When <i>filename</i> is entered without an IFS specification, this name defaults to the file in Flash memory.   |

## Defaults

Downloads SPE firmware in Flash memory.

## Command Modes

SPE configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.0(4)XI1 | This command was introduced on the Cisco AS5200, Cisco AS5300, and Cisco AS5800.   |
| 12.0(6)T   | This command was integrated into Cisco IOS Release 12.0(6)T.   |
| 12.0(7)T   | This command was implemented on the Cisco AS5300 and Cisco AS5800 for MICA technologies modems.                                  |
| 12.1(1)XD  | This command was implemented on the Cisco AS5400 for the NextPort dial feature card (DFC).                                       |
| 12.1(3)T   | This command was implemented on the Cisco AS5400 for the NextPort DFC and on the Cisco AS5800 for the universal port card (UPC). |
| 12.1(5)XM1 | This command was implemented on the Cisco AS5350.  |
| 12.2(11)T  | This command was integrated into Cisco IOS Release 12.2(11)T.  |

**Usage Guidelines**

Use the **firmware location** SPE configuration command to download firmware into your modems. This command specifies the location of the firmware file *and* downloads the firmware in the range of SPEs specified, depending on the states configured by the **firmware upgrade** command. Use the **firmware location** command with the **firmware upgrade** command. The entire SPE is affected by the **firmware location** command.

The latest SPE firmware image can usually be retrieved from Cisco.com. You must first copy the SPE image from a TFTP server to Flash memory using the **copy tftp flash** command.

The **firmware location** command is a configuration command and must be saved into the system configuration using the **write memory** command; otherwise, at the next reboot downloading of the specified firmware will not occur.

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

**Note**

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

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

**Examples**

The following example shows how to display all legal IFSs:

```
router# dir all-filesystems

Directory of nvram:/

   121  -rw-          1543          <no date>  startup-config
   122  ----           5          <no date>  private-config

126968 bytes total (125368 bytes free)

Directory of system:/

   6  dr-x           0          <no date>  memory
   1  -rw-          2929          <no date>  running-config
   2  dr-x           0          <no date>  ucode
  17  dr-x           0          <no date>  vfiles

No space information available

Directory of flash:/

   1  -rw-      12575032          <no date>  c5300-js-mz.122-11.T

16777216 bytes total (4202120 bytes free)

Directory of bootflash:/

   1  -rw-      1155864          <no date>  c5300-boot-mz.113-10.T.bin
   2  -rw-      381540          <no date>  mica-modem-pw.2.6.2.0.bin
   3  -rw-      384056          <no date>  pw2621.ios

8388608 bytes total (5682340 bytes free)
```

```
Directory of lex:/

No files in directory

No space information available
```

The following example shows how to enter the SPE configuration mode, set the range of SPEs, specify the firmware file location in Flash memory, download the file to the SPEs, and display a status report using the **show spe EXEC** command:

```
router# configure terminal
router(config)# spe 7/0 7/17
router(config-spe)# firmware location flash:np_6_75
Router(config-spe)# firmware upgrade busyout
Started downloading firmware flash:np_6_75.spe
router(config-spe)# exit
router# show spe 7
.
.
.
SPE#      Port #      SPE          SPE      SPE  SPE  Port      Call
State     Busyout Shut Crash State  Type
7/00     0000-0005  ACTIVE      1      0    0  BBBBBB  _____
7/01     0006-0011  DOWNLOAD    1      0    0  bbbbbb  _____
7/02     0012-0017  DOWNLOAD    1      0    0  bbbbbb  _____
7/03     0018-0023  DOWNLOAD    1      0    0  bbbbbb  _____
.
.
.
```

The following configuration example specifies a firmware file located in Flash memory:

```
spe 1/0 1/8
firmware location np-spe-upw-1.0.1.2.bin
```

The following configuration example shows how to download firmware that is not bundled with the Cisco IOS image:

```
spe 1/2 1/4
firmware location flash:portware.2620.ios
```

The following configuration example shows how to download firmware that is bundled with the Cisco IOS image:

```
spe 2/9 2/9
firmware location system:/ucode/microcom_firmware
```

#### Related Commands

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

# firmware upgrade

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

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

```
no firmware upgrade
```

**Cisco AS5350, Cisco AS5400, and Cisco AS5800**

```
firmware upgrade [ busyout | download-maintenance | reboot ]
```

## Syntax Description

|                             |  |
|-----------------------------|--|
| <b>busyout</b>              | Upgrades when all calls are terminated on the SPE. |
| <b>recovery</b>             | Upgrades during download maintenance time.         |
| <b>reboot</b>               | Upgrades at the next reboot.                       |
| <b>download-maintenance</b> | Upgrade during download maintenance time.          |

## Defaults

An upgrade occurs when all calls are terminated on the SPE (**busyout**). For the Cisco AS5350, Cisco AS5400, and Cisco AS5800 there is no default.

