

shutdown (port)

To disable a port, use the **shutdown** command in port configuration mode. To change the administrative state of a port from out-of-service to in service, use the **no** form of this command.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Defaults Port is enabled.

Command Modes Port configuration

Command History	Release	Modification
	12.1(1)XD	This command was introduced on the Cisco AS5400.
	12.1(3)T	This command was implemented on the Cisco AS5800.

Usage Guidelines The **shutdown** command disables a port.



Note

The **shutdown** command is similar to the **modem shutdown** MICA modem command.

Examples The following example disables ports 1 to 18 then re-enables them:

```
port 1/1 1/18
shutdown
no shutdown
exit
```

Related Commands	Command	Description
	busyout	Gracefully disables a port by waiting for the active services on the specified port to end.
	clear port	Resets the NextPort port and clears any active call.
	clear spe	Reboots all specified SPEs.
	show spe	Displays history statistics of all SPEs, a specified SPE, or the specified range of SPEs.

shutdown (spe)

To take a Service Processing Element (SPE) out of service, use the **shutdown** command in SPE configuration mode. To change the administrative state of this SPE from down to up, use the **no** form of this command.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Defaults SPE is enabled.

Command Modes SPE configuration

Command History	Release	Modification
	12.1(1)XD	This command was introduced on the Cisco AS5400.
	12.1(3)T	This command was implemented on the Cisco AS5800.

Examples The following example disables SPE ports 1 to 18 then re-enables them:

```
spe 1/1 1/18
shutdown
no shutdown
```

Related Commands	Command	Description
	busyout	Gracefully disables a port by waiting for the active services on the specified port to end.
	clear spe	Reboots all specified SPEs.
	show spe	Displays history statistics of all SPEs, a specified SPE, or the specified range of SPEs.

signaling-class cas

To define a signalling class with a template formed by directives guiding the Call Service Module (CSM) to process the digit sequence, use the **signaling-class cas** command in global configuration mode. To remove the signalling class assignment, use the **no** form of this command.

signaling-class cas *name*

no signaling-class cas *name*

Syntax Description

<i>name</i>	The signalling class name, which specifies the template that processes the ANI/DNIS delimiter.
-------------	--

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

The signalling class is referred by the *name* argument.

Examples

The following example enables the **signaling-class cas** command:

```
signaling-class cas test
profile incoming S<*a<*d<*n
controller T1 1/0/1
cas-custom 1
class test
```

Related Commands

Command	Description
class	Activates the signaling-class cas command.
profile incoming	Defines a template formed by directives guiding the CSM to process the digit sequence for a signaling class.

snapshot client

To configure a client router for snapshot routing, use the **snapshot client** command in interface configuration mode. To disable a client router, use the **no** form of this command.

snapshot client *active-time quiet-time* [**suppress-statechange-updates**] [**dialer**]

no snapshot client *active-time quiet-time* [**suppress-statechange-updates**] [**dialer**]

Syntax Description		
<i>active-time</i>		Amount of time, in minutes, that routing updates are regularly exchanged between the client and server routers. This can be an integer in the range 5 to 100. There is no default value. A typical value is 5 minutes.
<i>quiet-time</i>		Amount of time, in minutes, that routing entries are frozen and remain unchanged between active periods. Routes are not aged during the quiet period, so they remain in the routing table as if they were static entries. This argument can be an integer from 8 to 100000. There is no default value. The minimum quiet time is generally the active time plus 3.
suppress-statechange-updates		(Optional) Disables the exchange of routing updates each time the line protocol goes from “down” to “up” or from “dialer spoofing” to “fully up.”
dialer		(Optional) Specifies that the client router dials up the remote router in the absence of regular traffic.

Defaults

Snapshot routing is disabled.

The *active-time* and *quiet-time* arguments have no default values.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The value of the *active-time* argument must be the same for the client and server routers.

To specify that the remote server routers be called by this client router during each active period, use the **dialer map snapshot** command.

Examples

The following example configures a client router for snapshot routing:

```
interface dialer 1
 snapshot client 5 600 suppress-statechange-updates dialer
```

Related Commands	Command	Description
	clear resource-pool	Ends the quiet period on a client router within 2 minutes.
	dialer map snapshot	Defines a dialer map for the Cisco snapshot routing protocol on a client router connected to a DDR interface.
	show snapshot	Displays snapshot routing parameters associated with an interface.
	snapshot client	Configures a client router for snapshot routing.
	snapshot server	Configures a server router for snapshot routing.

snapshot server

To configure a server router for snapshot routing, use the **snapshot server** command in interface configuration mode. To disable a server router, use the **no** form of this command.

snapshot server *active-time* [**dialer**]

no snapshot server *active-time* [**dialer**]

Syntax Description

<i>active-time</i>	Amount of time, in minutes, that routing updates are regularly exchanged between the client and server routers. This can be an integer in the range 5 to 100. There is no default value. A typical value is 5 minutes.
dialer	(Optional) Specifies that the client router dials up the remote router in the absence of regular traffic.

Defaults

Snapshot routing is disabled.
The *active-time* argument has no default value.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The value of the *active-time* argument must be the same for the client and server routers.

Examples

The following example configures a server router for snapshot routing:

```
interface dialer 1
 snapshot server 5
```

Related Commands

Command	Description
show snapshot	Displays snapshot routing parameters associated with an interface.
snapshot client	Configures a client router for snapshot routing.

source template

To attach a configured customer profile template to a particular customer profile, use the **source template** command in customer profile configuration mode.

source template *name*

Syntax Description	<i>name</i>	Customer profile template name.
--------------------	-------------	---------------------------------

Defaults	No templates are sourced or attached to a customer profile.
----------	---

Command Modes	Customer profile configuration
---------------	--------------------------------

Command History	Release	Modification
	12.0(6)T	This command was introduced.

Usage Guidelines	All PPP and peer-default commands are allowed for a particular customer profile template under this grouping.
------------------	---

Examples	The following example shows the creation and configuration of a customer profile template named acme-direct and its subsequent assignment to the customer profile acme1:
----------	--

```
template acme-direct
 multilink {max-fragments num | max-links num | min-links num}
 peer match aaa-pools
 peer default ip address pool acme-numbers
 ppp ipcp dns 10.1.1.1 10.2.2.2
 ppp multilink
 exit
 resource-pool profile customer acme1
 source template acme-direct
```

Related Commands	Command	Description
	template	Accesses the template configuration mode for configuring a particular customer profile template.

source-ip (VPDN)

To specify an IP address that is different from the physical IP address used to open a virtual private dialup network (VPDN) tunnel for the tunnels associated with a VPDN group, use the **source-ip** command in VPDN group configuration mode. To remove the alternate IP address, use the **no** form of this command.

source-ip *ip-address*

no source-ip

Syntax Description	<i>ip-address</i>	Alternate IP address.
Command Default	No alternate IP address is specified.	
Command Modes	VPDN group configuration	
Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines

Use the **source-ip** command in VPDN group configuration mode to configure an alternate IP address to be used for only those tunnels associated with that VPDN group. Each VPDN group on a router can be configured with a unique **source-ip** command.

Use the **vpdn source-ip** command to specify a single alternate IP address to be used for all tunnels on the device. A single source IP address can be configured globally per device.

The VPDN group-level configuration will override the global configuration.

Examples

The following example configures a network access server (NAS) to accept Layer 2 Tunnel Protocol (L2TP) dial-out calls using the alternate IP address 172.23.33.7, which is different from the physical IP address used to open the L2TP tunnel:

```
vpdn-group 3
 accept-dialout
  protocol l2tp
  dialer 2
 terminate-from hostname router21
 source-ip 172.23.33.7
```


Related Commands	Command	Description
	accept-dialin	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.
	accept-dialout	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.
	request-dialin	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.
	request-dialout	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.
	vpdn source-ip	Globally specifies an IP address that is different from the physical IP address used to open a VPDN tunnel.

spe

To enter Service Processing Element (SPE) configuration mode and set the range of SPEs, use the **spe** command in global configuration mode.

Cisco AS5400 with NextPort DFC

```
spe { slot | slot/spe }
```

Cisco AS5800 with Universal Port Card

```
spe { shelf/slot | shelf/slot/spe }
```

Syntax Description	<i>slot</i>	All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	<i>slot/spe</i>	All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.
	<i>shelf/slot</i>	All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
	<i>shelf/slot/spe</i>	All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53.

Defaults	No default behavior or values.
----------	--------------------------------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.0(4)XI1	This command was introduced.
	12.0(5)T	This command was implemented on additional Cisco platforms.
	12.1(1)XD	This command was implemented on the Cisco AS5400.
	12.1(3)T	This command was implemented on the Cisco AS5800.

Usage Guidelines

The **spe** global configuration command enables the SPE configuration mode. Configure your SPE by specifying a slot and an SPE associated with the slot; or, you can configure a range of SPEs by specifying the first and last SPE in the range.

When the access server is booted, the **spe** global configuration command specifies the location from which the firmware image is downloaded to the SPE. If the **spe** configuration command is used to download the firmware from Flash memory and subsequently the **no** version of the exact command is entered, then the **spe** command downloads the embedded firmware.



Note Use this command when traffic is low because the **spe** download does not begin until the modems have no active calls.


Caution

The **spe** command is a configuration command. Save it using the **write memory** command; otherwise, the configuration is not saved. If the configuration is not saved, the downloading of the specified firmware does not occur after the next reboot.

Examples

The following example shows the **spe** command being used from global configuration mode to access the SPE configuration mode for the range of SPEs from 1/2 to 1/4 on the Cisco AS5400:

```
Router(config)# spe 1/2 1/4
```

The following example specifies the range for use of the **shutdown** command:

```
Router(config)# spe 1/1 1/18
Router(config-spe)# shutdown
Router(config-spe)# no shutdown
Router(config-spe)#
```

Related Commands

Command	Description
show spe	Displays SPE status.

spe call-record modem

To generate a modem call record at the end of each call, use the **spe call-record modem** command in global configuration mode. To cancel the request to generate the reports, use the **no** form of the command.

```
spe call-record modem {max-userid number | quiet}

no spe call-record modem {max-userid number | quiet}
```


Syntax Description	max-userid <i>number</i>	Maximum length of User ID for the modem call record report in number of bytes. The range is 0 to 100.
	quiet	Disables logging to console and terminal, but not to syslog.

Defaults SPE call record is enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(1)XD	This command was introduced on the Cisco AS5400.
	12.1(3)T	This command was implemented on the Cisco AS5800.

Usage Guidelines The **spe modem-call-record** command generates a modem call record at the end of each call.



Note The **spe call-record modem** command is similar to the **modem call-record** command.

