

# 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 | none | primary {nfas_int number | nfas_group number | rlm-group number}} | service]
```

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

## 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.  <b>Note</b> Groups of time slot ranges separated by commas (1-4,8-23 for example) are also accepted.
<b>nfas_d</b> { <b>backup</b>   <b>none</b>   <b>primary</b> }	(Optional) Configures the operation of the ISDN PRI D channel.  <ul style="list-style-type: none"> <li><b>backup</b>—The D-channel time slot is used as the Non-Facility Associated Signaling (NFAS) D backup.</li> <li><b>none</b>—The D-channel time slot is used as an additional B channel.</li> <li><b>primary</b>—The D-channel time slot is used as the NFAS D primary. The <b>primary</b> keyword requires further interface and group configuration: <ul style="list-style-type: none"> <li><b>nfas_int</b> <i>number</i>—Specifies the provisioned NFAS interface as a value; value is a number from 0 to 8.</li> <li><b>nfas_group</b> <i>number</i>—Specifies the NFAS group.</li> <li><b>rlm-group</b> <i>number</i>—Specifies the Redundant Link Manager (RLM) group and release the ISDN PRI signaling channel.</li> </ul> </li> </ul>
<b>primary</b> { <b>nfas_int</b> <i>number</i>   <b>nfas_group</b> <i>number</i>   <b>rlm-group</b> <i>number</i> }	
<b>service</b>	(Optional) Configures service type <b>mgcp</b> for Media Gateway Control Protocol service.

## Defaults

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	Release	Modification
	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*

### Syntax Description

*template*

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:

- **S**—Starts the state machine.
- **<\***—Waits for the digit **\*** 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.
- **a**—Digits are collected as the ANI until the first nondigit or a timeout occurs.
- **d**—Digits are collected as the DNIS until the first nondigit or a timeout occurs.
- **n**—Notifies the CSM of the collected ANI and DNIS.

### Defaults

No default behavior or values

### Command Modes

Global configuration

### Command History

#### Release

#### Modification

12.1(1)T

This command was introduced.

### Usage Guidelines

Arrange the directive special characters in the order necessary to process the digit sequence for your signaling class.

### Examples

The following example enables the **profile incoming** command:

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

### Related Commands

#### Command

#### Description

**class (controller)**

Activates the **signaling-class cas** command.

**signaling-class cas**

Defines a signaling class with a template formed by directives guiding the CSM to process the digit sequence.

# protocol (VPDN)

To specify the tunneling protocol that a virtual private dialup network (VPDN) subgroup will use, use the **protocol** command in VPDN subgroup configuration mode. To remove the protocol-specific configurations from a VPDN subgroup, use the **no** form of this command.

**protocol** { **any** | **l2f** | **l2tp** | **pppoe** | **pptp** }

**no protocol**

## Syntax Description

<b>any</b>	Specifies either the Layer 2 Forwarding (L2F) protocol or the Layer 2 Tunneling Protocol (L2TP).
<b>l2f</b>	Specifies the L2F protocol.
<b>l2tp</b>	Specifies L2TP.
<b>pppoe</b>	Specifies the PPP over Ethernet (PPPoE) protocol.
<b>pptp</b>	Specifies the Point-to-Point Tunneling Protocol (PPTP).

## Defaults

No protocol is specified.

## Command Modes

VPDN subgroup

## Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(1)T	The <b>pppoe</b> keyword was added.

## Usage Guidelines

This command is required for any VPDN subgroup configuration.

L2TP is the only protocol that can be used for dialout subgroup configurations.

Changing the protocol will remove all the commands from the VPDN subgroup configuration, and any protocol-specific commands from the VPDN group configuration.



### Note

Users must first enter the **vpdn enable** command to set up the PPP over Ethernet discovery daemon.

## Examples

The following example configures VPDN group 1 to accept dial-in calls using L2F and to request dial-out calls using L2TP:

```
vpdn-group 1
 accept-dialin
  protocol l2f
  virtual-template 1
 request-dialout
  protocol l2tp
```

```

pool-member 1
local name router1
terminate-from hostname router2
initiate-to ip 10.3.2.1
l2f ignore-mid-sequence
l2tp ip udp checksum

```

If you then use the **no protocol** command in request-dialout mode, the configuration will be changed to this:

```

vpdn-group 1
accept-dialin
  protocol l2f
  virtual-template 1
request-dialout
local name router1
terminate-from hostname router2
l2f ignore-mid-sequence

```

#### Related Commands

Command	Description
<b>accept-dialin</b>	Creates an accept dial-in VPDN subgroup that configures a tunnel server to accept requests from a NAS to tunnel dial-in calls, and enters accept dial-in VPDN subgroup configuration mode.
<b>accept-dialout</b>	Creates an accept dial-out VPDN subgroup that configures a NAS to accept requests from a tunnel server to tunnel L2TP dial-out calls, and enters accept dial-out VPDN subgroup configuration mode.
<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.
<b>request-dialout</b>	Creates a request dial-out VPDN subgroup that configures a tunnel server to request the establishment of dial-out L2TP tunnels to a NAS, and enters request dial-out VPDN subgroup configuration mode.

# 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 | limit slot/port | port slot [slot]}
```

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

## Cisco AS5200 and AS5300 Series Routers

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

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

### Syntax Description

<b>limit number</b>	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>limit slot/port</b>	Replace the <i>slot</i> argument with the slot number of the card and the <i>port</i> argument with the port range. Applicable to ISDN B-channels or HDLC controllers
<b>port range</b>	Range of resource ports to use in the resource group.
<b>port slot/port</b>	Specific ports to use in the resource group. A forward slash must be used to separate the slot and port numbers.

### Defaults

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:

**Cisco AS5300**

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

**Cisco AS5400**

```
resource-pool group resource hdlc
  range limit 2:255 (where 2 is slot#)
```

**Cisco AS5800**

```
resource-pool group resource hdlc
  range limit 2/0:255 (where 2 is slot# & 0 is subslot#
                    for the trunk card)
```

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 (:).

**Defaults** 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
```

## Syntax Description

**port *number*** (Optional) TCP port number.

## Defaults

If the router is configured for basic Net3 ISDN switch type, by default RAPI is enabled, and the port number is set to 2578.

## Command Modes

Global configuration

## Command History

Release	Modification
12.0(7)XV	This command was introduced on the Cisco 800 series router.

## Usage Guidelines

This command works only with the Net3 switch type. The same port number must be configured on both the router and client PC.

## Examples

The following example set the TCP port number to 2000:

```
rcapi server port 2000
```

## Related Commands

Command	Description
<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.

# redirect identifier

To configure a virtual private dialup network (VPDN) redirect identifier to use for Layer 2 Tunneling Protocol (L2TP) call redirection on a network access server (NAS), use the **redirect identifier** command in VPDN group or VPDN template configuration mode. To remove the name of the redirect identifier from the NAS, use the **no** form of this command.

**redirect identifier** *identifier-name*

**no redirect identifier** *identifier-name*

<b>Syntax Description</b>	<i>identifier-name</i>	Name of the redirect identifier to use for call redirection.
---------------------------	------------------------	--

<b>Command Default</b>	No redirect identifier is configured.
------------------------	---------------------------------------

<b>Command Modes</b>	VPDN group configuration VPDN template configuration
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(8)B	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

**Usage Guidelines**

The **redirect identifier** command is used only on the NAS. To configure the name of the redirect identifier on the stack group tunnel server, use the **vpdn redirect identifier** command in global configuration mode.

The NAS compares the redirect identifier with the one received from the stack group tunnel server to determine authorization information to redirect the call.

Configuring the redirect identifier is not necessary to perform redirects. If the redirect identifier is not configured, the NAS uses the redirect IP address in order to get authorization information to redirect the call. In that case, the IP address of the new redirected tunnel server must be present in the **initiate-to** command configuration of the VPDN group on the NAS.

The redirect identifier allows new stack group members to be added without the need to update the NAS configuration with their IP addresses. With the redirect identifier configured, a new stack group member can be added and given the same redirect identifier as the rest of the stack group.

If the authorization information for getting to the new redirected tunnel server is different, then you will need to configure the authorization information via RADIUS using tagged attributes:

```
Cisco:Cisco-Avpair = :0:"vpdn:vpdn-redirect-id=identifier name"
```

The NAS will choose the correct tagged parameters to get authorization information for the new redirected tunnel server by first trying to match the redirect identifier (if present) or else by matching the Tunnel-Server-Endpoint IP address.

**Examples**

The following example configures the redirect identifier named lns1 on the NAS for the VPDN group named group1:

```
vpdn-group group1
  redirect identifier lns1
```

**Related Commands**

Command	Description
<b>clear vpdn redirect</b>	Clears the L2TP redirect counters shown in the output from the <b>show vpdn redirect</b> command.
<b>show vpdn redirect</b>	Displays statistics for L2TP call redirects and forwards.
<b>vpdn redirect</b>	Enables L2TP redirect functionality.
<b>vpdn redirect attempts</b>	Restricts the number of redirect attempts possible for an L2TP call on the LAC.
<b>vpdn redirect identifier</b>	Configures a VPDN redirect identifier to use for L2TP call redirection on a stack group tunnel server.
<b>vpdn redirect source</b>	Configures the public redirect IP address of an LNS.
<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
<b>vpdn-template</b>	Creates a VPDN template and enters VPDN template configuration mode.

# redundancy

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

**redundancy**

**no redundancy**

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

**Defaults** Redundancy is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(2)T	This command was introduced.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

**Usage Guidelines** Use the **redundancy** global configuration command to enter redundancy-configuration mode.

**Examples** The following example assigns 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
```

Related Commands	Command	Description
	<b>failover group-number</b>	Assigns a router-shelf pair to a redundancy router-shelf pair code.
	<b>show redundancy</b>	Displays current or historical status and related information and displays the router-shelf redundancy status.

# 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.

---

# request-dialin

To create a request dial-in VPDN subgroup that configures a network access server (NAS) to request the establishment of a dial-in tunnel to a tunnel server, and to enter request dial-in VPDN subgroup configuration mode, use the **request-dialin** command in VPDN group configuration mode. To remove the request dial-in VPDN subgroup configuration from a virtual private dialup network (VPDN) group, use the **no** form of this command.

**request-dialin**

**no request-dialin**

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

**Defaults** No request dial-in VPDN subgroups are configured.

**Command Modes** VPDN group configuration

## Command History

Release	Modification
11.3(5)AA	This command was introduced.
12.0(5)T	This command was introduced.
12.0(5)T	The original keywords and arguments were removed and made into separate <b>request-dialin</b> subgroup commands.

## Usage Guidelines

Use the **request-dialin** command on a NAS to configure a VPDN group to request the establishment of dial-in VPDN tunnels to a tunnel server.

For a VPDN group to request dial-in calls, you must also configure the following commands:

- The **initiate-to** command in VPDN group configuration mode
- The **protocol** command in request dial-in VPDN subgroup configuration mode
- At least one **dnis** or **domain** command in request dial-in VPDN subgroup configuration mode

The NAS can also be configured to accept requests for Layer 2 Tunnel Protocol (L2TP) dial-out VPDN tunnels from the tunnel server using the **accept-dialout** command. Dial-in and dial-out calls can use the same L2TP tunnel.

## Examples

The following example requests an L2TP dial-in tunnel to a remote peer at IP address 172.17.33.125 for a user in the domain named cisco.com:

```
Router(config)# vpdn-group 1
Router(config-vpdn)# request-dialin
Router(config-vpdn-req-in)# protocol l2tp
Router(config-vpdn-req-in)# domain cisco.com
```

```
!
Router(config-vpdn)# initiate-to ip 172.17.33.125
```

### Related Commands

Command	Description
<b>accept-dialin</b>	Creates an accept dial-in VPDN subgroup that configures a tunnel server to accept requests from a NAS to tunnel dial-in calls, and enters accept dial-in VPDN subgroup configuration mode.
<b>accept-dialout</b>	Creates an accept dial-out VPDN subgroup that configures a NAS to accept requests from a tunnel server to tunnel L2TP dial-out calls, and enters accept dial-out VPDN subgroup configuration mode.
<b>authen before-forward</b>	Specifies that VPDN send the entire structured username to the AAA server the first time the router contacts the AAA server.
<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>domain</b>	Specifies the domain name of users that are to be forwarded to a tunnel server using VPDN.
<b>initiate-to</b>	Specifies the IP address that calls are tunneled to.
<b>protocol (VPDN)</b>	Specifies the tunneling protocol that a VPDN subgroup will use.

