



## Commands for the Cisco 6400 NRP

---

This chapter describes the commands specific to the Cisco 6400 node route processor (NRP) except **show** commands, which are described in [Chapter 2, “Show Commands for the Cisco 6400 NRP”](#)

Additional commands used to configure the NRP are described in the Cisco IOS command reference publications, available on Cisco.com or on the Documentation CD-ROM.

Tasks are presented only in the context of using a particular command; this chapter does not describe how the tasks interrelate, nor does it provide comprehensive configuration examples.

# accept dialin

To specify the virtual template to use for cloning new virtual-access interfaces when an incoming tunnel connection is requested from a specific peer, use the **accept dialin** VPDN group command. To disable authentication and virtual template cloning, use the **no** form of this command.

**accept dialin** [**l2f** | **l2tp** | **any** | **pppoe**] **virtual-template** *number* [**remote** *remote-peer-name*]

**no accept dialin** [**l2f** | **l2tp** | **any** | **pppoe**] **virtual-template** *number* [**remote** *remote-peer-name*]

## Syntax Descriptions

<b>l2f</b>   <b>l2tp</b>   <b>any</b>   <b>pppoe</b>	(Optional) Indicates which protocol to use for a dial-in tunnel.  <b>l2f</b> —Layer 2 Forwarding protocol. <b>l2tp</b> —Layer 2 Tunnel Protocol. <b>any</b> —VPDN will use autodetect to select either L2F or L2TP. Does not apply to PPPoE. <b>pppoe</b> —Point-to-Point Protocol over Ethernet.
<b>virtual-template</b> <i>number</i>	The virtual template interface from which the new virtual-access interface is cloned.
<b>remote</b> <i>remote-peer-name</i>	(Optional) Case-sensitive name that the remote peer will use for identification and tunnel authentication. Does not apply to PPPoE.

## Syntax Description

Disabled

## Command Modes

VPDN group mode

## Command History

Release	Modification
10.0	This command was introduced.
11.3(3)T	The <b>log</b> keyword was added.
12.0(1)T	This command was modified.
12.0(3)DC	The <b>pppoe</b> keyword was added on the Cisco 6400 NRP.

## Usage Guidelines

This command replaces the **vpdn incoming** command used in Cisco IOS Release 11.3. The user interface will automatically be upgraded when you reload the router with a 12.0 T image.

When used with L2F or L2TP, the router replies to a dial-in Layer 2 tunnel open request from the specified peer. When the access server accepts the request, the router uses the specified virtual template to clone new virtual-access interfaces.



### Note

The Cisco 6400 does not support L2F.

When used with PPPoE, the **accept dialin** command enables the router to accept incoming PPPoE discovery packets from clients and establish PPPoE sessions with them. After the PPPoE discovery stage is completed, PPPoE uses the specified virtual template to clone new virtual-access interfaces. If a pre-cloned virtual-access interface is available in PPPoE private list, PPPoE uses that virtual-access interface to establish a PPP session with the client.

**Note**

Configure the **vpdn-group** command with the **accept dialin** or **request dialin** command.

**Examples**

This example shows how to allow an access server to accept a PPPoE dial-in tunnel. A virtual-access interface will be cloned from virtual-template 1:

```
accept dialin pppoe virtual-template 1
```

If you use the **accept dialin** command with the **pppoe** and **virtual-template** keywords and omit the **remote-peer-name** argument, you automatically enable a default PPPoE VPDN group, which allows all tunnels to share the same tunnel attributes:

```
vpdn-group 1
! Default PPPoE VPDN group
accept dialin pppoe virtual-template 1
```

**Related Commands**

Command	Description
<b>vpdn incoming</b>	Specifies the local name to use for authenticating, and the virtual template to use for building interfaces for incoming connections.

# atm route-bridge

To configure an interface to use ATM routed bridging, use the **atm route-bridge** interface configuration command.

**atm route-bridge** *protocol*

Syntax Description	<i>protocol</i>	Protocol to be route-bridged.
--------------------	-----------------	-------------------------------

**Defaults** No default behavior or values.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.0(5)DC	This command was introduced on the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

**Examples** This example shows how to configure ATM routed bridging on an interface:


```
Router(config)# interface atm 4/0.100 point-to-point
Router(config-if)# ip address 172.69.5.9 255.255.255.0
Router(config-if)# pvc 0/32
Router(config-if)# atm route-bridged ip
```

## atm vc tx

To set the PVC segmentation buffer size, use the **atm vc tx** interface configuration command. To revert to the default value of 32, use the **no** form of this command.

**atm vc tx** *queue-depth*

**no atm vc tx** *queue-depth*

<b>Syntax Description</b>	<i>queue-depth</i>	Maximum number of packets in the buffer queue. Possible values: 32, 64, 128, 256.
<b>Defaults</b>	32	
<b>Command Modes</b>	ATM VC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(1)DC1	This command was introduced on the Cisco 6400 NRP.
	12.2(4)B	The service internal requirement was removed.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.
<b>Usage Guidelines</b>	For each PVC, a segmentation buffer slot is reserved for high-priority packets.	
 <b>Caution</b>	Entering the <b>atm vc tx</b> command can cause service disruption. Only enter this command during maintenance windows.	
<b>Examples</b>	This example shows how to set the maximum number of packets in the segmentation buffer of each PVC to 64:	
	<pre>! interface atm 0/0/0 →  atm vc tx 64 !</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>interface atm</b>	Configures an ATM interface type and enters interface configuration mode.

# attribute

To configure an attribute in a local service profile, use the **attribute** profile configuration command. Use the **no** form of this command to delete an attribute from a service profile.

**attribute** *radius-attribute-id* [*vendor-id*] [*cisco-vsa-type*] *attribute-value*

**no attribute** *radius-attribute-id* [*vendor-id*] [*cisco-vsa-type*] *attribute-value*

Syntax Description		
<i>radius-attribute-id</i>		RADIUS attribute ID to be configured.
<i>vendor-id</i>		(Optional) Vendor ID. Required if the RADIUS attribute ID is 26, indicating a vendor-specific attribute. Cisco's vendor ID is 9.
<i>cisco-vsa-type</i>		(Optional) Cisco vendor-specific attribute (VSA) type. Required if the vendor ID is 9, indicating a Cisco VSA.
<i>attribute-value</i>		Attribute value.

**Defaults** No default behavior or values.

**Command Modes** Profile configuration

Command History	Release	Modification
	12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

**Usage Guidelines** Use this command to configure attributes in local service profiles.

For the SSG Open Garden feature, use this command to configure the Service Route, DNS Server Address, and Domain Name attributes in a local service profile before adding the service to the open garden.