Examples

The following example displays SPE call record:

```
Router# configure terminal
Router(config)# spe call-record modem max-userid 50
Router(config)# end
Router#
00:18:30: %SYS-5-CONFIG_I: Configured from console by console
Router# write memory
Building configuration...
[OK]
```

The following is an example of traces generated when a call terminates. The logs from the **show port modem log** command do not change as a result of using the **spe call-record modem** command.

```
...
%LINK-3-UPDOWN: Interface Async5/105, changed state to down
%MODEMCALLRECORD-6-PM_TERSE_CALL_RECORD: DS0 slot/contr/chan=4/2/15,
shelf/slot/port=5/37, call_id=EE, userid=touraco-e1-4, ip=79.188.24.1,
calling=(n/a), called=35160, std=V.34+, prot=LAP-M, comp=V.42bis,
```

```
init-rx/tx b-rate=33600/33600, finl-rx/tx b-rate=33600/33600, rbs=0,
d-pad=None, retr=1, sq=5, snr=10495, rx/tx chars=286/266, bad=0, rx/tx
ec=16/6, bad=0, time=96, finl-state=Steady Retrain,
disc(radius)=(n/a)/(n/a), disc(modem)=1F00 <unknown>/Requested by
host/non-specific host disconnect
%MODEMCALLRECORD-6-PM_TERSE_CALL_RECORD: DS0 slot/contr/chan=4/1/24,
shelf/slot/port=5/38, call_id=FD, userid=touraco-e1-4, ip=79.205.24.1,
calling=(n/a), called=35170, std=V.34+, prot=LAP-M, comp=V.42bis,
init-rx/tx b-rate=33600/33600, finl-rx/tx b-rate=33600/33600, rbs=0,
d-pad=None, retr=1, sq=5, snr=10495, rx/tx chars=289/267, bad=0, rx/tx
ec=17/7, bad=0, time=93, finl-state=Steady Retrain,
disc(radius)=(n/a)/(n/a), disc(modem)=1F00 <unknown>/Requested by
host/non-specific host disconnect
%MODEMCALLRECORD-6-PM_TERSE_CALL_RECORD: DS0 slot/contr/chan=4/3/15,
shelf/slot/port=5/2, call_id=FF, userid=touraco-e1-4, ip=79.200.24.1,
calling=(n/a), called=35170, std=V.34+, prot=LAP-M, comp=V.42bis,
init-rx/tx b-rate=33600/33600, finl-rx/tx b-rate=33600/33600, rbs=0,
d-pad=None, retr=1, sq=5, snr=10495, rx/tx chars=287/270, bad=0, rx/tx
ec=17/7, bad=0, time=92, finl-state=Steady Retrain,
disc(radius)=(n/a)/(n/a), disc(modem)=1F00 <unknown>/Requested by
host/non-specific host disconnect
%MODEMCALLRECORD-6-PM_TERSE_CALL_RECORD: DS0 slot/contr/chan=4/3/10,
shelf/slot/port=5
...
```

spe country

To specify the country while setting the Universal Port DFC parameters (including country code and encoding), use the **spe country** command in global configuration mode. To set the country code to the default value, use the **no** form of this command.

spe country *country-name*

no spe country *country-name*

Syntax Description

country-name Name of the country; see [Table 127](#) for a list of supported country name keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.

Usage Guidelines

The **spe country** command is similar to the **modem country** command. On the Cisco access server, DS0 companding law selection is configured for the entire system rather than on individual voice ports. Set **spe country** to the appropriate country. A list of all supported countries is displayed in [Table 127](#).

If T1s are configured, the default is **t1-default**; if E1s are configured, the default is **e1-default**.

The Cisco access server must be in an Idle state (no calls are active) to execute the **spe country** command. All sessions on all modules in all slots must be Idle.

Table 127 Country Names and Corresponding Companding Law

Keyword	Country	Companding Law
australia	Australia	a-law
austria	Austria	a-law
belgium	Belgium	a-law
china	China	a-law
cyprus	Cyprus	a-law
czech-republic	Czech/Slovak Republic	a-law
denamrk	Denmark	a-law
e1-default	Default for E-1	a-law
finland	Finland	a-law
france	France	a-law

Table 127 Country Names and Corresponding Companding Law (continued)

Keyword	Country	Companding Law
germany	Germany	a-law
hong-kong	Hong Kong	u-law
india	India	a-law
ireland	Ireland	a-law
israel	Israel	a-law
italy	Italy	a-law
japan	Japan	u-law
malaysia	Malaysia	a-law
netherlands	Netherlands	a-law
new-zealand	New Zealand	a-law
norway	Norway	a-law
poland	Poland	a-law
portugal	Portugal	a-law
ruissia	Russia	a-law
singapore	Singapore	a-law
south-africa	South Africa	a-law
spain	Spain	a-law
sweden	Sweden	a-law
switzerland	Switzerland	a-law
t1-default	Default for T1	u-law
taiwan	Taiwan	u-law
thailand	Thailand	a-law
turkey	Turkey	a-law
united-kingdom	United Kingdom	a-law
usa	United States of America	u-law

Examples

The following example configures the setting of the country code to the default for **E1**:

```
spe country e1-default
```

The following example configures the setting of the country code to the default for **T1**:

```
spe country t1-default
```

Related Commands

Command	Reference
show spe	Displays SPE status.

spe download maintenance

To perform download maintenance on Service Processing Elements (SPEs) that are marked for recovery, use the **spe download maintenance** command in global configuration mode. To unmark the ports, use the **no** form of the command.

spe download maintenance {**time** *hh:mm* | **stop-time** *hh:mm* | **max-spes** *num-of-spes* | **window** *time-period* | **expired-window** {**drop-call** | **reschedule**}}

no spe download maintenance {**time** *hh:mm* | **stop-time** *hh:mm* | **max-spes** *num-of-spes* | **window** *time-period* | **expired-window** {**drop-call** | **reschedule**}}

Syntax Description		
time <i>hh:mm</i>		Time of the day to start the download maintenance activity. Enter the value in the format of the variable as shown. Default is 03:00 a.m.
stop-time <i>hh:mm</i>		Time of the day to stop the download maintenance activity. Enter the value in the format of the variable as shown.
max-spes <i>num-of-spes</i>		Maximum number of SPEs that can simultaneously be in maintenance. The value is between 1 and 10,000. Default is equal to 20 percent of the maximum number of SPEs in each NextPort DFC.
window <i>time-period</i>		Time window to perform the maintenance activity. The value is between 0 and 360 minutes. Default is 60 minutes.
expired-window		Action to take if SPE maintenance is not completed within the specified window. Default is reschedule .
drop-call		Expired window choice that forces download by dropping active calls.
reschedule		Expired window choice that defers recovery to the next maintenance time (default for expired-window keyword).

Defaults Enabled

Command Modes Global configuration

Command History	Release	Modification
	12.1(1)XD	This command was introduced on the Cisco AS5400.
	12.1(3)T	This command was implemented on the Cisco AS5800.

Usage Guidelines The SPE download maintenance activity takes place when SPEs are marked for recovery. The settings are enabled by default. When you want to change the default settings to a desired setting, use the **spe download maintenance** command parameters to perform SPE download maintenance activity with the specific changes.

Enter the **time** *hh:mm* keyword to set a time to start the SPE download maintenance activity. Then enter the **stop-time** *hh:mm* keyword to set a time to stop the download maintenance. Next enter the **max-spes** *num-of-spes* keyword to set the number of SPEs for the download maintenance. Then enter the **window**

time-period keyword to set a time period to perform the download maintenance. Finally, enter the **expired-window** keyword to set actions in the event the SPE download maintenance is not completed in the set **window time-period**.

The download maintenance activity starts at the set start **time** and steps through all the SPEs that need recovery and the SPEs that need a firmware upgrade and starts maintenance on the maximum number of set SPEs for maintenance. The system waits for the **window** delay time for all the ports on the SPE to become inactive before moving the SPE to the Idle state. Immediately after the SPE moves to Idle state, the system starts to download firmware. If the ports are still in use by the end of **window** delay time, depending upon the **expired-window** setting, connections on the SPE ports are shutdown and the firmware is downloaded by choosing the **drop-call** option, or the firmware download is rescheduled to the next download maintenance time by choosing the **reschedule** option. This process continues until the number of SPEs under maintenance is below **max-spes**, or until **stop-time** (if set), or until all SPEs marked for recovery or upgrade have had their firmware reloaded.

Examples

The following example displays the SPE download maintenance with the different keyword parameters:

```
spe download maintenance time 03:00
spe download maintenance stop-time 04:00
spe download maintenance max-spes 50
spe download maintenance window 30
spe download maintenance expired-window reschedule
```

Related Commands

Command	Description
firmware location	Downloads firmware from Flash memory into the modems from this file location.
firmware upgrade	Specifies the method in which the SPE will be downloaded.
show spe version	Displays the firmware version on an SPE.
spe recovery	Sets an SPE port for recovery.

spe log-size

To set the size of the port event log, use the **spe log-size** command in global configuration mode. To restore the default size, use the **no** version of this command.

spe log-size *number*

no spe log-size

Syntax Description

<i>number</i>	The number of recorded events. Valid values for the <i>number</i> argument range from 0 to 100. The default value is 50 events.
---------------	---

Command Default

The port event log records 50 events.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T on the Cisco AS5400 and Cisco AS5800.
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 and support was added for the Cisco AS5350.

Examples

The following example sets the size of the event log to 70 events:

```
Router(config)# spe log-size 70
```

Related Commands

Command	Description
show port digital log	Displays the digital data event log with the oldest event first.
show port modem log	Displays the modem port history event log or modem test log.

spe recovery

To set a service processing element (SPE) port for recovery, use the **spe recovery** command in global configuration mode. To disable SPE recovery or to restore the default **port-threshold** value, use the **no** form of this command.

```
spe recovery {port-action {disable | recover} | port-threshold number-failures}
```

```
no spe recovery {port-action | port-threshold}
```

Syntax Description

port-action	Action to apply to the port for recovery when the configured port-threshold value has been exceeded.
disable	Sets the port to the bad state.
recover	Sets the port for recovery.
port-threshold <i>number-failures</i>	Number of consecutive failed attempts made on the port before the port-action keyword is applied. The range is from 1 to 10000. The default value is 30.

Defaults

There is no default **port-action** value. SPE recovery is disabled.
The default **port-threshold** value is 30 failed attempts.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(2.3)T1	This command was implemented on the Cisco AS5800.

Usage Guidelines

Failure of an SPE port to connect after repeated tries indicates that a problem exists in the SPE or firmware. An SPE port in this state is recovered by downloading firmware.

When an SPE port fails to connect consecutively for a number of times, as specified by the **port-threshold** *number-failures* keyword and argument, the SPE is moved to a state based on the **port-action** configuration.

If the **spe recovery port-action recover** command has been configured, when the **port-threshold** *number-failures* value is exceeded, the port is temporarily marked as disabled (“d” state) to avoid further incoming calls, and it is then marked for recovery (“r” state). Any SPE that has a port marked for recovery will download firmware when the SPE is idle (when none of the ports on the SPE have active calls).

If the **spe recovery port-action disable** command has been configured, when the **port-threshold** *number-failures* value is exceeded, the port is marked as bad (“BAD” state). An SPE with a port that is marked as bad must be explicitly cleared in order for that port to be used again.

If no **port-action** is configured, the port will be marked as not in use (“_” state). An SPE with a port marked as not in use will remain unusable until it is explicitly cleared, and the SPE will not accept incoming calls on any of the ports.

SPE recovery can be disabled by issuing the **no spe recovery port-action** command. If SPE recovery is disabled, the SPE will behave as if no **port-action** has been configured.

**Note**

Beginning with Cisco IOS Release 12.1(2.3)T1, the modem recovery action for MICA technologies modems on the Cisco AS5800 platforms is done using the **spe recovery** command rather than the **modem recovery** command.