## Command Modes

SPE configuration

## Command History

| Release    | Modification  |
|------------|---|
| 12.0(4)XI1 | This command was introduced on the Cisco AS5200, Cisco AS5300, and Cisco AS5800.  |
| 12.0(6)T   | This command was integrated into Cisco IOS Release 12.0(6)T.  |
| 12.0(7)T   | This command was implemented on the Cisco AS5300 and Cisco AS5800 for MICA technologies modems.                           |
| 12.1(1)XD  | This command was implemented on the Cisco AS5400 for the NextPort dial feature card (DFC).                                |
| 12.1(3)T   | This command was implemented on the Cisco AS5400 for the NextPort DFC and Cisco AS5800 for the universal port card (UPC). |
| 12.1(5)XM1 | This command was implemented on the Cisco AS5350.   |
| 12.2(11)T  | This command was integrated into Cisco IOS Release 12.2(11)T.   |

## Usage Guidelines

Three methods of upgrade are available: busyout, reboot, and download-maintenance or recovery. The **reboot** keyword requests the Cisco access servers to upgrade SPE firmware at the next reboot. The **busyout** keyword upgrades SPE firmware after waiting for all calls to be terminated on an SPE.

The **download-maintenance** or **recovery** keyword requests SPE firmware download during maintenance time.

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

The SPE **firmware location** command is designed to integrate all continuous ranges of SPEs containing the same firmware location. However, the **firmware upgrade** command does not affect the ranges of SPEs. As such, all SPEs within the ranges of SPEs must have the same firmware upgrade mode or the router uses the default upgrade mode to busyout state. If you want to upgrade a single SPE within an existing range of SPEs with a different upgrade mode than is currently configured, you must first change the upgrade mode for the entire range of SPEs and then change the firmware location for the specific SPE being upgraded. Furthermore, each time you merge ranges of SPEs due to configuration changes, verify that the configuration of the SPE firmware upgrade remains effective to what is desired.

## Examples

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

```
Router(config)# spe 1/03
Router(config-spe)# firmware location np-spe-upw-1.0.1.2.bin
Router(config-spe)# firmware upgrade busyout
```

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

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

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

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

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

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

For the Cisco AS5350, Cisco AS5400, or Cisco AS5800, use the following syntax to set the system for a firmware upgrade recovery:

```
Router(config-spe)# firmware upgrade download-maintenance
```

**Related Commands**

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

# flowcontrol

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

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

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

## Syntax Description

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

## Defaults

Flow control is disabled.

## Command Modes

Line configuration

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 10.0    | This command was introduced. |

## Usage Guidelines

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

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

## Examples

The following example sets hardware flow control on line 7:

```
line 7
 flowcontrol hardware
```

**Related Commands**

| <b>Command</b>         | <b>Description</b>                     |
|------------------------|--|
| <b>source template</b> | Sets the flow control start character. |
| <b>stop-character</b>  | Sets the flow control stop character.  |

# force-local-chap

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

**force-local-chap**

**no force-local-chap**

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

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

**Command Modes** VPDN group configuration

## Command History

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

## Usage Guidelines

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

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

## Examples

The following example enables CHAP authentication at the LNS:

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

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

# group-range

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

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

**no group-range** *interface*

## Syntax Description

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

## Defaults

No interfaces are designated as members of a group.

## Command Modes

Interface configuration

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 11.1    | This command was introduced. |

## Usage Guidelines

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

## Examples

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

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

## Related Commands

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

# group session-limit

To specify the maximum number of concurrent sessions allowed across all virtual private dialup network (VPDN) groups associated with a particular VPDN template, use the **group session-limit** command in VPDN template configuration mode. To disable session limiting for a VPDN template, use the **no** form of this command.

**group session-limit** *number*

**no group session-limit** *number*

|                           |               |  |
|---------------------------|---------------|--|
| <b>Syntax Description</b> | <i>number</i> | Maximum number of concurrent sessions allowed across all VPDN groups associated with a particular VPDN template. Valid values are from 1 to 32767. |
|---------------------------|---------------|--|

**Defaults** No session limit is configured at the VPDN template level.

**Command Modes** VPDN template configuration

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>   |
|------------------------|----------------|---|
|                        | 12.2(4)B       | This command was introduced.                                  |
|                        | 12.2(13)T      | This command was integrated into Cisco IOS Release 12.2(13)T. |

**Usage Guidelines** Use this command to specify the maximum number of concurrent sessions across all VPDN groups associated with a VPDN template. If you configure a group session limit for the default VPDN template, that session limit is the session limit for all VPDN groups not associated with a named VPDN template. The group session limit configured by this command does not terminate active sessions. If you configure a group session limit that is lower than the number of current active sessions, no sessions are terminated and no new sessions can start.

Session limits configured at the VPDN group level by the **session-limit** (VPDN) command take precedence over session limits configured at the VPDN template level when the VPDN group level session limit has a lower configured value than the VPDN template level.

**Examples** The following example shows how to configure 100 as the maximum number of concurrent sessions across all VPDN groups attached to the VPDN template called template1:

```
vpdn session-limit 100
vpdn-template template1
 group session-limit 100
```

**Related Commands**

| <b>Command</b>              | <b>Description</b>  |
|-----------------------------|---|
| <b>session-limit</b>        | Limits the number of VPDN sessions.   |
| <b>session-limit (VPDN)</b> | Limits the number of sessions that are allowed through a specified VPDN group.                    |
| <b>show vpdn session</b>    | Displays information about active L2F Protocol tunnel and message identifiers in a VPDN.          |
| <b>source vpdn-template</b> | Configures an individual VPDN group to use VPDN template settings for all unspecified parameters. |
| <b>vpdn-group</b>           | Creates a VPDN group and enters VPDN group configuration mode.                                    |
| <b>vpdn session-limit</b>   | Limits the number of simultaneous VPN sessions that can be established on a router.               |
| <b>vpdn-template</b>        | Creates a VPDN template and enters VPDN template configuration mode.                              |