**Examples** In the following example, the Cisco-AVpair Upstream Access Control List (inacl) attribute is configured in the local service profile called cisco.com:

```
Router(config)# local-profile cisco.com
Router(config-prof)# attribute 26 9 1 "ip:inacl#101=deny tcp 10.2.1.0 0.0.0.255 any eq 21"
```

In the following example, the Session-Timeout attribute is deleted from the local service profile called cisco.com:

```
Router(config)# local-profile cisco.com
Router(config-prof)# no attribute 27 600
```

In the following example, an open garden service called “opencisco.com” is defined.

```

Router(config)# local-profile opencisco.com
Router(config-prof)# attribute 26 9 251 "Oopengarden1.com"
Router(config-prof)# attribute 26 9 251 "D10.13.1.5"
Router(config-prof)# attribute 26 9 251 "R10.1.1.0;255.255.255.0"
Router(config-prof)# exit
Router(config)# ssg open-garden opencisco.com

```

Related Commands	Command	Description
	<b>local-profile</b>	Configures a local service profile.
	<b>show ssg open-garden</b>	Displays a list of all configured open garden services.
	<b>ssg open-garden</b>	Designates a service, defined in a local service profile, to be an open garden service.

## debug pmbox

To display debug messages for traffic flowing on the NRP-2 PAM mailbox serial interface, use the **debug pmbox** EXEC command. The **no** form of this command disables debugging output.

```
debug pmbox {events | {rx-path | tx-path} {all | config-download | config-update | diag | driver
| ehsa | force-fail | image-download | info-request | nrp | ping | status-update | syslog | test1
| test2 | xc-request | xc-response}}
```

```
no debug pmbox {events | {rx-path | tx-path} {all | config-download | config-update | diag |
driver | ehsa | force-fail | image-download | info-request | nrp | ping | status-update | syslog
| test1 | test2 | xc-request | xc-response}}
```

### Syntax Description

<b>events</b>	Displays PAM mailbox messaging events. Traces routine execution as message are moved from one CPU to another.
<b>rx-path</b>	Selects messages received by the PAM mailbox serial interface from the NSP.
<b>tx-path</b>	Selects messages transmitted by the PAM mailbox serial interface to the NSP.
<b>all</b>	Displays all messages.
<b>config-download</b>	Displays configuration download messages.
<b>config-update</b>	Displays configuration update messages.
<b>diag</b>	Displays diagnostic messages.
<b>driver</b>	Displays driver messages.
<b>ehsa</b>	Displays enhanced high system availability (EHSA) messages.
<b>force-fail</b>	Displays force failover messages.
<b>image-download</b>	Displays image download messages.
<b>info-request</b>	Displays information request messages.
<b>nrp</b>	Displays NRP messages.
<b>ping</b>	Displays ping messages.
<b>status-update</b>	Displays status update messages.
<b>syslog</b>	Displays PAM mailbox system log messages.
<b>test1</b>	Displays test1 messages.
<b>test2</b>	Displays test2 messages.
<b>xc-request</b>	Displays cross connect request messages.
<b>xc-response</b>	Displays cross connect response messages.

### Defaults

No default behavior or values.

### Command History

Release	Modification
12.1(4)DC	This command was introduced on the Cisco 6400 NRP-2.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.



---

**Examples**

This example shows how image download messages are received and transmitted by the PAM mailbox serial interface of the NRP-2 in slot 5. Notice that the request messages are 24 bytes long and the response messages are 12288 bytes long.

```
Switch# debug pmbox rx-path tx-path image-download
```

```
Switch#  
RX(5/0) type:IMAGE DNLD, len = 24  
TX(5/0) type:IMAGE DNLD, len = 12288  
RX(5/0) type:IMAGE DNLD, len = 24  
TX(5/0) type:IMAGE DNLD, len = 12288  
RX(5/0) type:IMAGE DNLD, len = 24  
TX(5/0) type:IMAGE DNLD, len = 12288
```

# debug se64

To display debug messages for the NRP-2 ATM SAR, use the **debug se64** EXEC command. The **no** form of this command disables debugging output.

**debug se64 {detail | errors}**

**no debug se64 {detail | errors}**

Syntax Description	detail	errors
	Enables the <b>show controllers atm 0/0/0</b> privileged EXEC command to display internal ATM SAR data and register values.	Displays run time SAR driver error information.

**Defaults** No default behavior or values.

Command History	Release	Modification
	12.1(4)DC	This command was introduced on the Cisco 6400 NRP-2.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

**Examples** This debug output example shows that the SAR was not ready to transmit packets:

NRP-2# **debug se64 errors**

```
NRP-2#
01:39:05:%SYS-5-CONFIG_I:Configured from console by console
01:39:15:%NRP2_SE64-3-LLD_SNDPAK_SARNOTREADY:SAR not ready during packet TX:
vcd 2644
-Traceback= 60124A88 601CFF28 6012D878 602EFBCC 802C7EAC
01:39:45:%NRP2_SE64-3-LLD_SNDPAK_SARNOTREADY:SAR not ready during packet TX:
vcd 2249
-Traceback= 60124A88 601CFF28 6012D878 602EFBCC 802C7EAC
01:40:15:%NRP2_SE64-3-LLD_SNDPAK_SARNOTREADY:SAR not ready during packet TX:
vcd 3810
```

Related Commands	Command	Description
	<a href="#">show controllers atm 0/0/0</a>	Displays information on the physical ATM interface.

# debug vpdn pppoe-data

To display the contents of PPPoE session data packets, use the **debug vpdn pppoe-data** privileged EXEC command. Use the **no** form of the command to disable debugging output.

**[no] debug vpdn pppoe-data**

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

**Defaults** Disabled

Command History	Release	Modification
	12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

**Examples** The following type of output appears when a PPPoE data packet is transmitted by the router:

```
Jun 13 11:33:49.407: PPPoE: OUT
contiguous pak, size 14
FF 03 C0 21 02 0D 00 0A 05 06 1E 17 75 59
```

Related Commands	Command	Description
	<a href="#">debug vpdn pppoe-errors</a>	Displays PPPoE protocol and code errors.
	<a href="#">debug vpdn pppoe-events</a>	Displays PPPoE session events and incoming and outgoing active discovery packets.
	<a href="#">debug vpdn pppoe-packets</a>	Displays contents of PPPoE active discovery packets.

# debug vpdn pppoe-errors

To display PPPoE protocol and code errors, use the **debug vpdn pppoe-errors** privileged EXEC command. Use the no form of the command to disable debugging output.

**[no] debug vpdn pppoe-errors**

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

**Defaults** Disabled

Command History	Release	Modification
	12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

**Examples** This example shows output from a PPPoE encounter with a MAC addressing error:

```
Jun 13 11:33:49.407: PPPoE: Bad MAC address: 1111.2222.3333
```

Related Commands	Command	Description
	<a href="#">debug vpdn pppoe-data</a>	Displays the contents of PPPoE session data packets.
	<a href="#">debug vpdn pppoe-events</a>	Displays PPPoE session events and incoming and outgoing active discovery packets.
	<a href="#">debug vpdn pppoe-packets</a>	Displays contents of PPPoE active discovery packets.