Examples

The following example configures the SPE to recover ports that exceed the call failure threshold:

```
Router(config)# spe recovery port-action recover
```

The following example sets a value of 50 for the number of consecutive failed attempts on the port before the **port-action** keyword is applied:

```
Router(config)# spe recovery port-threshold 50
```

Related Commands

Command	Description
clear port	Resets the NextPort port and clears any active call.
clear spe	Reboots all specified SPEs.
firmware upgrade	Specifies an SPE firmware upgrade method.
show spe	Displays history statistics of all SPEs, a specified SPE, or the specified range of SPEs.
show spe version	Displays the firmware version on an SPE and displays the version to firmware file mappings.
spe download maintenance	Performs download maintenance on SPEs that are marked for recovery.

start-character

To set the flow control start character, use the **start-character** command in line configuration mode. To remove the character, use the **no** form of this command.

start-character *ascii-number*

no start-character

Syntax Description	<i>ascii-number</i>	Decimal representation of the start character.
Defaults	Decimal 17	
Command Modes	Line configuration	
Command History	Release	Modification
	10.0	This command was introduced.
Usage Guidelines	This command defines the character that signals the start of data transmission when software flow control is in effect. Refer to the “ASCII Character Set” appendix in the <i>Cisco IOS Configuration Fundamentals Command Reference</i> for a list of ASCII characters.	
Examples	<p>The following example changes the start character to Ctrl-B, which is decimal 2:</p> <pre> line 2 start-character 2 </pre>	
Related Commands	Command	Description
	flowcontrol	Sets the method of data flow control between the terminal or other serial device and the router.
	stop-character	Sets the flow control stop character.
	terminal start-character	Changes the flow control start character for the current session.

start-chat

To specify that a chat script start on a specified line at any point, use the **start-chat** command in privileged EXEC mode. To stop the chat script, use the **no** form of this command.

start-chat *regex* [*line-number* [*dialer-string*]]

no start-chat

Syntax Description	<i>regex</i>	Name of a regular expression or modem script to be executed. If there is more than one script with a name that matches the argument <i>regex</i> , the first script found will be used.
	<i>line-number</i>	(Optional) Line number on which to execute the chat script. If you do not specify a line number, the current line number is chosen. If the specified line is busy, the script is not executed and an error message appears. If the dialer-string argument is specified, line-number must be entered; it is not optional if you specify a dialer string. This command functions only on physical terminal (TTY) lines. It does not function on virtual terminal (VTY) lines.
	<i>dialer-string</i>	(Optional) String of characters (often a telephone number) to be sent to a DCE. If you enter a dialer string, you must also specify <i>line-number</i> , or the chat script <i>regex</i> will not start.

Command Modes Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines

This command provides modem dialing commands for a chat script that you want to apply immediately to a line. If you do not specify a line, the script runs on the current line. If the specified line is already in use, the script is not activated and an error message appears.

The argument *regex* is used to specify the name of the modem script that is to be executed. The first script that matches the argument in this command and the **dialer map** command will be used. For more information about regular expressions, refer to the “Regular Expressions” appendix in this publication.

This command functions only on physical terminal (TTY) lines. It does not function on virtual terminal lines.

Examples The following example forces a dialout on line 8 using the script telebit:

```
start-chat telebit line 8
```

Related Commands	Command	Description
	chat-script	Places calls over a modem and logs in to remote systems.
	dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
	script activation	Specifies that a chat script start on a physical terminal line when the line is activated.
	script connection	Specifies that a chat script start on a physical terminal line when a remote network connection is made to a line.
	script dialer	Specifies a default modem chat script.
	script reset	Specifies that a chat script start on a physical terminal line when the specified line is reset.
	script startup	Specifies that a chat script start on a physical terminal line when the router is powered up.

stop-character

To set the flow control stop character, use the **stop-character** command in line configuration mode. To remove the character, use the **no** form of this command.

stop-character *ascii-number*

no stop-character

Syntax Description	<i>ascii-number</i>	Decimal representation of the stop character.
Defaults	Decimal 19	
Command Modes	Line configuration	
Command History	Release	Modification
	10.0	This command was introduced.
Usage Guidelines	This command defines the character that signals the end of data transmission when software flow control is in effect. Refer to the “ASCII Character Set” appendix in the <i>Cisco IOS Configuration Fundamentals Command Reference</i> for a list of ASCII characters.	
Examples	<p>The following example changes the stop character to Ctrl-E, which is decimal 5:</p> <pre>line 3 stop-character 5</pre>	
Related Commands	Command	Description
	flowcontrol	Sets the method of data flow control between the terminal or other serial device and the router.
	source template	Sets the flow control start character.
	stop-character	Sets the flow control stop character.

syscon address

To specify the system controller for a managed shelf, use the **syscon address** command in global configuration mode. To stop the management of the shelf by the system controller, use the **no** form of this command.

syscon address *ip-address password*

no syscon address

Syntax Description	<i>ip-address</i>	IP address of the system controller.
	<i>password</i>	Password string.

Command Default No system controller is specified.

Command Modes Global configuration

Command History	Release	Modification
	11.3AA	This command was introduced.

Usage Guidelines This command is required in order for the shelf to be managed by the system controller.

Examples The following example configures a shelf to be managed by a system controller at 10.2.3.4 using the password green:

```
Router# syscon address 10.2.3.4 green
```

Related Commands	Command	Description
	show syscon sdp	Displays information about the Shelf Discovery Protocol.
	syscon source-interface	Specifies the interface to use for the source address in SDP packets.

syscon shelf-id

To specify a shelf ID for a managed shelf, use the **syscon shelf-id** command in global configuration mode. To remove the shelf ID, use the **no** form of this command.

syscon shelf-id *number*

no syscon shelf-id

Syntax Description	<i>number</i>	Shelf ID. The value ranges from 0 to 9999.
---------------------------	---------------	--

Command Default	No shelf ID is specified.
------------------------	---------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.3AA	This command was introduced.

Usage Guidelines	Use this command to specify a shelf ID for a managed shelf. Some platforms, such as the Cisco AS5800, use other commands to assign a shelf ID. In these situations, do not specify a shelf ID with the syscon shelf-id command. Use the platform-specific command instead.
-------------------------	---

Examples	The following example configures a shelf ID of 5 for the managed shelf: Router# syscon shelf-id 5
-----------------	--

Related Commands	Command	Description
	show syscon sdp	Displays information about the Shelf Discovery Protocol.
	syscon address	Specifies the system controller for a managed shelf.

syscon source-interface

To specify the interface to use for the source address in Shelf Discovery Protocol (SDP) packets, use the **syscon source-interface** command in global configuration mode. To return to the default source interface for a packet (the interface that sent the packet from the shelf), use the **no** form of this command.

syscon source-interface *type number*

no syscon source-interface

Syntax Description	<div><i>type number</i></div> Type and number of the interface to use for the source IP address.							
Command Default	SDP packets use the IP address of the output interface.							
Command Modes	Global configuration							
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>11.3AA</td><td>This command was introduced.</td></tr></table>		Release	Modification	11.3AA	This command was introduced.		
Release	Modification							
11.3AA	This command was introduced.							
Usage Guidelines	Use this command to ensure that all SDP packets sent by the managed shelf have the same source IP address.							
Examples	The following example configures a shelf to use the IP address of Ethernet interface 99/1/0: <pre>Router# syscon source-address Ethernet99/1/0</pre>							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show syscon sdp</td><td>Displays information about the Shelf Discovery Protocol.</td></tr><tr><td>syscon shelf-id</td><td>Specifies a shelf ID for a managed shelf.</td></tr></table>		Command	Description	show syscon sdp	Displays information about the Shelf Discovery Protocol.	syscon shelf-id	Specifies a shelf ID for a managed shelf.
Command	Description							
show syscon sdp	Displays information about the Shelf Discovery Protocol.							
syscon shelf-id	Specifies a shelf ID for a managed shelf.							

tdm clock priority

To configure the clock source and priority of the clock source used by the time-division multiplexing (TDM) bus on the Cisco AS5350 and AS5400 access servers, use the **tdm clock priority** command in global configuration mode. To return the clock source and priority to the default values, use the **no** form of this command.

tdm clock priority *priority-number* { *slot/ds1-port* | *slot/ds3-port:ds1-port* | **external** | **freerun** }

no tdm clock priority *priority-number* { *slot/ds1-port* | *slot/ds3-port:ds1-port* | **external** | **freerun** }

Syntax Description

<i>priority-number</i>	Priority of the clock source. The priority range is from 1 to 99. A clock set to priority 100 will not drive the TDM bus.
<i>slot/ds1-port</i>	Trunk-card slot is a value from 1 to 7. DS1 port number controller is a value between 0 and 7. Specify with a slash separating the numbers; for example, 1/1.
<i>slot/ds3-port:ds1-port</i>	Trunk-card slot is a value from 1 to 7. DS3 port specifies the T3 port. DS1 port number controller is a value from 1 to 28. Specify with a slash separating the slot and port numbers, and a colon separating the DS1 port number. An example is 1/0:19.
external	Synchronizes the TDM bus with an external clock source that can be used as an additional network reference.
freerun	Selects the free-running clock from the local oscillator when there is no good clocking source from a trunk card or an external clock source.

Defaults

If no clocks are configured, the system uses a default, primary clock. An external clock is never selected by default; it must be explicitly configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

The TDM bus on the Cisco AS5350 and Cisco AS5400 backplane can receive an input clock from one of three sources on the gateway:

- CT1, CE1, and CT3 trunk cards
- An external T1/E1 clock source feed directly through the Building Integrated Timing Supply (BITS) interface port on the motherboard
- Free-running clock providing clock from an oscillator

**Note**

BITS is a single building master timing supply. BITS generally supplies DS1- and DS0-level timing throughout an office. BITS is the clocks that provide and distribute timing to a wireline network's lower levels.

Trunk-Card Ports

The TDM bus can be synchronized with any trunk cards. On the CT1/CE1 trunk card, each port receives the clock from the T1/E1 line. The CT3 trunk card uses an M13 multiplexer to receive the DS1 clock. Each port on each trunk-card slot has a default clock priority. Also, clock priority is configurable through the **tdm clock priority** command.

External Clock

The TDM bus can be synchronized with an external clock source that can be used as an additional network reference. If no clocks are configured, the system uses a primary clock through a software-controlled default algorithm. If you want the external T1/E1 clock (from the BITS interface) as the primary clock source, you must configure it using the **external** keyword with the **tdm clock priority** command; the external clock is never selected by default.

The BITS interface requires a T1 line composite clock reference set at 1.544 MHz and an E1 line composite clock reference set at 2.048 MHz.

Free-Running Clock

If there is no good clocking source from a trunk card or an external clock source, then select the free-running clock from the internal oscillator using the **freerun** keyword with the **tdm clock priority** command.

Examples

In the following example, BITS clock is set at priority 1:

```
AS5400(config)# tdm clock priority priority 1 external
```

In the following example, a trunk clock from a CT1 trunk card is set at priority 2 and uses slot 4 and DS1 port (controller) 6:

```
AS5400(config)# tdm clock priority priority 2 4/6
```

In the following example, a trunk clock from a CT3 trunk card is set at priority 2 and uses slot 1, DS3 port 0, and DS1 port 19:

```
AS5400(config)# tdm clock priority priority 2 1/0:19
```

In the following example, free-running clock is set at priority 3:

```
AS5400(config)# tdm clock priority priority 3 freerun
```

Related Commands

Command	Description
dial-tdm-clock	Configures the clock source and priority of the clock source used by the TDM bus on the dial shelf of the Cisco AS5800.
show tdm clocks	Displays default system clocks and clock history.

template

To access the template configuration mode for configuring a particular customer profile template, use the **template** command in global configuration mode. To delete the template of the specified name, use the **no** form of this command.

template *name* [**default** | **exit** | **multilink** | **no** | **peer** | **ppp**]

no template *name* [**default** | **exit** | **multilink** | **no** | **peer** | **ppp**]

Syntax Description

<i>name</i>	Identifies the template.
default	(Optional) Sets the command to its defaults.
exit	(Optional) Exits from resource-manager configuration mode.
multilink	(Optional) Configures multilink parameters.
no	(Optional) Negates the command or its defaults.
peer	(Optional) Accesses peer parameters for point-to-point interfaces.
ppp	(Optional) Accesses Point-to-Point Protocol.

Defaults

No templates are configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(6)T	This command was introduced.

Usage Guidelines

All PPP and peer-default commands are enabled for a customer profile template under this grouping.