# request-dialout

To create a request dial-out VPDN subgroup that configures a tunnel server to request the establishment of dial-out Layer 2 Tunnel Protocol (L2TP) tunnels to a network access server (NAS), and to enter request dial-out VPDN subgroup configuration mode, use the **request-dialout** command in VPDN group configuration mode. To remove the request dial-out VPDN subgroup configuration from a virtual private dialup network (VPDN) group, use the **no** form of this command.

**request-dialout**

**no request-dialout**

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

**Defaults** No request dial-out VPDN subgroups are configured.

**Command Modes** VPDN group configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced.

**Usage Guidelines** Use the **request-dialout** command on a tunnel server to configure a VPDN group to request the establishment of dial-out VPDN tunnels to a NAS. L2TP is the only tunneling protocol that can be used for dial-out VPDN tunnels.

For a VPDN group to request dial-out calls, you must also configure the following commands:

- The **initiate-to** command in VPDN group configuration mode
- The **protocol l2tp** command in request dial-out VPDN subgroup configuration mode
- Either the **pool-member** or **rotary-group** command in request dial-out VPDN subgroup configuration mode, depending on the type of dialer resource to be used by the VPDN subgroup
- The **dialer vpdn** command in dialer interface configuration mode

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 configuration.

The tunnel server can also be configured to accept requests to establish dial-in VPDN tunnels from a NAS using the **accept-dialin** command. Dial-in and dial-out calls can use the same L2TP tunnel.

**Examples** The following example configures VPDN group 1 to request an L2TP tunnel to the peer at IP address 10.3.2.1 for tunneling dial-out calls from dialer pool 1:

```
Router(config)# vpdn-group 1
Router(config-vpdn)# request-dialout
Router(config-vpdn-req-ou)# protocol l2tp
Router(config-vpdn-req-ou)# pool-member 1
```

```

!
Router(config-vpdn)# initiate-to ip 10.3.2.1
!
Router(config)# interface Dialer2
Router(config-if)# ip address 172.16.2.3 255.255.128
Router(config-if)# encapsulation ppp
Router(config-if)# dialer remote-name reuben
Router(config-if)# dialer string 5551234
Router(config-if)# dialer vpdn
Router(config-if)# dialer pool 1
Router(config-if)# dialer-group 1
Router(config-if)# ppp authentication chap

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>accept-dialin</b>	Creates an accept dial-in VPDN subgroup that configures a tunnel server to accept requests from a NAS to tunnel dial-in calls, and enters accept dial-in VPDN subgroup configuration mode.
<b>accept-dialout</b>	Creates an accept dial-out VPDN subgroup that configures a NAS to accept requests from a tunnel server to tunnel L2TP dial-out calls, and enters accept dial-out VPDN subgroup configuration mode.
<b>dialer vpdn</b>	Enables a dialer profile or DDR dialer to use L2TP dial-out.
<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 tunneling protocol that a VPDN subgroup will use.
<b>rotary-group</b>	Assigns a request-dialout VPDN subgroup to a dialer rotary group.

# 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 framers (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.

## Defaults

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 group resource modem1
  range port 1/0 1/47
exit
```

```
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.

## Defaults

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.

## Defaults

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.

## Defaults

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.

## Defaults

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

```
Router(config)# resource-pool call treatment profile ?
busy          Send busy code when profile authorization fails
no-answer     Don't answer when profile authorization fails
```

# 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.

## Defaults

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.
-------------	--

## Defaults

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.

## Defaults

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-vpdn-customer)# vpdn 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>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.

# 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.
-------------	---

## Defaults

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 **clidKiller** created and configured to block digital calls from the CLID group named **zot**:

```
resource-pool profile discriminator clidKiller
  call-type digital
  clid group zot
```

## 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.
-------------	---

---

---

**Defaults**

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*

## Syntax Description

*name* VPDN profile name.

## Defaults

No VPDN 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 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>Defaults</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: <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.

## Defaults

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 queueing:

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

The following example enables asynchronous rotary line queueing 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.

## Defaults

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) dialout to IP address 172.16.4.6 using dialer profile pool 1 and identifying itself using the local name harold.

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<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.