# debug vpdn pppoe-events

To display PPPoE session events and incoming and outgoing active discovery packets, use the **debug vpdn pppoe-events** privileged EXEC command. Use the no form of the command to disable debugging output.

**[no] debug vpdn pppoe-events**

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

**Defaults** Disabled

Command History	Release	Modification
	12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

**Examples** The following display shows output when PPPoE established a virtual private networking session.  
Jun 13 11:33:49.407: PPPOE: VPN session created.

Related Commands	Command	Description
	<a href="#">debug vpdn pppoe-data</a>	Displays the contents of PPPoE session data packets.
	<a href="#">debug vpdn pppoe-errors</a>	Displays PPPoE protocol and code errors.
	<a href="#">debug vpdn pppoe-packets</a>	Displays contents of PPPoE active discovery packets.

# debug vpdn pppoe-packets

To display contents of PPPoE active discovery packets, use the **debug vpdn pppoe-packets** privileged EXEC command. Use the no form of the command to disable debugging output.

**[no] debug vpdn pppoe-packets**

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

**Defaults** Disabled

Command History	Release	Modification
	12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

**Examples** This example shows output from a PPPoE encounter with an active discovery packet.

```
Jun 13 11:33:49.407: PPPoE: discovery packet
contiguous pak, size 74
00 04 09 00 AA AA 03 00 80 C2 00 07 00 00 00 00
22 22 33 33 00 50 73 27 5D C3 88 63 11 65 00 01
00 1C 01 01 00 00 01 02 00 0A 70 70 70 6F 65 00
.....
```

Related Commands	Command	Description
	<a href="#">debug vpdn pppoe-data</a>	Displays the contents of PPPoE session data packets.
	<a href="#">debug vpdn pppoe-errors</a>	Displays PPPoE protocol and code errors.
	<a href="#">debug vpdn pppoe-events</a>	Displays PPPoE session events and incoming and outgoing active discovery packets.

# encapsulation aal5autopp virtual-template

The PPP Autosense feature enables the NAS to distinguish between incoming PPPoA and PPPoE sessions and allocates resources on demand for both PPP types.

To enable PPP Autosense, use the **encapsulation aal5autopp virtual-template** ATM VC or VC class command. To disable PPP Autosense, use the **no** form of this command.

**encapsulation aal5autopp virtual-template** *template-number*

**no encapsulation aal5autopp virtual-template** *template-number*

<b>Syntax Description</b>	<i>template-number</i>	Number of the virtual template that will be used to clone virtual-access interfaces for PPPoA sessions.
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	ATM VC or VC class	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.
<b>Usage Guidelines</b>	This command functions only when the PPPoA sessions are LLC encapsulated. Do not use this command on a router that initiates PPPoA sessions.	
<b>Examples</b>	This example shows how to enable PPP Autosense for virtual-template 1: encapsulation aal5autopp virtual-template 1	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">virtual-template pre-clone</a>	Specifies the number of virtual access interfaces to be created and cloned from a specific virtual template.

# initiate-to

To specify the IP address that will be tunneled to, use the **initiate-to** VPDN group command. To remove an IP address from the VPDN group, use the **no** form of this command.

**initiate-to ip** *ip-address* [**limit** *limit-number*] [**priority** *priority-number*]

**no initiate-to** [**ip** *ip-address*]

Syntax Description		
<b>ip</b> <i>ip-address</i>	IP address of the router that will be tunneled to.	
<b>limit</b> <i>limit-number</i>	(Optional) Maximum number of sessions in each tunnel to the IP address.	
<b>priority</b> <i>priority-number</i>	(Optional) Priority for the IP address (1 is the highest).	

Defaults	
	Disabled.
	Unlimited number of sessions per tunnel.

Command Modes	
	VPDN Group Mode

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.1(1) DC1	This command was modified for the Cisco 6400 NRP. The command option “ <b>limit</b> <i>limit-number</i> ” was extended for use without RPM, and its syntax description was modified. Sessions are now limited per tunnel instead of limited per IP address.

Usage Guidelines	
	Before you can use this command, you must enable one of the two request VPDN subgroups by using either the <b>request dialin</b> or <b>request dialout</b> command.
	A LAC configured to request dial-in can be configured with multiple <b>initiate-to</b> commands to tunnel to more than one IP address.
	An LNS configured to request dialout can only be configured with a single <b>initiate-to</b> command. If you enter a second <b>initiate-to</b> command, it will replace the original <b>initiate-to</b> command.
	At least one <b>initiate-to</b> command must be configured for the VPDN group initiator services ( <b>request-dialin</b> and <b>request-dialout</b> ) to function.



---

**Examples**

This example shows how to configure VPDN group 1 to request up to three L2TP tunnels to the LNS. This group can tunnel a maximum of 40 sessions per tunnel.

```
!  
vpdn-group 1  
request-dialin  
  protocol l2tp  
  domain net.com  
initiate-to ip 10.1.1.1 limit 40  
initiate-to ip 10.2.2.2 limit 40  
initiate-to ip 10.2.2.2 limit 40  
!
```

---

**Related Commands**

Command	Description
<b>request-dialin</b>	Enables a router to request L2TP tunnels for dial-in.
<b>request-dialout</b>	Enables a router to request L2TP tunnels for dialout calls.

# ip local pool

To configure a local IP address pool group, use the **ip local pool** configuration command with the group name. To disband the group, use the **no** form of this command.

```
ip local pool pool-name start-IP [end-IP] [group group-name] [cache-size size]
```

```
no ip local pool
```

## Syntax Description

<i>pool-name</i>	User-defined name for the local address pool.
<i>start-IP</i>	IP address defining the start of the group.
<i>end-IP</i>	IP address defining the end of the contiguous addresses in the group.
<b>group</b>	Define a group containing this pool.
<i>group-name</i>	User-defined name for the pool group.
<b>cache-size</b>	Specify the size of the cache.
<i>size</i>	Size of the cache.

## Defaults

Any pool created without the optional **group** keyword is a member of the base system group.

## Command Modes

Global configuration

## Command History

Release	Modification
11.0	This command was introduced.
11.3AA	This command was enhanced to allow address ranges to be added and removed.
12.0	This command was migrated to Release 12.0.
12.1(5)DC	This command was modified for the Cisco 6400 NRP for the IP Overlapping Address Pools feature.

## Usage Guidelines

All pool names must be unique. Use of a duplicate name simply extends that pool.

Specifying a (named) pool within a group allows their IP addresses to overlap those of pools in other groups and pools in the “base system” pool. However, (named) pool IP addresses cannot overlap within the same group. Belonging to a group does not otherwise affect processing of pools. This means that you can use (named) pools anywhere you can use pools.

Addresses are returned to the pool from which they were allocated.