Examples

The following example shows the creation and configuration of a customer profile template named **acme-direct** and its subsequent assignment to the customer profile **acme1**:

```
template acme-direct
  multilink max-fragments 10
  peer match aaa-pools
  peer default ip address pool acme-numbers
  ppp ipcp dns 10.1.1.1 10.2.2.2
  ppp multilink
  exit
resource-pool profile customer acme1
source template acme-direct
```

Related Commands

Command	Description
source template	Attaches a configured customer profile template to a customer profile.

terminate-from

To specify the host name of the remote L2TP access concentrator (LAC) or L2TP network server (LNS) that will be required when accepting a virtual private dialup network (VPDN) tunnel, use the **terminate-from** command in VPDN group configuration mode. To remove the host name from the VPDN group, use the **no** form of this command.

terminate-from *hostname host-name*

no terminate-from [*hostname host-name*]

Syntax Description	hostname <i>host-name</i> The host name that this VPDN group will accept connections from.
---------------------------	---

Defaults	Disabled
-----------------	----------

Command Modes	VPDN group configuration
----------------------	--------------------------

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

Usage Guidelines	Before you can use this command, you must have already enabled one of the two accept VPDN subgroups by using either the accept-dialin or accept-dialout command.
	Each VPDN group can only terminate from a single host name. If you enter a second terminate-from command on a VPDN group, it will replace the first terminate-from command.

Examples	The following example configures a VPDN group to accept L2TP tunnels for dialout calls from the LNS cerise by using dialer 2 as its dialing resource:
-----------------	---

```
vpdn-group 1
 accept-dialout
 protocol l2tp
 dialer 2
 terminate-from hostname cerise
```

Related Commands	Command	Description
	accept-dialin	Specifies the LNS to use for authenticating, and the virtual template to use for cloning, new virtual access interfaces when an incoming L2TP tunnel connection is requested from a specific peer.
	accept-dialout	Accepts requests to tunnel L2TP dial-out calls and creates an accept-dialout VPDN subgroup

test modem back-to-back

To diagnose an integrated modem that may not be functioning properly, use the **test modem back-to-back** command in EXEC mode.

test modem back-to-back *first-slot/port second-slot/port*

Syntax Description

<i>first-slot/port</i>	Slot and modem number of the first test modem. (Include the forward slash (/) when entering this variable.)
<i>second-slot/port</i>	Slot and modem number of the second test modem. (Include the forward slash (/) when entering this variable.)

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to perform back-to-back testing of two modems. You might need to enable this command on several different combinations of modems to determine which one is not functioning properly.

Examples

The following example performs a back-to-back modem test between modem 2/0 and modem 2/1 and removes modem 2/1 (which is associated with TTY line 26) from all dial-in and dial-out services:

```
Router# test modem back-to-back 2/0 2/1
```

```
back2back 2/0 2/1
Repetitions (of 10-byte packets) [1]:
```

```
Router#
```

```
%MODEM-5-B2BCONNECT: Modems (2/0) and (2/1) connected in back-to-back test:
CONNECT9600/REL-MNPM
%MODEM-5-B2BMODEMS: Modems (2/0) and (2/1) completed back-to-back test: success/packets =
2/2
```

Related Commands

Command	Description
modem bad	Removes an integrated modem from service and indicates it as suspected or proven to be inoperable.

test port modem back-to-back

To test two specified ports back-to-back and transfer a specified amount of data between the ports, use the **test port modem back-to-back** command in EXEC mode.

Cisco AS5400 with NextPort DFC

test port modem back-to-back {*slot/port*}

Cisco AS5800 with Universal Port Card

test port modem back-to-back {*shelf/slot/port*}

Syntax Description	<i>slot/port</i>	All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and port values range from 0 to 107.
	<i>shelf/slot/port</i>	All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and port values range from 0 to 323.

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	11.3	The test modem back-to-back form of this command was introduced.
	12.1(1)XD	This command was implemented on the Cisco AS5400.
	12.1(3)T	This command was implemented on the Cisco AS5800.

Usage Guidelines	The test port modem back-to-back command should be performed on different combinations to determine a good port.
-------------------------	---



Note

The **test port modem back-to-back** command is similar to the **test modem back-to-back** MICA modem command.

Examples	The following example displays a back-to-back test:
-----------------	---

```
Router# test port modem back-to-back 1/1/1
```

```
Repetitions (of 10-byte packets) [1]:
```

```
*Mar 02 12:13:51.743:%PM_MODEM_MAINT-5-B2BCONNECT:Modems (2/10) and (3/20) connected in back-to-back test:CONNECT33600/V34/LAP
```

```
*Mar 02 12:13:52.783:%PM_MODEM_MAINT-5-B2BMODEMS:Modems (3/20) and (2/10) completed back-to-back test:success/packets = 2/2
```

Related Commands	Command	Description
	port modem autotest	Automatically and periodically performs a modem diagnostics test for modems inside the access server or router.
	show port modem test	Displays the modem test log.

timeout absolute

To specify a timeout period that controls how long a session can be connected before it is terminated, use the **timeout absolute** command in interface configuration mode. To remove the session timeout period, use the **no** form of this command.

timeout absolute *minutes* [*seconds*]

no timeout absolute

Syntax Description	<i>minutes</i>	Session lifetime in minutes, in the range from 0 to 71582787 minutes.
	<i>seconds</i>	(Optional) Session lifetime in seconds, in the range from 0 to 59 seconds.

Defaults	No default behavior or values.
-----------------	--------------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	11.3	This command was introduced.

Examples The following partial example shows how to impose a 15-minute (900-second) idle timeout and a 12-hour (720-minute) absolute timeout for session connections:

```
interface Serial0:23
  dialer idle-timeout 900
  timeout absolute 720
!
interface Serial11:23
  dialer idle-timeout 900
  timeout absolute 720
.
.
.
```

Related Commands	Command	Description
	ppp idle timeout	Sets PPP idle timeout parameters.
	dialer idle-timeout	Specifies the idle time before the line is disconnected.

timer

To set the Redundant Link Manager (RLM) timer, use the **timer** command in RLM configuration mode. The associated options can overwrite the default setting of timeout values. To disable this function, use the **no** form of this command.

timer {**force-down** | **keepalive** | **minimum-up** | **open-wait** | **recovery** | **retransmit** | **switch-link**} *seconds*

no timer {**force-down** | **keepalive** | **minimum-up** | **open-wait** | **recovery** | **retransmit** | **switch-link**} *seconds*

Syntax Description		
force-down		After RLM enters the down state, RLM will stay in the down state for a certain amount of time to make sure that the remote end will also enter the down state. After this occurs, both can be forced to be in sync again. This timer can also prevent RLM links from going up and down rapidly in an unstable network environment.
keepalive		A keepalive packet will be sent out from Network Access Server (NAS) to CSC periodically.
minimum-up		After a link is recovered from the failure state and RLM is in the up state, RLM will wait for a minimum time to make sure the new recovered link is stabilized before doing any operation.
open-wait		To overcome the latency while opening several links at the same time, RLM will use this timer to wait before opening the new links, and then choose the link with the highest weighting to become the active signalling link.
recovery		When the network access server (NAS) loses the active connection to CSC, it will try to reestablish the connection within the interval specified by this command. If it fails to reestablish the connection, RLM will declare that the RLM signalling link is down.
retransmit		Because RLM is operating under UDP, it needs to retransmit the control packet if the packet is not acknowledged within this retransmit interval.
<i>seconds</i>		Time, in seconds, before executing the designated function.
switch-link		The maximum transition period allows RLM to switch from a lower preference link to a higher preference link. If the switching link does not complete successfully before this timer expires, RLM will go into the recovery state.

Defaults Disabled

Command Modes RLM configuration

Command History	Release	Modification
	11.3(7)	This command was introduced.

Related Commands	Command	Description
	clear interface	Resets the hardware logic on an interface.
	clear rlm group	Clears all RLM group time stamps to zero.
	interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
	link (RLM)	Specifies the link preference.
	protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
	retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
	server (RLM)	Defines the IP addresses of the server.
	show rlm group statistics	Displays the network latency of the RLM group.
	show rlm group status	Displays the status of the RLM group.
	show rlm group timer	Displays the current RLM group timer values.
	shutdown (RLM)	Shuts down all of the links under the RLM group.

trunk group (global)

To define a trunk group, use the **trunk group** command in global configuration mode. To disable the specified trunk group, use the **no** form of this command.

trunk group *group-number* [**max-calls** { **any** | **voice** | **data** } *number*] [**direction in** | **out**]
[**max-retries** *retries*]

no trunk group *group-number*

Syntax Description

<i>group-number</i>	Identifier for this trunk group, in the range 1 to 1000.
max-calls [any voice data] <i>number</i>	(Optional) Specifies the maximum number of voice or data calls allowed on this trunk group or the maximum number of any type of calls allowed on this trunk group, in the range 1 to 1000.
direction in out	(Optional) Specifies whether the trunk group is restricted to incoming or outgoing calls.
max-retries <i>retries</i>	(Optional) Specifies the maximum number of outgoing call attempts when a glare situation is encountered, in the range 1 to 5. The default value is the number of interfaces that belong to the trunk group

Defaults

No trunk group is defined.

If the **max-calls any** keyword is not specified, the trunk group allows all calls, both incoming and outgoing.

The default maximum number of retries is 1.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use this command to define the trunk group. Then if you decide to configure an interface for the Network Side ISDN PRI feature, use a **trunk-group** interface configuration command to assign the interface to a defined trunk group.

However, a trunk group need not be defined globally before being configured on an interface. If it has not been defined, it will be created.

The **max-calls** keyword set can be repeated to allow you to specify the maximum number of voice calls, the maximum number of data calls, and the maximum number of any calls.

Examples

The following example defines trunk group 101 but does not specify a maximum number of calls:

```
trunk group 101
```

The following example specifies multiple maximums. In the first version of the example, the maximums are shown on separate lines for readability, but in reality they are part of a single command:

```
trunk group 101
  max-calls any 100
  max-calls voice 30
  max-calls data 60 direction in
```

In the second version of the example, the same command is shown in a single run-on line:

```
trunk group 101 max-calls any 100 max-calls voice 30 max-calls data 60 direction in
```

Related Commands

Command	Description
trunk-group (interface)	Assigns a PRI interface to a defined trunk group.

tunnel

To set up a network layer connection to a router, use the **tunnel** command in EXEC mode.

tunnel *host*

Syntax Description	<i>host</i>	Name or IP address of a specific host on a network that can be reached by the router.
--------------------	-------------	---

Command Modes	User EXEC
---------------	-----------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines

If you are a mobile user, it is often impractical to dial in to your “home” router from a remote site. The asynchronous mobility feature allows you to dial in to different routers elsewhere on the internetwork while experiencing the same server environment that you would if you were connecting directly to your home router.

This asynchronous host mobility is accomplished by packet tunneling, a technique by which raw data from the dial-in user is encapsulated and transported directly to the host site where your home router performs the actual protocol processing.

You enable asynchronous mobility by entering the **tunnel** command to set up a network layer connection to a specified host. From a router other than a Cisco router, however, you need to use the Telnet protocol.

After a connection is established, you receive an authentication dialog or prompt from your home router and can proceed as if you are connected directly to it. When communications are complete, the network connection can be closed and terminated from either end of the connection.

Examples

The following example establishes a network layer connection with an IBM host named mktg:

```
Router> tunnel mktg
```


virtual-profile aaa

To enable virtual profiles by authentication, authorization, and accounting (AAA) configuration, use the **virtual-profile aaa** command in global configuration mode. To disable virtual profiles, use the **no** form of this command.

virtual-profile aaa

no virtual-profile aaa

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	11.2 F	This command was introduced.
	12.0(7)T	This command was enhanced to allow virtual profiles to be downloaded from an AAA server using the HDLC, LAPB-TA, X.25, and Frame Relay encapsulations, in addition to the originally supported PPP encapsulation.