**Examples**

This example shows the configuration of two pool groups, including pools in the base system group.

```
ip local pool p1_g1 10.1.1.1 10.1.1.50 group grp1
ip local pool p2_g1 10.1.1.100 10.1.1.110 group grp1
ip local pool p1_g2 10.1.1.1 10.1.1.40 group grp2
ip local pool lp1 10.1.1.1 10.1.1.10
ip local pool p3_g1 10.1.2.1 10.1.2.30 group grp1
ip local pool p2_g2 10.1.1.50 10.1.1.70 group grp2
ip local pool lp2 10.1.2.1 10.1.2.10
```

This example specifies pool group “grp1” consisting of pools “p1\_g1”, “p2\_g1” and “p3\_g1”; pool group “grp2” consisting of pools “p1\_g2”, “p2\_g2”; and pools “lp1” and “lp2” which are members of the base system group. Note the overlap addresses: IP address 1.1.1.1 is in all of them (“grp1” group, “grp2” group and the base system group). Also note that there is no overlap within any group (including the base system group, which is unnamed).

This example shows pool names that provide an easy way to associate a pool name with a group (when the pool name stands alone). While this may be an operational convenience, there is no required relationship between the names used to define a pool and the name of the group.

**Related Commands**

Command	Description
<b>debug ip peer</b>	This command contains additional output when pool groups are defined.

# I2tp tunnel receive-window

To set the local control channel receive window size (RWS), use the **I2tp tunnel receive-window** VPDN group command.

**I2tp tunnel receive-window** *packets*

<b>Syntax Description</b>	<i>packets</i>	Specifies size, in packets, of local RWS.
<b>Defaults</b>	The default local RWS is platform dependent. For the Cisco 6400 NRP, the local RWS is 3000 packets.	
<b>Command Modes</b>	VPDN group mode	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(7) DC	This command was introduced on the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.
<b>Usage Guidelines</b>	The local RWS determines the number of L2TP control packets that can be queued by the system for processing, and the new default local RWS is considerably larger than the value outlined in RFC 2661. While a large RWS enables the system to open PPP sessions more quickly, a small RWS is useful on networks that cannot handle large bursts of traffic.	
<b>Examples</b>	This example shows how to set the local RWS to 500 packets: I2tp tunnel receive-window 500	

# I2tp tunnel retransmit

To set the control channel retransmission parameters, use the **l2tp tunnel retransmit** VPDN group command. To disable a parameter setting, use the **no** form of this command.

**l2tp tunnel retransmit** [retries *value* | [timeout [min | max] *seconds*]]

**no l2tp tunnel retransmit** [retries *value* | [timeout [min | max] *seconds*]]

## Syntax Description

<b>retries</b>	Retransmission attempts.
<i>value</i>	Specifies number of retransmission attempts.
<b>timeout</b>	Length of time between retransmission attempts.
<b>min</b>	Sets the minimum timeout.
<b>max</b>	Sets the maximum timeout, up to 8 seconds.
<i>seconds</i>	Specifies timeout length, in seconds.

## Defaults

10 retries.  
1-second timeout minimum.  
8-second timeout maximum.

## Command Modes

VPDN group mode

## Command History

Release	Modification
12.0(7) DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

## Usage Guidelines

Control channel retransmissions follow an exponential backoff, starting at the minimum retransmit timeout length, and ending at the maximum retransmit timeout length (up to 8 seconds). For example, if the minimum timeout length is set to 1 second, the next retransmission attempt occurs 2 seconds later. The following attempt occurs 4 seconds later, and all additional attempts occur in 8-second intervals.

## Examples

This example shows how to configure 8 retransmission attempts, with the minimum timeout length set at 2 seconds and the maximum timeout length set at 4 seconds:

```
l2tp tunnel retransmit retries 8
l2tp tunnel retransmit timeout min 2
l2tp tunnel retransmit timeout max 4
```

# lcp max-load-metric

To limit load metric, use the **lcp max-load-metric** global configuration command. To disable this limit, use the **no** form of the command.

**lcp max-load-metric** *number*

**no lcp max-load-metric**

<b>Syntax Description</b>	<i>number</i>	Maximum load metric based on the length of the PPP manager process input queue.
---------------------------	---------------	---

<b>Defaults</b>	Unlimited
-----------------	-----------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

<b>Usage Guidelines</b>	The nominal limit depends on many factors. Try several numbers and select the one that results in the shortest session recovery time after a link dropout.
-------------------------	--

<b>Examples</b>	This example shows how to limit the load metric to 100: lcp max-load-metric 100
-----------------	--

# lcp max-session-starts

To limit the number of simultaneous link control protocol (LCP) session initiations, use the **lcp max-session-starts** global configuration command. To disable this limit, use the **no** form of the command.

**lcp max-session-starts** *number*

**no lcp max-session-starts**

Syntax Description	<i>number</i>	Maximum number of simultaneous LCP session initiations.
--------------------	---------------	---

Defaults	Unlimited number of simultaneous LCP sessions initiations
----------	---

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

Command History	Release	Modification
	12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines	<p>Range of possible values: 100 to 3000.</p> <p>The nominal limit depends on many factors. Try several numbers and select the one that results in the shortest session recovery time after a link dropout.</p>
------------------	---

Examples	<p>This example shows how to limit the number of simultaneous LCP session initiations to 100:</p> <pre>lcp max-session-starts 100</pre>
----------	---

# local-profile

To configure a local service profile and enter profile configuration mode, use the **local-profile** global configuration command. Use the **no** form of this command to delete the local service profile.

**local-profile** *profile-name*

**no local-profile** *profile-name*

<b>Syntax Description</b>	<i>profile-name</i>	Name of profile to be configured.
---------------------------	---------------------	-----------------------------------

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.	
12.3	This command was integrated into Cisco IOS Release 12.3.	

<b>Usage Guidelines</b>	Use this command to configure local service profiles.
-------------------------	---

<b>Examples</b>	The following example shows how to configure a RADIUS profile called cisco.com and enter profile configuration mode:
-----------------	--

```
Router(config)# local-profile cisco.com
Router(config-prof)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>attribute</b>	Configures attributes in local RADIUS profiles.
	<b>ssg service-search-order</b>	Specifies the order in which NRP-SSG searches for a service profile.
	<b>show ssg open-garden</b>	Displays a list of all configured open garden services.
	<b>ssg open-garden</b>	Designates a service, defined in a local service profile, to be an open garden service.



# multihop hostname

To enable the L2TP tunnel switch to initiate a tunnel based on the LAC host name or ingress tunnel ID, use the **multihop hostname** VPDN request-dialin group configuration mode command. To disable this option, use the **no** form of this command.

**multihop hostname** *ingress-tunnel-name*

**no multihop hostname** *ingress-tunnel-name*

<b>Syntax Description</b>	<i>ingress-tunnel-name</i> LAC hostname or ingress tunnel ID.
---------------------------	---

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	VPDN request-dialin group
----------------------	---------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.	
12.3	This command was integrated into Cisco IOS Release 12.3.	

**Examples** This example shows how to enable the L2TP tunnel switch to forward sessions from LAC-1 through an outgoing tunnel to IP address 10.3.3.3:

```
!
vpdn-group 11
 request-dialin
  protocol l2tp
  multihop hostname LAC-1
  initiate-to ip 10.3.3.3
  local name Tunnel-Switch
!
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>domain</b> <i>domain-name</i>	Selects VPDN group for tunnel initiation based on domain name.
<b>dnis</b> <i>dnis-number</i>	Selects VPDN group for tunnel initiation based on DNIS.	

## ppp ipcp mask

To request or reject IPCP subnet mask negotiation, or to specify a secondary subnet mask to use in case the RADIUS user profile does not contain one, use the **ppp ipcp mask** interface configuration command. To return to the default behavior, use the **no** form of this command.

**ppp ipcp mask** {*subnet-mask* / **reject** | **request**}

**no ppp ipcp mask** [*subnet-mask* | **reject** | **request**]

### Syntax Description

<i>subnet-mask</i>	<i>a.b.c.d</i> —Subnet mask sent to requesting peer when the RADIUS user profile does not include the Framed-IP-netmask attribute.
<b>reject</b>	Rejects IPCP subnet mask negotiations.
<b>request</b>	Requests the subnet mask from the peer.

### Defaults

Responds to IPCP subnet mask requests, but does not initiate IPCP subnet mask negotiations.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.1(3) DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

### Usage Guidelines

Typically, the CPE is configured or hard coded to **request** the subnet mask information from the Cisco 6400 NRP.

If the subnet mask is not available from either the NRP configuration or the RADIUS user profile, the NRP rejects the CPE request as if the **ppp ipcp mask reject** command was configured on the NRP.

### Examples

In this example, the PPP sessions in PVC 1/43 are configured to support IPCP subnet negotiation. If the RADIUS user profile does not contain the Framed-IP-netmask attribute, the NRP returns 255.255.255.224 to the requesting CPE.

```
!
interface ATM 0/0/0.30 multipoint
 pvc 1/43
  encapsulation aal5cisco ppp Virtual-Template 2
!
!
interface Virtual-Template 2
 ip unnumbered FastEthernet 0/0/0
 no peer default ip address
 ppp authentication pap chap
 ppp ipcp mask 255.255.255.224
```

# ppp timeout authentication

To set the time to wait for a response from the remote peer before retransmitting a PAP authenticate request, CHAP challenge, or CHAP response, use the **ppp timeout authentication** interface configuration command. To return to the default timeout, use the **no** form of the command.

**ppp timeout authentication** *seconds*

**no ppp timeout authentication**

<b>Syntax Description</b>	<i>seconds</i>	0 - 255. Time between retransmissions.
---------------------------	----------------	--

<b>Defaults</b>	10 seconds
-----------------	------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.3	This command was introduced.
12.1(1)DC	This command was first supported on the Cisco 6400 NRP for session scalability enhancements.	
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.	

<b>Usage Guidelines</b>	The nominal value depends on many factors. Cisco recommends that you start with a PPP authentication timeout of 15 seconds. Try several values and select the one that results in the highest number of stable sessions.
-------------------------	--

<b>Examples</b>	This example shows how to set authentication timeout to 15 seconds:
-----------------	---

```

!
interface Virtual-Template1
no ip address
no logging event link-status
keepalive 200
no peer default ip address
ppp authentication chap
ppp timeout retry 15
→ ppp timeout authentication 15
!

```

## ppp timeout retry

To set the time the PPP state machine (for LCP and NCP) waits for a response from the remote peer before retransmitting a configuration request or connection termination request, use the **ppp timeout retry** interface configuration command. To return to the default timeout, use the **no** form of the command.

**ppp timeout retry** *seconds*

**no ppp timeout retry**

<b>Syntax Description</b>	<i>seconds</i>	1 - 255. Time between retransmissions.
---------------------------	----------------	--

<b>Defaults</b>	2 seconds
-----------------	-----------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.3	This command was introduced as <b>ppp restart-timer</b> .
12.2	This command was changed to <b>ppp timeout retry</b> .	
12.1(1)DC	This command was modified for the Cisco 6400 NRP with a default of 2 seconds.	
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.	

<b>Usage Guidelines</b>	The nominal value depends on many factors. Cisco recommends that you start with a PPP retry timeout of 15 seconds. Try several values and select the one that results in the highest number of stable sessions.
-------------------------	---

<b>Examples</b>	This example shows how to set the retry timeout to 15 seconds:
-----------------	--

```

!
interface Virtual-Template1
no ip address
no logging event link-status
keepalive 200
no peer default ip address
ppp authentication chap
ppp timeout retry 15
→ ppp timeout authentication 15
!

```

## pppoe limit max-sessions

To set the maximum number of PPP over Ethernet (PPPoE) sessions that are permitted on a router, and to set the PPPoE session count threshold at which an SNMP trap is generated, use the **pppoe limit max-sessions** command in virtual private dial-up network (VPDN) group configuration mode. To remove these settings, use the **no** form of this command.

**pppoe limit max-sessions** *number-of-sessions* [**threshold-sessions** *threshold-value*]

**no pppoe limit max-sessions**

Syntax Description		
<i>number-of-sessions</i>		Maximum number of PPPoE sessions that will be permitted on the router. The range is from 0 to the maximum number of interfaces on the router.
<b>threshold-sessions</b>	(Optional)	Sets the PPPoE session limit threshold at which an SNMP trap is generated.
<i>threshold-value</i>		Number of PPPoE sessions that will cause an SNMP trap to be generated. The range is from 0 to the maximum number of interfaces on the router.

### Defaults

There is no default *number-of-sessions*.

The default *threshold-value* is the configured *number-of-sessions*.

### Command Modes

VPDN group configuration

### Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(7)T	This command was modified to configure the PPPoE session limit threshold.
12.3	This command was integrated into Cisco IOS Release 12.3.

### Usage Guidelines

You must configure the **snmp-server enable traps pppoe** command in order for SNMP traps to be generated when the PPPoE session limit threshold is exceeded.

The following statements describe the different types of PPPoE session limits:

- The **pppoe limit max-sessions** command limits the total number of PPPoE sessions on the router, regardless of the type of medium the sessions are using.
- The **pppoe limit per-mac** command limits the number of PPPoE sessions that can be sourced from a single MAC address. This limit also applies to all PPPoE sessions on the router.
- The **pppoe limit per-vc** and **pppoe limit per-vlan** commands limit the number of PPPoE sessions on all PVCs or VLANs on the router. The **pppoe max-sessions** command limits the number of PPPoE sessions on a specific PVC or VLAN. Limits created for a specific PVC or VLAN using the **pppoe max-session** command take precedence over the global limits created with the **pppoe limit per-vc** and **pppoe limit per-vlan** commands.