Usage Guidelines The effect of this command for any specific user depends on the router being configured for AAA and the AAA server being configured for that user's specific configuration information.

Examples The following example configures virtual profiles by AAA configuration only:

```
virtual-profile aaa
```

Related Commands	Command	Description
	aaa authentication	Enables AAA authentication to determine if a user can access the privileged command level.
	virtual-profile if-needed	Enables virtual profiles by virtual interface template.

virtual-profile if-needed

To specify that a virtual profile be used to create a virtual access interface only if the inbound connection requires a virtual access interface, use the **virtual-profile if-needed** command in global configuration mode. To create virtual access interfaces for every inbound connection, use the **no** form of this command.

virtual-profile if-needed

no virtual-profile if-needed

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

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

Usage Guidelines This command is intended to prevent the creating of virtual-access interfaces for inbound calls on physical interfaces that do not require virtual-access interfaces.

This command is compatible with local, RADIUS, and TACACS+ AAA.

Examples The following example enables selective virtual-access interface creation:

```
virtual-profile if-needed
```

Related Commands	Command	Description
	interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
	virtual-profile aaa	Enables virtual profiles by AAA configuration.
	virtual-profile virtual-template	Enables virtual profiles by virtual interface template.

virtual-profile virtual-template

To enable virtual profiles by virtual interface template, use the **virtual-profile virtual-template** command in global configuration mode. To disable this function, use the **no** form of this command.

virtual-profile virtual-template *number*

no virtual-profile virtual-template *number*

Syntax Description

<i>number</i>	Number of the virtual template to apply, in the range 1 to 30.
---------------	--

Defaults

Disabled. No virtual template is defined, and no default virtual template number is used.

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

When virtual profiles are configured by virtual templates only, any interface-specific configuration information that is downloaded from the AAA server is ignored in configuring the virtual access interface for a user.

The **interface virtual-template** command defines a virtual template to be used for virtual profiles. Because several virtual templates might be defined for different purposes on the router (such as MLP, PPP over ATM, and virtual profiles), it is important to be clear about the virtual template number to use in each case.

Examples

The following example configures virtual profiles by virtual templates only. The number 2 was chosen because virtual template 1 was previously defined for use by Multilink PPP.

```
virtual-profile virtual-template 2
```

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.

virtual-template

To specify which virtual template will be used to clone virtual access interfaces, use the **virtual-template** command in accept-dialin configuration mode. To remove the virtual template from an accept-dialin virtual private dialup network (VPDN) subgroup, use the **no** form of this command.

virtual-template *template-number*

no virtual-template

Syntax Description

<i>template-number</i>	Number of the virtual template that will be used to clone virtual-access interfaces.
------------------------	--

Defaults

Disabled

Command Modes

Accept-dialin configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(1)T	This command was enhanced to enable PPPoE on ATM to accept dialin PPPoE sessions.

Usage Guidelines

Each accept-dialin group can only clone virtual-access interfaces using one virtual template. If you enter a second **virtual-template** command on an accept-dialin subgroup, it will replace the first **virtual-template** command.

You must first enable a tunneling protocol on the accept-dialin VPDN subgroup (using the **protocol** command) before you can enable the **virtual-template** command. Removing or modifying the **protocol** command will remove **virtual-template** command from the request-dialin subgroup.

Examples

The following example enables the LNS to accept an L2TP tunnel from a LAC named mugsy. A virtual-access interface will be cloned from virtual template 1.

```
vpdn-group 1
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname mugsy
```

The following example enables PPPoE on ATM to accept dialin PPPoE sessions. A virtual access interface for the PPP session is cloned from virtual template 1.

```
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
```

Related Commands	Command	Description
	accept-dialin	Configures an LNS to accept tunneled PPP connections from a LAC and create an accept-dialin VPDN subgroup.

vpng aaa attribute

To enable reporting of network access server (NAS) authentication, authorization, and accounting (AAA) attributes related to a virtual private dialup network (VPDN) to the AAA server, use the **vpng aaa attribute** command in global configuration mode. To disable reporting of AAA attributes related to VPDN, use the **no** form of this command.

vpng aaa attribute {nas-ip-address vpng-nas | nas-port vpng-nas}

no vpng aaa attribute {nas-ip-address vpng-nas | nas-port}

Syntax Description

nas-ip-address vpng-nas	Enable reporting of the VPDN NAS IP address to the AAA server.
nas-port vpng-nas	Enable reporting of the VPDN NAS port to the AAA server.

Command Default

AAA attributes are not reported to the AAA server.

Command Modes

Global configuration

Command History

Release	Modification
11.3 NA	This command was introduced.
11.3(8.1)T	This command was integrated into Cisco IOS Release 11.3(8.1)T.
12.1(5)T	This command was modified to support the PPP extended NAS-Port format.

Usage Guidelines

This command can be used with RADIUS or TACACS+, and is applicable only on the VPDN tunnel server.

The PPP extended NAS-Port format enables the NAS-Port and NAS-Port-Type attributes to provide port details to a RADIUS server when one of the following protocols is configured:

- PPP over ATM
- PPP over Ethernet (PPPoE) over ATM
- PPPoE over 802.1Q VLANs

Before PPP extended NAS-Port format attributes can be reported to the RADIUS server, the **radius-server attribute nas-port format** command with the **d** keyword must be configured on both the tunnel server and the NAS, and the tunnel server and the NAS must both be Cisco routers.

Examples

The following example configures VPDN on a tunnel server and enables reporting of VPDN AAA attributes to the AAA server:

```
vpng enable
vpng-group 1
accept-dialin
```

```

protocol any
virtual-template 1
!
terminate-from hostname nas1
local name ts1
!
vpdn aaa attribute nas-ip-address vpdn-nas
vpdn aaa attribute nas-port vpdn-nas

```

The following example configures the tunnel server for VPDN, enables AAA, configures a RADIUS AAA server, and enables reporting of PPP extended NAS-Port format values to the RADIUS server. PPP extended NAS-Port format must also be configured on the NAS for this configuration to be effective.

```

vpdn enable
vpdn-group L2TP-tunnel
accept-dialin
protocol l2tp
virtual-template 1
!
terminate-from hostname nas1
local name ts1
!
aaa new-model
aaa authentication ppp default local group radius
aaa authorization network default local group radius
aaa accounting network default start-stop group radius
!
radius-server host 171.79.79.76 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute nas-port format d
radius-server key ts123
!
vpdn aaa attribute nas-port vpdn-nas

```

Related Commands

Command	Description
radius-server attribute nas-port format	Selects the NAS-Port format used for RADIUS accounting features.

vpdn aaa override-server

To specify an authentication, authorization, and accounting (AAA) server to be used for virtual private dialup network (VPDN) tunnel authorization other than the default AAA server, use the **vpdn aaa override-server** global configuration command. To return to the default setting, use the **no** form of this command.

vpdn aaa override-server {*aaa-server-ip-address* | *aaa-server-name*}

no vpdn aaa override-server {*aaa-server-ip-address* | *aaa-server-name*}

Syntax Description

<i>aaa-server-ip-address</i>	The IP address of the AAA server to be used for tunnel authorization.
<i>aaa-server-name</i>	The name of the AAA server to be used for tunnel authorization.

Defaults

If the AAA server is not specified, the default AAA server configured for network authorization is used.

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

This command can be used with RADIUS or TACACS+, and is applicable only on the VPDN network access server (NAS). Configuring this command restricts tunnel authorization to the specified AAA servers only. This command can be used to specify multiple AAA servers.

For TACACS+ configuration, the **tacacs-server directed-request** command must be configured using the **restricted** keyword, or authorization will continue with all configured TACACS+ servers.

Examples

The following example enables AAA attributes and specifies the AAA server to be used for VPDN tunnel authorization:

```
aaa new-model
aaa authorization network default group radius
vpdn aaa override-server 10.1.1.1
vpdn enable
radius-server host 10.1.1.2 auth-port 1645 acct-port 1646
radius-server key Secret
```


Related Commands	Command	Description
	aaa new-model	Enables the AAA access control model.
	tacacs-server directed-request	Sends only a username to a specified server when a direct request is issued.
	vpdn enable	Enables VPDN on the router and directs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.

vpdn aaa untagged

To apply untagged attribute values obtained from the authentication, authorization, and accounting (AAA) RADIUS server to all attribute sets for Virtual Private Dialup Network (VPDN) tunnels, use the **vpdn aaa untagged** command in global configuration mode. To disable this function, use the **no** form of this command.

vpdn aaa untagged

no vpdn aaa untagged

Syntax Description

This command has no arguments or keywords.

Defaults

Untagged attribute values are applied to all attribute sets.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)T	This command was introduced.

Usage Guidelines

Untagged attribute values obtained from the AAA RADIUS server will be applied to all attribute sets by default, unless a value for that attribute is already specified in the tagged attribute set. To prevent untagged attribute values from being applied to tagged attribute sets, use the **no** form of this command.

Examples

The following example disables the application of untagged attribute values to attribute sets:

```
no vpdn aaa untagged
```

vpdn authen-before-forward

To configure a network access server (NAS) to request authentication of a complete username before making a forwarding decision for all dial-in Layer 2 Tunnel Protocol (L2TP) or Layer 2 Forwarding (L2F) tunnels, use the **vpdn authen-before-forward** command in global configuration mode. To disable this configuration, use the **no** form of this command.

vpdn authen-before-forward

no vpdn authen-before-forward

Syntax Description This command has no arguments or keywords.

Command Default L2TP or L2F tunnels are forwarded to the tunnel server without first requesting authentication of the complete username.

Command Modes Global configuration

Command History	Release	Modification
	11.3	This command was introduced.

Usage Guidelines To configure the NAS to perform authentication of all dial-in L2TP or L2F sessions before the sessions are forwarded to the tunnel server, configure the **vpdn authen-before-forward** command in global configuration mode.

To configure the NAS to perform authentication of dial-in L2TP or L2F sessions belonging to a specific VPDN group before the sessions are forwarded to the tunnel server, use the **authen-before-forward** command in VPDN group configuration mode.

Enabling the **vpdn authen-before-forward** command instructs the NAS to authenticate the complete username before making a forwarding decision based on the domain portion of the username. A user may be forwarded or terminated locally depending on the information contained in the users RADIUS profile. Users with forwarding information in their RADIUS profile are forwarded based on that information. Users without forwarding information in their RADIUS profile are either forwarded or terminated locally based on the Service-Type in their RADIUS profile. The relationship between forwarding decisions and the information contained in the users RADIUS profile is summarized in [Table 128](#).

Table 128 Forwarding Decisions Based on RADIUS Profile Attributes

Forwarding Information Is	Service-Type Is Outbound	Service-Type Is Not Outbound
Present in RADIUS profile	Forward User	Forward User
Absent from RADIUS profile	Check Domain	Terminate Locally

Examples

The following example configures the NAS to request authentication of all dial-in L2TP or L2F sessions before the sessions are forwarded to the tunnel server:

```
vpdn authen-before-forward
```

Related Commands

Command	Description
authen-before-forward	Configures a NAS to request authentication of a complete username before making a forwarding decision for dial-in L2TP or L2F tunnels belonging to a VPDN group.

vpdn authorize directed-request

To enable virtual private dialup network (VPDN) authorization for directed-request users, use the **vpdn authorize directed-request** command in global configuration mode. To disable VPDN authorization for directed request users, use the **no** form of this command.

vpdn authorize directed-request

no vpdn authorize directed-request

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

Defaults	VPDN authorization for directed-request users is disabled.
-----------------	--

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.1	This command was introduced.

Usage Guidelines	<p>When a username includes both a username and a domain portion, such as user@site.com, directed request configuration allows the authorization request to be sent to a specific RADIUS or TACACS+ server based on the domain name portion of the username (site.com). The vpdn authorize directed-request command must be enabled to allow VPDN authorization of any directed request user.</p> <p>Directed request for RADIUS users is enabled by issuing the radius-server directed-request command. Directed request for TACACS+ users is enabled by default, and may be disabled using the no tacacs-server directed request command. The ip host command must be configured to enable directed requests to RADIUS or TACACS+ servers.</p> <p>The vpdn authorize directed-request command is usually configured on the L2TP network server (LNS). When directed-requests are used on an L2TP access concentrator (LAC) in conjunction with per-user VPDN configuration, the authen before-forward command must be enabled.</p>
-------------------------	--

Examples	The following example enables VPDN authorization and RADIUS directed requests on an LNS:
-----------------	--

```
ip host site.com 10.1.1.1
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server directed-request
vpdn authorize directed-request
```

The following example enables VPDN authorization and TACACS+ directed requests on an LNS:

```
ip host site.com 10.1.1.1
tacacs-server host 10.1.1.1
tacacs-server directed-request
vpdn authorize directed-request
```

The following example enables per-user VPDN and enables VPDN authorization for directed request users on a LAC:

```
vpdn-group 1
 request-dialin
  protocol l2f
  domain site.com
!
 initiate-to ip 10.1.1.1
 local name local1
 authen before-forward
!
 ip host site.com 10.1.1.1
 vpdn authorize directed-request
!
 radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
 radius-server directed-request
```

Related Commands

Command	Description
authen before-forward	Specifies that the VPDN sends the entire structured username to the AAA server the first time the router contacts the AAA server.
ip host	Defines a static host name-to-address mapping in the host cache.
radius-server directed-request	Allows users logging into a Cisco NAS to select a RADIUS server for authentication.
tacacs-server directed-request	Sends only a username to a specified server when a direct request is issued.

vpdn domain-delimiter

To specify the characters to be used to delimit the domain prefix or domain suffix, use the **vpdn domain-delimiter** command in global configuration mode. To disable this function, use the **no** form of this command.

vpdn domain-delimiter *characters* [**suffix** | **prefix**]

no vpdn domain-delimiter *characters* [**suffix** | **prefix**]

Syntax Description	<i>characters</i>	One or more specific characters to be used as suffix or prefix delimiters. Available characters are %, -, @, \, #, and /. If a backslash (\) is the last delimiter in the command line, enter it as a double backslash (\\).
	suffix prefix	(Optional) Usage of the specified characters.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	11.3	This command was introduced.

Usage Guidelines You can enter one **vpdn domain-delimiter** command to list the suffix delimiters and another **vpdn domain-delimiter** command to list the prefix delimiters. However, no character can be both a suffix delimiter and a prefix delimiter.

This command allows the network access server to parse a list of home gateway DNS domain names and addresses sent by an AAA server. The AAA server can store domain names or IP addresses in the following AV pair:

cisco-avpair = "lcp:interface-config=ip address 10.1.1.1 255.255.255.255.0",

cisco-avpair = "lcp:interface-config=ip address bigrouter@excellentinc.com,

Examples The following example lists three suffix delimiters and three prefix delimiters:

```
vpdn domain-delimiter %-@ suffix
vpdn domain-delimiter #/\ prefix
```

This example allows the following host and domain names:

```
cisco.com#houstondrr
houstondrr@cisco.com
```

Related Commands

Command	Description
vpdn enable	Enables VPDN on the router and directs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
vpdn-group	Sets the failure history table depth beyond the default value of 20 entries.
vpdn history failure	Enables logging of VPDN failures to the history failure table or to set the failure history table size.
vpdn profile	Specifies how the network access server for the service provider is to perform VPDN tunnel authorization searches.

vpdn enable

To enable virtual private dialup networking on the router and inform the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present, use the **vpdn enable** command in global configuration mode. To disable, use the **no** form of this command.

vpdn enable

no vpdn enable

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

Defaults	Disabled
-----------------	----------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines	To disable a VPN tunnel, use the command clear vpdn tunnel in EXEC mode. The command no vpdn enable does not automatically disable a VPN tunnel.
-------------------------	--

Examples	The following example enables virtual private dialup networking on the router: vpdn enable
-----------------	---

Related Commands	Command	Description
	vpdn-group	Sets the failure history table depth beyond the default value of 20 entries.
	vpdn history failure	Enables logging of VPDN failures to the history failure table or to set the failure history table size.

vpdn group

To associate a virtual private dialup network (VPDN) group with a customer or VPDN profile, use the **vpdn group** command in customer profile or VPDN profile configuration mode. To disassociate a VPDN group from a customer or VPDN profile, use the **no** form of this command.

vpdn group *name*

no vpdn group *name*

Syntax Description

<i>name</i>	Name of the VPDN group.
Note	This name should match the name defined for the VPDN group configured with the vpdn-group command.

Defaults

No default behavior or values.

Command Modes

Customer profile configuration
VPDN profile 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

Use the **vpdn group** command in customer profile configuration mode or VPDN profile configuration mode to associate a VPDN group with a customer profile or a VPDN profile, respectively.

VPDN groups are created using the **vpdn-group** command in global configuration mode.

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
```

The following example creates two VPDN groups and configures them under a customer profile named company2:

```
Router(config)# vpdn-group mygroup
Router(config-vpdn)#
!
Router(config)# vpdn-group yourgroup
Router(config-vpdn)#
!
Router(config)# resource-pool profile vpdn company2
Router(config-vpdn-profile)# vpdn group mygroup
Router(config-vpdn-profile)# vpdn group yourgroup
```

Related Commands

Command	Description
resource-pool profile customer	Creates a customer profile and enters customer profile configuration mode.
resource-pool profile vpdn	Creates a VPDN profile and enters VPDN profile configuration mode.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn profile	Associates a VPDN profile with a customer profile.

vpdn history failure

To enable logging of virtual private dialup network (VPDN) failures to the history failure table or to set the failure history table size, use the **vpdn history failure** command in global configuration mode. To disable logging of VPDN history failures or to restore the default table size, use the **no** form of this command.

```
vpdn history failure [table-size entries]

no vpdn history failure [table-size]
```

Syntax Description	table-size <i>entries</i> (Optional) Sets the number of entries in the history failure table. Valid entries range from 20 to 50.
--------------------	---

Defaults	VPDN failures are logged by default. table size: 20 entries
----------	---

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	11.3 T	This command was introduced.

Usage Guidelines	<p>Logging of VPDN failure events is enabled by default. You can disable the logging of VPDN failure events by issuing the no vpdn history failure command.</p> <p>The logging of a failure event to the history table is triggered by event logging by the syslog facility. The syslog facility creates a failure history table entry, which keeps records of failure events. The table starts with 20 entries, and the size of the table can be expanded to a maximum of 50 entries using the vpdn history failure table-size <i>entries</i> command. You may configure the vpdn history failure table-size <i>entries</i> command only if VPDN failure event logging is enabled.</p> <p>All failure entries for the user are kept chronologically in the history table. Each entry records the relevant information of a failure event. Only the most recent failure event per user, unique to its name and tunnel client ID (CLID), is kept.</p> <p>When the total number of entries in the table reaches the configured table size, the oldest record is deleted and a new entry is added.</p>
------------------	--

Examples	<p>The following example disables logging of VPDN failures to the history failure table:</p> <pre>no vpdn history failure</pre> <p>The following example enables logging of VPDN failures to the history table and sets the history failure table size to 40 entries:</p> <pre>vpdn history failure vpdn history failure table-size 40</pre>
----------	--

Related Commands

Command	Description
show vpdn history failure	Displays the content of the failure history table.

vpdn incoming

The **vpdn incoming** command is replaced by the **accept-dialin** command. See the description of the [accept-dialin](#) command for more information.

vpdn logging

To enable the logging of virtual private dialup network (VPDN) events, use the **vpdn logging** command in global configuration mode. To disable the logging of VPDN events, use the **no** form of this command.

vpdn logging [**local** | **remote** | **user**]

no vpdn logging [**local** | **remote** | **user**]

Syntax Description	local	(Optional) Enables logging of VPDN events to the syslog locally.
	remote	(Optional) Enables logging of VPDN events to the syslog of the remote tunnel endpoint.
	user	(Optional) Enables logging of VPDN user events to the syslog.

Defaults All VPDN event logging is disabled.

Command Modes Global configuration

Command History	Release	Modification
	11.3T	This command was introduced.
	12.1	The user keyword was introduced in Cisco IOS Release 12.1.

Usage Guidelines

This command controls the logging of VPDN events. By default, all VPDN event logging is disabled.

To enable the logging of VPDN events to the system message logging (syslog) of the local or remote tunnel endpoint router, issue the **vpdn logging** command with the **local** or **remote** keyword.

To log VPDN user events to the syslog, you must configure the **vpdn logging** command with the **user** keyword.

You may configure as many types of VPDN event logging as you want.

Examples

The following example enables VPDN logging locally:

```
vpdn logging local
```

The following example disables VPDN event logging locally, enables VPDN event logging at the remote tunnel endpoint, and enables the logging of VPDN user events to the syslog of the remote router:

```
no vpdn logging local
vpdn logging remote
vpdn logging user
```

Related Commands

Command	Description
vpdn history failure	Enables logging of VPDN failures to the history failure table or sets the failure history table size.

vpdn multihop

To enable virtual private dialup network (VPDN) multihop, use the **vpdn multihop** command in global configuration mode. To disable VPDN multihop capability, use the **no** form of this command.

vpdn multihop

no vpdn multihop

Syntax Description This command has no arguments or keywords.

Defaults Multihop is not enabled.

Command Modes Global configuration

Command History	Release	Modification
	11.3(5)T	This command was introduced.

Usage Guidelines The Cisco Multihop VPDN feature allows you to perform Multichassis Multilink Point-to-Point Protocol (MMP) on a home gateway (HGW) or Layer 2 Tunneling Protocol (L2TP) network server (LNS) in a VPDN scenario. This feature allows sharing tunnel resources between the HGW and LNS routers, and the possibility to offload by default to another router in the network.

The VPDN multihop feature also allows a router configured as a tunnel switch to terminate tunnels from Layer 2 access concentrators (LACs) and forward the sessions through up to four newly established L2TP tunnels. The tunnels are selected using client-supplied matching criteria configured by the **vpdn search-order** global configuration command.

Before using the **vpdn multihop** command, refer to the [Cisco IOS Dial Technologies Configuration Guide](#), Release 12.2, to learn more about Multilink PPP and MMP.

Examples The following example shows a configuration where a packet traverses a VPDN tunnel over a service provider link, and then a second tunnel by traversing a hop between home gateways on the corporate network. The bundle owner is Home-Gateway1 and the stack group peer, Home-Gateway2, is specified as a peer (10.10.1.2).