**Examples**

The following example shows a limit of 100 PPPoE sessions configured for the router. An SNMP trap is generated when the number of PPPoE sessions on the router exceeds 90.

```
vpdn enable
!
vpdn-group 1
accept dialin
protocol pppoe
virtual-template 1
pppoe limit max-sessions 100 threshold-sessions 90
```

**Related Commands**

Command	Description
<a href="#">debug vpdn pppoe-errors</a>	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be closed.
<a href="#">pppoe limit per-mac</a>	Specifies the maximum number of PPPoE sessions to be sourced from a MAC address.
<a href="#">pppoe limit per-vc</a>	Specifies the maximum number of PPPoE sessions permitted on all VCs.
<a href="#">pppoe limit per-vlan</a>	Specifies the maximum number of PPPoE sessions permitted on a VLAN.
<a href="#">pppoe max-sessions</a>	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session count threshold at which an SNMP trap will be generated.
<a href="#">snmp-server enable traps pppoe</a>	Enables PPPoE session count SNMP notifications.

## pppoe limit per-mac

To limit the number of PPPoE sessions that can originate from a single MAC address, use the **pppoe limit per-mac** command.

**pppoe limit per-mac** *number*

Syntax Description	<i>number</i>	The maximum number of PPPoE sessions for a single MAC address.
--------------------	---------------	--

Defaults	100
----------	-----

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

Command History	Release	Modification
	12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

Examples	This example shows how to place a limit of 5 PPPoE sessions per MAC address: pppoe limit per-mac 5
----------	---

Related Commands	Command	Description
	<a href="#">pppoe limit per-vc</a>	Limits the number of PPPoE sessions that can be established on a VC.

## pppoe limit per-vc

To limit the number of PPPoE sessions that can be established on a VC, use the **pppoe limit per-vc** command.

**pppoe limit per-vc** *number*

Syntax Description	<i>number</i>	The maximum number of PPPoE sessions for a VC.
--------------------	---------------	--

Defaults	100
----------	-----

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

Command History	Release	Modification
	12.0(3)DC	This command was first introduced on the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

Examples	This example shows how to place a limit of 50 PPPoE sessions per VC: pppoe limit per-vc 50
----------	---

Related Commands	Command	Description
	<a href="#">pppoe limit per-mac</a>	Limits the number of PPPoE sessions that can be established on a single MAC address.



## pppoe max-sessions

To set the maximum number of PPP over Ethernet (PPPoE) sessions that will be permitted on an ATM permanent virtual circuit (PVC), PVC range, virtual circuit (VC) class, or VLAN, and to set the PPPoE session count threshold at which an SNMP trap will be generated, use the **pppoe max-sessions** command in the appropriate command mode. To remove this specification, use the **no** form of this command.

**pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *threshold-value*]

**no pppoe max-sessions**

Syntax Description		
	<i>number-of-sessions</i>	Maximum number of PPPoE sessions that are permitted.
	<b>threshold-sessions</b>	(Optional) Sets the PPPoE session limit threshold at which an SNMP trap is generated. This option is not available in Ethernet subinterface configuration mode.
	<i>threshold-value</i>	Number of PPPoE sessions that will cause an SNMP trap to be generated. This option is not available in Ethernet subinterface configuration mode.

### Defaults

The default *number-of-sessions* is 100.

The default *threshold-value* is the *number-of-sessions*.

### Command Modes

Ethernet subinterface  
Interface-ATM-VC configuration  
VC-class configuration  
ATM PVC range configuration  
PVC-in-range configuration

### Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(2)T	This command was modified to limit PPPoE sessions on ATM PVCs, PVC ranges, and VC classes.
12.2(7)T	This command was modified to configure the PPPoE session limit threshold.
12.3	This command was integrated into Cisco IOS Release 12.3.

### Usage Guidelines



#### Note

You can configure PPPoE session limit thresholds for PVCs, PVC ranges, and VC classes. You cannot configure PPPoE session limit thresholds for VLANs.

You must configure the **snmp-server enable traps pppoe** command in order for SNMP traps to be generated when the PPPoE session limit threshold is exceeded.

The following statements describe the different types of PPPoE session limits:

- The **pppoe limit max-sessions** command limits the total number of PPPoE sessions on the router, regardless of the type of medium the sessions are using.
- The **pppoe limit per-mac** command limits the number of PPPoE sessions that can be sourced from a single MAC address. This limit also applies to all PPPoE sessions on the router.
- The **pppoe limit per-vc** and **pppoe limit per-vlan** commands limit the number of PPPoE sessions on all PVCs or VLANs on the router. The **pppoe max-sessions** command limits the number of PPPoE sessions on a specific PVC or VLAN. Limits created for a specific PVC or VLAN using the **pppoe max-session** command take precedence over the global limits created with the **pppoe limit per-vc** and **pppoe limit per-vlan** commands.

PPPoE session limits created on an ATM PVC take precedence over limits created in a VC class or ATM PVC range.

PPPoE session limits created in an ATM PVC range take precedence over limits created in a VC class.

## Examples

### VLAN Example

The following example shows a maximum of 200 PPPoE sessions configured for an 802.1Q VLAN subinterface:

```
interface FastEthernet0/0.10
encapsulation dot1Q 10
pppoe enable
pppoe max-session 200
```

### ATM PVC Example

The following example shows a limit of 10 PPPoE sessions configured for the PVC. An SNMP trap will be generated when the number of PPPoE sessions on the router exceeds 8.

```
interface ATM1/0.102 multipoint
pvc 3/304
encapsulation aal5snap
protocol pppoe
pppoe max-sessions 10 threshold-sessions 8
```

### VC Class Example

The following example shows a limit of 20 PPPoE sessions and a session count threshold of 15 sessions configured for the VC class called “main”:

```
vc-class atm main
pppoe max-sessions 20 threshold-sessions 15
```

### ATM PVC Range Example

The following example shows a limit of 30 PPPoE sessions configured for the ATM PVC range called “range-1”. The session count threshold is also 30 sessions because when the *threshold-value* has not been explicitly configured, it defaults to the *number-of-sessions* value.

```
interface atm 6/0.110 multipoint
range range-1 pvc 100 4/199
encapsulation aal5snap
protocol ppp virtual-template 2
pppoe max-sessions 30
```

**Individual PVC Within a PVC Range Example**

The following example shows a limit of 10 PPPoE sessions configured for “pvc1”, which is part of the ATM PVC range called “range1”. The PPPoE session count threshold is also 10 sessions.

```
interface atm 6/0.110 multipoint
range range1 pvc 100 4/199
pvc-in-range pvc1 3/104
pppoe max-sessions 10
```

**Related Commands**

Command	Description
<a href="#">debug vpdn pppoe-errors</a>	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be closed.
<a href="#">pppoe limit max-sessions</a>	Sets the maximum number of PPP over Ethernet (PPPoE) sessions that will be permitted on a router, and sets the PPPoE session count threshold at which an SNMP trap will be generated.
<a href="#">pppoe limit per-mac</a>	Specifies the maximum number of PPPoE sessions to be sourced from a MAC address.
<a href="#">pppoe limit per-vc</a>	Specifies the maximum number of PPPoE sessions permitted on all VCs.
<a href="#">pppoe limit per-vlan</a>	Specifies the maximum number of PPPoE sessions permitted on a VLAN.
<a href="#">snmp-server enable traps pppoe</a>	Enables PPPoE session count SNMP notifications.