```
vpdn multihop
username stack password hellothere
multilink virtual-template 1

sgbp group stack
sgbp member Home-Gateway2 10.10.1.2

interface virtual-template 1
ip unnumbered e0
ppp multilink
ppp auth chap
```

The following example also shows how to configure the Cisco Multihop VPDN feature:

```
!  
vpdn enable  
vpdn multihop  
vpdn search-order domain  
!  
vpdn-group 1  
  request-dialin  
  protocol l2tp  
  domain cisco.com  
  initiate-to ip 172.22.53.144 priority 1  
  initiate-to ip 172.22.53.145 priority 1  
!  
l2tp tunnel password 7 <deleted>  
!
```

Related Commands

Command	Description
vpdn enable	Enables VPDN networking on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
vpdn-group	Associates a VPDN group to a customer or VPDN profile.
vpdn search-order	Specifies how the service provider's network access server is to perform VPDN tunnel authorization searches.

vpdn outgoing

The **vpdn outgoing** command is replaced by the **request-dialin** command. See the description of the [request-dialin](#) command for more information.

vpdn profile

To associate a virtual private dialup network (VPDN) profile with a customer profile, use the **vpdn profile** command in customer profile configuration mode. To remove a VPDN profile from a customer profile, use the **no** form of this command.

vpdn profile *name*

no vpdn profile *name*

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

Defaults	No default behavior or values.
----------	--------------------------------

Command Modes	Customer profile 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 **vpdn profile** command to associate a VPDN profile with a customer profile.

VPDN profiles can be used to combine session counting over multiple VPDN groups. This ability can be applied to customer profiles by configuring multiple VPDN groups under a VPDN profile, then associating the VPDN profile with the customer profile using the **vpdn profile** command.

Examples

The following example shows how to create two VPDN groups, configure the VPDN groups under a VPDN profile named profile1, then associates 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	Command	Description
	resource-pool profile customer	Creates a customer profile.
	resource-pool profile vpdn	Creates a VPDN profile and enters VPDN profile configuration mode.
	vpdn group	Associates a VPDN group with a customer or VPDN profile.
	vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

vpdn search-order

To specify how a network access server (NAS) or tunnel switch is to perform virtual private dialup network (VPDN) tunnel authorization searches, use the **vpdn search-order** command in global configuration mode. To restore the default search order, use the **no** form of this command.

vpdn search-order {[dnis] [domain] [multihop-hostname]}

no vpdn search-order

Syntax Description

dnis	Searches on the Dialed Number Information Service (DNIS) information.
domain	Searches on the domain name.
multihop-hostname	Searches on the hostname or tunnel ID of the ingress tunnel for a multihop tunnel switch.

Command Default

When this command is not enabled, the default is to search first on the DNIS information provided on ISDN lines, and then search on the domain name. This is equivalent to issuing the **vpdn search-order dnis domain** command.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(13)T	Support was added for the multihop-hostname option.

Usage Guidelines

To issue the **vpdn search-order** command, you must include at least one of the search parameter keywords. You may enter multiple keywords, and they can be entered in any order. The order of the keywords specifies the order of precedence given to the search parameters. If you do not issue a particular keyword, no search will be performed on that parameter.

Issue the **multihop-hostname** keyword only on a device configured as a multihop tunnel switch.

The configuration shows the **vpdn search-order** command setting only if the command is explicitly configured.

Examples

The following example configures a NAS to perform tunnel authorization searches based on DNIS information only:

```
vpdn search-order dnis
```

The following example configures a tunnel switch to select a tunnel destination based on the multihop hostname first, then on the domain name, and finally on the DNIS number:

```
vpdn search-order multihop-hostname domain dnis
```

Related Commands

Command	Description
multihop-hostname	Enables the tunnel switch to initiate a tunnel based on the hostname or tunnel ID of the ingress tunnel.

vpdn session-limit

To limit the number of simultaneous VPN sessions that can be established on a router, use the **vpdn session-limit** command in global configuration mode. To allow an unlimited number of simultaneous VPN sessions, use the **no** form of this command.

vpdn session-limit *sessions*

no vpdn session-limit

Syntax Description	<i>sessions</i>	Maximum number of simultaneous VPN sessions that are allowed on a router.
--------------------	-----------------	---

Defaults	Disabled
----------	----------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.0(6)T	This command was introduced.

Usage Guidelines	When this command is enabled, use the show vpdn history failure command to view records of refused attempts to establish new sessions.
------------------	---

Examples	The following example first sets a limit of two simultaneous VPN sessions on the router and then shows a Syslog message stating that an attempt to establish a new session was refused:
----------	---

```
Router(config)# vpdn session-limit 2
Router(config)#
00:11:17:%VPDN-6-MAX_SESS_EXCD:L2F HGW great_went exceeded configured local session-limit
and rejected user wilson@soam.com
Router(config)#
```

Related Commands	Command	Description
	show vpdn history failure	Displays the content of the failure history table.
	vpdn softshut	Prevents new sessions from being established on a VPN tunnel without disturbing existing sessions.

vpdn softshut

To prevent new sessions from being established on a VPN tunnel without disturbing existing sessions, use the **vpdn softshut** command in global configuration mode. To return the VPN tunnel to active service, use the **no** form of this command.

vpdn softshut

no vpdn softshut

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

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

Usage Guidelines

When this feature is enabled on a NAS, the potential session will be authorized before it is refused. This authorization ensures that accurate accounting records can be kept.

When this feature is enabled on a home gateway, the reason for the session refusal will be returned to the NAS. This information is recorded in the VPN history failure table.

When this command is enabled, use the **show vpdn history failure** command to view records of refused attempts to establish new sessions.

Examples The following example first enables the **vpdn softshut** command and then shows a Syslog message stating that an attempt to establish a new session was refused:

```
Router(config)# vpdn softshut
Router(config)#
00:11:17:%VPDN-6-SOFTSHUT:L2F HGW great_went has turned on softshut and rejected user
wilson@soam.com
Router(config)#
```

Related Commands	Command	Description
	show vpdn history failure	Displays the content of the failure history table.
	vpdn session-limit	Limits the number of simultaneous VPN sessions that can be established on a router.

vpdn source-ip

To globally specify an IP address that is different from the physical IP address used to open a virtual private dialup network (VPDN) tunnel, use the **vpdn source-ip** command in global configuration mode. To disable use of the alternate IP address, use the **no** form of this command.

vpdn source-ip *ip-address*

no vpdn source-ip *ip-address*

Syntax Description

ip-address Alternate IP address.

Command Default

No alternate IP address is specified.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Use the **vpdn source-ip** command to specify a single alternate IP address to be used for all tunnels on the device. A single source IP address can be configured globally per device.

Use the **source-ip** command in VPDN group configuration mode to configure an alternate IP address to be used for only those tunnels associated with that VPDN group.

The VPDN group-level configuration will override the global configuration.

Examples

This example sets a source IP address of 172.24.48.3:

```
vpdn source-ip 172.24.48.3
```

Related Commands

Command	Description
source-ip	Specifies an IP address that is different from the physical IP address used to open a VPDN tunnel for the tunnels associated with a VPDN group.
vpdn enable	Enables VPDN on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server, if one is present.

vpdn-group

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

vpdn-group *name*

no vpdn-group *name*

Syntax Description

name Name of the VPDN group.

Defaults

No VPDN groups are defined.

Command Modes

Global 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

Issuing the **vpdn-group** command creates a VPDN group with the specified name and enters VPDN group configuration mode. If a VPDN group with the specified name already exists, issuing the **vpdn-group** command will enter VPDN group configuration mode and allow configuration of that VPDN group.

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

Examples

The following example creates the VPDN group named l2tp and enters VPDN group configuration mode:

```
Router(config)# vpdn-group l2tp
Router(config-vpdn)#
```

The following example associates the VPDN group created in the preceding example with the VPDN profile named profile1:

```
Router(config)# resource-pool profile vpdn profile1
Router(config-vpdn-profile)# vpdn group l2tp
```

The following example creates a VPDN group named l2f and associates it with the customer profile named customer1:

```
Router(config)# vpdn-group l2f
!
Router(config)# resource-pool profile customer customer1
Router(config-customer-profile)# vpdn group l2f
```

Related Commands	Command	Description
	resource-pool profile customer	Creates a customer profile and enters customer profile configuration mode.
	resource-pool profile vpdn	Creates a VPDN profile and enters VPDN profile configuration mode.
	vpdn group	Associates a VPDN group with a customer or VPDN profile.

vty-async

To configure all virtual terminal lines on a router to support asynchronous protocol features, use the **vty-async** command in global configuration mode. To disable asynchronous protocol features on virtual terminal lines, use the **no** form of this command.

vty-async

no vty-async

Syntax Description

This command has no arguments or keywords.

Defaults

By default, asynchronous protocol features are not enabled on virtual terminal lines.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The **vty-async** command extends asynchronous protocol features from physical asynchronous interfaces to virtual terminal lines. Normally, SLIP and PPP can function only on asynchronous interfaces, not on virtual terminal lines. However, extending asynchronous functionality to virtual terminal lines permits you to run SLIP and PPP on these *virtual asynchronous interfaces*. One practical benefit is the ability to tunnel SLIP and PPP over X.25 PAD, thus extending remote node capability into the X.25 area. You can also tunnel SLIP and PPP over Telnet or LAT on virtual terminal lines. To tunnel SLIP and PPP over X.25, LAT, or Telnet, you use the protocol translation feature in the Cisco IOS software.

To tunnel SLIP or PPP inside X.25, LAT, or Telnet, you can use two-step protocol translation or one-step protocol translation, as follows:

- If you are tunneling SLIP or PPP using the two-step method, you need to first enter the **vty-async** command. Next, you perform two-step translation.
- If you are tunneling SLIP or PPP using the one-step method, you do not need to enter the **vty-async** command. You need to issue only the **translate** command with the SLIP or PPP keywords, because the **translate** command automatically enables asynchronous protocol features on virtual terminal lines.

Examples

The following example enables asynchronous protocol features on virtual terminal lines:

```
vty-async
```

Related Commands

Command	Description
ppp	Starts an asynchronous connection using PPP.
slip	Starts a serial connection to a remote host using SLIP.
translate	Enables asynchronous protocol features on virtual terminal lines.

vty-async dynamic-routing

To enable dynamic routing on all virtual asynchronous interfaces, use the **vty-async dynamic-routing** command in global configuration mode. To disable asynchronous protocol features on virtual terminal lines, and therefore disable routing on virtual terminal lines, use the **no** form of this command.

vty-async dynamic-routing

no vty-async dynamic-routing

Syntax Description

This command has no arguments or keywords.

Defaults

Dynamic routing is not enabled on virtual asynchronous interfaces.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This feature enables IP routing on virtual asynchronous interfaces. When you issue this command and a user later makes a connection to another host using SLIP or PPP, the user must specify **/routing** on the SLIP or PPP command line.

If you had not previously entered the **vty-async** command, the **vty-async dynamic-routing** command creates virtual asynchronous interfaces, and then enables dynamic routing on them.

Examples

The following example enables dynamic routing on virtual asynchronous interfaces:

```
vty-async dynamic-routing
```

Related Commands

Command	Description
async dynamic routing	Enables manually configured routing on an asynchronous interface.
vty-async	Enables manually configured routing on an asynchronous interface.

vty-async header-compression

To compress the headers of all TCP packets on virtual asynchronous interfaces, use the **vty-async header-compression** command in global configuration mode. To disable virtual asynchronous interfaces and header compression, use the **no** form of this command.

vty-async header-compression [passive]

no vty-async header-compression

Syntax Description

passive (Optional) Outgoing packets are compressed only when TCP incoming packets on the same virtual asynchronous interface are compressed. For SLIP, if you do not specify this option, the Cisco IOS software will compress all traffic. The default is no compression. For PPP, the Cisco IOS software always negotiates header compression.

Defaults

Header compression is not enabled on virtual asynchronous interfaces.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This feature compresses the headers on TCP/IP packets on virtual asynchronous connections to reduce the size of the packets and to increase performance. This feature only compresses the TCP header, so it has no effect on UDP packets or other protocol headers. The TCP header compression technique, described fully in RFC 1144, is supported on virtual asynchronous interfaces using SLIP or PPP encapsulation. You must enable compression on both ends of a connection.

Examples

The following example compresses outgoing TCP packets on virtual asynchronous interfaces only if incoming TCP packets are compressed:

```
vty-async header-compression passive
```

Related Commands

Command	Description
async dynamic routing	Enables manually configured routing on an asynchronous interface.

vty-async ipx ppp-client loopback

To enable IPX-PPP on virtual terminal lines, use the **vty-async ipx ppp-client loopback** command in global configuration mode. To disable IPX-PPP sessions on virtual terminal lines, use the **no** form of this command.

vty-async ipx ppp-client loopback *number*

no vty-async ipx ppp-client loopback

Syntax Description	<i>number</i>	Number of the loopback interface configured for IPX to which the virtual terminal lines are assigned.
--------------------	---------------	---

Defaults	IPX over PPP is not enabled on virtual terminal lines.
----------	--

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	11.0	This command was introduced.

Usage Guidelines	<p>This command enables users to log into the router from a device running a virtual terminal protocol, then issue the PPP command at the EXEC prompt to connect to a remote device.</p> <p>A loopback interface must already have been defined and an IPX network number must have been assigned to the loopback interface before the vty-async ipx ppp-client loopback command will permit IPX-PPP on virtual terminal lines.</p>
------------------	--

Examples	The following example enables IPX over PPP on virtual terminal lines:
----------	---

```
ipx routing ramana
interface loopback0
 ipx network 12345
vty-async ipx ppp-client loopback0
```

Related Commands	Command	Description
	interface loopback	Creates a loopback interface.
	ipx network	Enables IPX routing on a particular interface and optionally selects the type of encapsulation (framing).

vty-async keepalive

To change the frequency of keepalive packets on all virtual asynchronous interfaces, use the **vty-async keepalive** command in global configuration mode. To disable asynchronous protocol features on virtual terminal lines, use the **no vty-async keepalive** command. To disable keepalive packets on virtual terminal lines, use the **vty-async keepalive 0** command.

vty-async keepalive *seconds*

no vty-async keepalive

vty-async keepalive 0

Syntax Description

seconds Frequency, in seconds, with which the Cisco IOS software sends keepalive messages to the other end of a virtual asynchronous interface. To disable keepalive packets, use a value of 0. The active keepalive interval range is 1 to 32,767 seconds. Keepalive is disabled by default.

Defaults

Keepalive is disabled.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Use this command to change the frequency of keepalive updates on virtual asynchronous interfaces, or to disable keepalive updates. To determine if keepalive is enabled on an interface, use the **show running-config EXEC** command. If the router has not received a keepalive packet after three update intervals have passed, the connection is considered down.

Examples

The following example sets the keepalive interval to 30 seconds:

```
vty-async keepalive 30
```

The following example sets the keepalive interval to 0 (off):

```
vty-async keepalive 0
```

Related Commands

Command	Description
keepalive	Sets the keepalive timer for a specific interface.

vty-async mtu

To set the maximum transmission unit (MTU) size on virtual asynchronous interfaces, use the **vty-async mtu** command in global configuration mode. To disable asynchronous protocol features on virtual terminal lines, use the **no** form of this command.

vty-async mtu *bytes*

no vty-async

Syntax Description	<i>bytes</i>	MTU size of IP packets that the virtual asynchronous interface can support. The default MTU is 1500 bytes, the minimum MTU is 64 bytes, and the maximum is 1,000,000 bytes.
---------------------------	--------------	---

Defaults	1500 bytes
-----------------	------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines

Use this command to modify the MTU for packets on a virtual asynchronous interfaces. You might want to change to a smaller MTU size for IP packets transmitted on a virtual terminal line configured for asynchronous functions for any of the following reasons:

- The SLIP or PPP application at the other end only supports packets up to a certain size.
- You want to ensure a shorter delay by using smaller packets.
- The host echoing takes longer than 0.2 seconds.

Do not change the MTU size unless the SLIP or PPP implementation running on the host at the other end of the virtual asynchronous interface supports reassembly of IP fragments. Because each fragment occupies a spot in the output queue, it might also be necessary to increase the size of the SLIP or PPP hold queue if your MTU size is such that you might have a high amount of packet fragments in the output queue.

Examples

The following example sets the MTU for IP packets to 256 bytes:

```
vty-async mtu 256
```

Related Commands	Command	Description
	mtu	Adjusts the maximum packet size or MTU size.

vty-async ppp authentication

To enable PPP authentication on virtual asynchronous interfaces, use the **vty-async ppp authentication** command in global configuration mode. To disable PPP authentication, use the **no** form of this command.

vty-async ppp authentication {chap | pap}

no vty-async ppp authentication {chap | pap}

Syntax Description

chap	Enables CHAP on all virtual asynchronous interfaces.
pap	Enables PAP on all virtual asynchronous interfaces.

Defaults

No CHAP or PAP authentication for PPP.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command configures the virtual asynchronous interface to either authenticate CHAP or PAP while running PPP. After you have enabled CHAP or PAP, the local router requires a password from remote devices. If the remote device does not support CHAP or PAP, no traffic will be passed to that device.

Examples

The following example enables CHAP authentication for PPP sessions on virtual asynchronous interfaces:

```
vty-async ppp authentication chap
```

Related Commands

Command	Description
ppp bap call	Sets PPP BACP call parameters.
ppp use-tacacs	Enables TACACS for PPP authentication.
vty-async	Configures all virtual terminal lines on a router to support asynchronous protocol features.
vty-async ppp use-tacacs	Enables TACACS authentication for PPP on virtual asynchronous interfaces.

vty-async ppp use-tacacs

To enable TACACS authentication for PPP on virtual asynchronous interfaces, use the **vty-async ppp use-tacacs** command in global configuration mode. To disable TACACS authentication on virtual asynchronous interfaces, use the **no** form of this command.

vty-async ppp use-tacacs

no vty-async ppp use-tacacs

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

Defaults	TACACS for PPP is disabled.
-----------------	-----------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines	<p>This command requires the extended TACACS server.</p> <p>After you have enabled TACACS, the local router requires a password from remote devices.</p> <p>This feature is useful when integrating TACACS with other authentication systems that require a clear-text version of a user's password. Such systems include one-time password systems and token card systems.</p> <p>If the username and password are contained in the CHAP password, the CHAP secret is not used by the router. Because most PPP clients require that a secret be specified, you can use any arbitrary string; Cisco IOS software ignores it.</p> <p>You cannot enable TACACS authentication for SLIP on asynchronous or virtual asynchronous interfaces.</p>
-------------------------	--

Examples	<p>The example enables TACACS authentication for PPP sessions:</p> <pre>vty-async ppp use-tacacs</pre>
-----------------	--

Related Commands	Command	Description
	ppp use-tacacs	Enables TACACS for PPP authentication.
	vty-async ppp authentication	Enables PPP authentication on virtual asynchronous interfaces.

vty-async virtual-template

To configure virtual terminal lines to support asynchronous protocol functions based on the definition of a virtual interface template, use the **vty-async virtual-template** command in global configuration mode. To disable virtual interface templates for asynchronous functions on virtual terminal lines, use the **no** form of this command.

```
vty-async virtual-template number

no vty-async virtual-template
```

Syntax Description	<i>number</i>	Virtual interface number.
--------------------	---------------	---------------------------

Defaults	Asynchronous protocol features are not enabled by default on virtual terminal lines.
----------	--

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	10.3	The vty-async command was introduced.
	11.3	The vty-async virtual-template command was introduced.

The **vty-async virtual-template** command enables you to support tunneling of SLIP or PPP across X.25, TCP, or LAT networks by using two-step protocol translation.

Before issuing the **vty-async virtual-template** command, create and configure a virtual interface template by using the **interface virtual-template** command. Configure this virtual interface as a regular asynchronous serial interface. That is, assign the virtual interface template the IP address of the Ethernet interface, and configure addressing, just as on an asynchronous interface. You can also enter commands in interface configuration mode that compress TCP headers or configure CHAP authentication for PPP.

After creating a virtual interface template, apply it by issuing the **vty-async virtual-template** command. When a user dials in through a virtual terminal line, the router creates a virtual access interface, which is a temporary interface that supports the asynchronous protocol configuration specified in the virtual interface template. This virtual access interface is created dynamically, and is freed up as soon as the connection drops.

Before virtual templates were implemented, you could use the **vty-async** command to extend asynchronous protocol functions from physical asynchronous interfaces to virtual terminal lines. However, in doing so, you created a virtual asynchronous interface, rather than the virtual access interface. The difference is that the virtual asynchronous interfaces are allocated permanently, whereas the virtual access interfaces are created dynamically when a user calls in and closed down when the connection drops.

You can have up to 25 virtual templates interfaces, but you can apply only one template to vty-async interfaces on a router. There can be up to 300 virtual access interfaces on a router.

Examples

The following example enables asynchronous protocol features on virtual terminal lines:

```
vty-async
vty-async virtual-template 1
vty-async dynamic-routing
vty-async header-compression
!
interface virtual-template1
 ip unnumbered Ethernet0
 encapsulation ppp
 no peer default ip address
 ppp authentication chap
```

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
ppp	Starts an asynchronous connection using PPP.
slip	Starts a serial connection to a remote host using SLIP.
translate lat	Translates a LAT connection request automatically to another outgoing protocol connection.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection.
translate x25	Translates an X.25 connection request automatically to another outgoing protocol connection.

x25 aodi

To enable the Always On/Dynamic ISDN (AO/DI) client on an interface, use the **x25 aodi** command in interface configuration mode. To remove AO/DI client functionality, use the **no** form of this command.

x25 aodi

no x25 aodi

Syntax Description This command has no arguments or keywords.

Defaults AO/DI client is not enabled.

Command Modes Interface configuration

Command History	Release	Modification
	11.3 T	This command was introduced.

Usage Guidelines Use this command to enable the AO/DI client on an interface.

Examples The following example enables the AO/DI client on the interface running X.25, using the **x25 aodi** command:

```
interface bri0
  isdn x25 dchannel
  isdn x25 static-tei 8
interface bri0:0
  x25 aodi
  x25 address 12135551234
  x25 htc 4
  x25 win 3
  x25 wout 3
  x25 map ppp 12135556789 interface dialer 1
```



Note

Configuring the BRI interface with the **isdn x25 dchannel** command creates a configurable interface (bri 0:0) for other necessary X.25 commands. Refer to the description for this command earlier in this publication for additional information about this command.

x25 map ppp

To enable a PPP session over the X.25 protocol, use the **x25 map ppp** command in interface configuration mode. To remove a prior mapping, use the **no** form of this command.

x25 map ppp *x121-address* **interface** *cloning-interface* [**no-outgoing**]

no x25 map ppp *x121-address* **interface** *cloning-interface* [**no-outgoing**]

Syntax Description

<i>x121-address</i>	X.121 address as follows: <ul style="list-style-type: none">• Client side—The calling number.• Server side—The called number.
interface <i>cloning-interface</i>	Interface to be used for cloning the configuration.
no-outgoing	(Optional) Ensures that the X.25 map does not originate calls.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use **x25 map ppp** command to allow a PPP session to run over X.25.

The **interface** keyword refers to the interface that will be used to clone the configuration.



Note

For the **x25 map** command used in standard X.25 implementations, refer to the *Cisco IOS Wide-Area Networking Command Reference* publication.

Examples

Client Examples

The following example enables the AO/DI client on the interface and configures the D channel (BRI interface 0:0) with the x25 map statement in order to allow PPP sessions over X.25 encapsulation with the configured AO/DI server:

```
interface BRI0:0
  x25 address 16193368208
  x25 aodi
  x25 htc 4
  x25 win 3
  x25 wout 3
  x25 map ppp 16193368209 interface dialer 1
```

Server Examples

The following example enables the AO/DI server to receive calls from the AO/DI client and configures the D channel (BRI0:0) with the x25 map statement which allows PPP sessions over X.25 encapsulation with the configured AO/DI client. The **no-outgoing** option is used with the x.25 map command since the AO/DI server is receiving, versus initiating, calls.

```
interface BRI0:0
x25 address 16193368209
x25 htc 4
x25 win 3
x25 wout 3
x25 map ppp 16193368208 interface dialer 1 no-outgoing
```



Note

Configuring the BRI interface with the **isdn x25 dchannel** command creates a configurable interface (bri 0:0).