# protocol

Use the **protocol** command in the appropriate command mode to do one or more of the following tasks:

- Configure a static map for an ATM PVC, SVC, or VC class.
- Enable Inverse ARP or Inverse ARP broadcasts on an ATM PVC by either configuring Inverse ARP directly on the PVC or in a VC class (applies to IP and IPX protocols only).
- Configure PPP over Ethernet for an ATM PVC or VC class.
- Override the virtual-template configuration inherited from VC classes for all PPP over Ethernet encapsulations.

Use the **no** form of this command to remove a static map, disable Inverse ARP, or remove PPP over Ethernet encapsulation.

```
protocol protocol [protocol-address | inarp] [[no] broadcast] [virtual-template number]
```

```
no protocol protocol [protocol-address | inarp] [[no] broadcast] [virtual-template number]
```

Syntax Description	<i>protocol</i>	Choose one of the following keywords:
		<p><b>aarp</b>—AppleTalk ARP</p> <p><b>apollo</b>—Apollo domain</p> <p><b>appletalk</b>—AppleTalk</p> <p><b>arp</b>—IP ARP</p> <p><b>bridge</b>—bridging</p> <p><b>bstun</b>—block serial tunnel</p> <p><b>cdp</b>—Cisco Discovery Protocol</p> <p><b>clns</b>—ISO CLNS</p> <p><b>clns_es</b>—ISO CLNS end system</p> <p><b>clns_is</b>—ISO CLNS intermediate system</p> <p><b>cmns</b>—ISO CMNS</p> <p><b>compressedtcp</b>—Compressed TCP</p> <p><b>decnet</b>—DECnet</p> <p><b>decnet_node</b>—DECnet node</p> <p><b>decnet_prime_router</b>—DECnet prime router</p> <p><b>decnet_router-11</b>—DECnet router L1</p> <p><b>decnet_router-12</b>—DECnet router L2</p> <p><b>dls</b>—data link switching</p> <p><b>ip</b>—IP</p> <p><b>ipx</b>—Novell IPX</p> <p><b>llc2</b>—llc2</p> <p><b>pad</b>—PAD links</p> <p><b>ppp</b>—PPP over ATM LLC encapsulation</p> <p><b>pppoe</b>—PPP over Ethernet encapsulation</p> <p><b>qllc</b>—Qualified Logical Link Control protocol</p> <p><b>rsrb</b>—remote source-route bridging</p> <p><b>snapshot</b>—snapshot routing support</p> <p><b>stun</b>—serial tunnel</p> <p><b>vines</b>—Banyan VINES</p> <p><b>xns</b>—Xerox Network Systems protocol</p>
	<i>protocol-address</i>	Destination address that is being mapped to a PVC.
	<b>inarp</b>	(Only valid for IP and IPX protocols on PVCs) Use this keyword to enable Inverse ARP on an ATM PVC. If you specify a protocol-address instead of <b>inarp</b> , Inverse ARP is automatically disabled for that protocol.

<b>[no] broadcast</b>	(Optional) Broadcast indicates that this map entry is used when the corresponding protocol sends broadcast packets to the interface-. For example, IGRP updates. Pseudobroadcasting is supported. The broadcast keyword of the protocol command takes precedence if you previously configured the broadcast command on the ATM PVC or SVC.
<b>virtual-template</b> <i>number</i>	(Optional) Use these keywords and argument only when you specify pppoe encapsulation for the protocol argument. Specifies which virtual template number to use.

**Defaults**

Inverse ARP is enabled for IP and IPX if the protocol is running on the interface and no static map is configured.

**Command Modes**

Interface-ATM-VC configuration (for an ATM PVC or SVC)  
 VC-class configuration (for a VC class)

**Command History**

Release	Modification
11.3(3)T	This command was introduced.
12.0(3)DC	The <b>pppoe</b> keyword was added for the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

**Usage Guidelines**

If the protocol command is not explicitly configured on an ATM PVC or SVC, the VC inherits the following default configuration (listed in order of next highest precedence):

- Configuration of the protocol command in a VC class assigned to the PVC or SVC itself.
- Configuration of the protocol command in a VC class assigned to the PVCs or SVCs ATM subinterface.
- Configuration of the protocol command in a VC class assigned to the PVCs or SVCs ATM main interface.
- Global default: Inverse ARP is enabled for IP and IPX if the protocol is running on the interface and no static map is configured.

Although you can assign an explicit network layer address to a virtual-template interface, Cisco recommends that you consider two other procedures. One procedure is to use AAA to assign an address to the virtual-access interface created from the virtual template, instead of configuring any network-layer address on the virtual template. The other procedure is to use an unnumbered IP address on the virtual template.

It is currently not possible to disable a virtual-access on an individual basis. To achieve a similar effect, either delete the relevant RADIUS user entries or deconfigure the VC associated with the virtual-access.

---

**Examples**

This example shows how to create a static map on a VC. 192.68.34.237 is connected to the VC and ATM pseudobroadcasts are sent.

```
protocol ip 192.68.34.237 broadcast
```

This example shows how to enable Inverse ARP for IPX. ATM pseudobroadcasts are not sent.

```
protocol ipx inarp no broadcast
```

This example shows how to remove a static map from a VC and restore the default behavior for Inverse ARP (refer to the "Default" section described above):

```
no protocol ip 192.68.34.237
```

This example shows how to configure PPP over Ethernet for an ATM PVC:

```
interface atm 2/0.1 multipoint
pvc 0/60
encapsulation aal5snap
protocol pppoe
```

# radius-server attribute 4 nrp

To change the default-selected IP address, use the **radius-server attribute 4 nrp** global configuration command. To restore the default-selected IP address, use the **no** form of this command.

**radius-server attribute 4 nrp**

**no radius-server attribute 4 nrp**

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

**Defaults** The NSP IP address is sent in RADIUS attribute 4.

**Command Modes** Global configuration mode

Command History	Release	Modification
	12.1(5)DC	This command was introduced on the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

**Usage Guidelines** When using RADIUS attribute 4 and "format d" in a VPI/VCI configuration or in a SSG configuration, this command allows the default-selected IP address to be changed. This command can only be enabled if "format d" is already configured.

[Table 1-1](#) shows how RADIUS global configuration commands can be combined to select an IP address.

*Table 1-1 RADIUS Global Configuration Commands*

Global Configuration Commands			Selected IP Address
<b>ip radius source-interface</b> <int x>	<b>radius-server attribute nas-port</b> <b>format d</b>	<b>radius-server attribute 4 nrp</b>	
Enabled			NRP IP Address <sup>1</sup>
	Enabled		NSP IP Address
Enabled	Enabled		NSP IP Address
Enabled	Enabled	Enabled	NRP IP Address <sup>1</sup>
	Enabled	Enabled	NRP best-select IP Address <sup>2</sup>

1. NRP IP Address of <int x>

2. Automatic choice, 1st choice is loopback, etc.



---

**Examples**

This example selects the NRP IP address to be sent in RADIUS attribute 4.

```
Router(config)# ip radius source-interface FastEthernet0/0/0
Router(config)# radius-server attribute nas-port format d
Router(config)# radius-server attribute 4 nrp
```

# radius-server attribute 8 include in access-req

To send the IP address of a user to the RADIUS server in the access request, use the **radius-server attribute 8 include in access-req** global configuration command. To disable sending of the user IP address to the RADIUS server during authentication, use the **no** form of this command.

**radius-server attribute 8 include in access-req**

**no radius-server attribute 8 include in access-req**

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

**Defaults** This feature is disabled.

**Command Modes** Global configuration mode

Command History	Release	Modification
	12.1(3)AA	This command was introduced on the Cisco AS5200, Cisco AS5300, and Cisco AS5800.
	12.1(3)DC	This command was supported on the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

**Usage Guidelines** Using the **radius-server attribute 8 include in access-req** command makes it possible for a network access server (NAS) to provide the RADIUS server with a hint of the user IP address in advance of user authentication. An application can be run on the RADIUS server to use this hint and build a table (map) of user names and addresses. By using the mapping information, service applications can begin preparing user login information to have available upon successful user authentication.

When a network device dials in to a NAS that is configured for RADIUS authentication, the NAS begins the process of contacting the RADIUS server in preparation for user authentication. Typically, the IP address of the dial-in host is not communicated to the RADIUS server until after successful user authentication. Communicating the device IP address to the server in the RADIUS access request allows other applications to begin to take advantage of that information.

As the NAS sets up communication with the RADIUS server, the NAS assigns an IP address to the dial-in host from a pool of IP addresses configured at the specific interface. The NAS sends the IP address of the dial-in host to the RADIUS server as attribute 8. At that time, the NAS sends other user information, such as the user name, to the RADIUS server.

After the RADIUS server receives the user information from the NAS, it has two options:

- If the user profile on the RADIUS server already includes attribute 8, the RADIUS server can override the IP address sent by the NAS with the IP address defined as attribute 8 in the user profile. The address defined in the user profile is returned to the NAS.

- If the user profile does not include attribute 8, the RADIUS server can accept attribute 8 from the NAS.

The address returned by the RADIUS server is saved in memory on the NAS for the life of the session. If the NAS is configured for RADIUS accounting, the accounting start packet sent to the RADIUS server includes the same IP address as in attribute 8. All subsequent accounting packets, updates (if configured), and stop packets will also include the same IP address as in attribute 8.

**Note**

Configuring the NAS to send the host IP address in the RADIUS access request assumes that the login host is configured to request an IP address from the NAS server. It also assumes that the login host is configured to accept an IP address from the NAS. In addition, the NAS must be configured with a pool of network addresses at the interface supporting the login hosts.

**Examples**

This example shows a NAS configuration that sends the IP address of the dial-in host to the RADIUS server in the RADIUS access request. The NAS is configured for RADIUS authentication, authorization, and accounting (AAA). A pool of IP addresses (async1-pool) has been configured and applied at interface Async1.

```
aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
!
ip address-pool local
!
interface Async1
peer default ip address pool async1-pool
!
ip local pool async1-pool 10.165.200.225 10.165.200.229
!
radius-server host 10.31.71.146 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute 8 include-in-access-req
radius-server key radhost
```

# radius-server attribute nas-port format

To select the NAS port format used for RADIUS accounting features, use the **radius-server attribute nas-port format** global configuration command. To restore the default NAS port format, use the **no** form of this command.

**radius-server attribute nas-port format** *format*

**no radius-server attribute nas-port format** *format*

<b>Syntax Description</b>	<i>format</i>	Choose one of the following keywords: <b>a</b> —Standard NAS port format. <b>b</b> —Extended NAS port format. <b>c</b> —Shelf-slot NAS port format. <b>d</b> —ATM VC extended NAS port format.
---------------------------	---------------	--

<b>Defaults</b>	Standard NAS port format.
-----------------	---------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.3(7)T	This command was introduced.
	11.3(9)DB and 12.0(5)DC	The <b>d</b> format was added for the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

<b>Usage Guidelines</b>	This command replaces the deprecated <b>radius-server attribute nas-port extended</b> command.
-------------------------	--

The **radius-server attribute nas-port format** command configures RADIUS to change the size and format of the NAS port attribute field (RADIUS IETF Attribute 5).

- **Standard format (a)**—This 16-bit NAS port format indicates the type, port, and channel of the controlling interface. This is the default format used by Cisco IOS software.
- **Extended format (b)**—The standard NAS port attribute field is expanded to 32 bits. The upper 16 bits of the NAS port attribute display the type and number of the controlling interface; the lower 16 bits indicate the interface undergoing authentication.
- **Shelf-slot format (c)**—This 16-bit NAS port format supports expanded hardware models requiring shelf and slot entries.
- **ATM VC extended format (d)**—This NAS port format uses 32 bits to indicate the interface, VPI, and VCI of an incoming PPP session.

**Note**

The ATM VC extended NAS port format on the NRP applies only to VCs created or recreated after the command is entered. The format does not apply retroactively to VCs configured before the **radius-server attribute nas-port format d** command is entered.

**Examples**

This example shows how to select the ATM VC extended NAS port format used for RADIUS VC Logging:

```
radius-server attribute nas-port format d
```

**Related Commands**

Command	Purpose
<b>radius-server host non-standard</b>	Specifies a vendor-proprietary RADIUS server host.

## snmp-server enable traps pppoe

To enable PPPoE session count Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps pppoe** global configuration command. To disable PPPoE session count SNMP notifications, use the **no** form of this command.

**snmp-server enable traps pppoe**

**no snmp-server enable traps pppoe**

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

**Defaults** SNMP notifications are disabled by default.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(2)B	This command was introduced.
	12.2(7)T	This command was integrated into Cisco IOS Release 12.2(7)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

**Usage Guidelines** This command enables SNMP traps only. It does not support inform requests.

To configure the PPPoE session thresholds at which SNMP notifications will be sent, use the **pppoe limit max-sessions** or **pppoe max-sessions** commands.

For a complete description of this notification and additional MIB functions, see the CISCO-PPPOE-MIB.my file, available on Cisco.com at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

**Examples** The following example enables the router to send PPPoE session count SNMP notifications to the host at the address 10.64.131.20:

```
snmp-server community public RW
snmp-server enable traps pppoe
snmp-server host 10.64.131.20 version 2c public udp-port 1717
```

Related Commands	Command	Description
	<b>pppoe limit max-sessions</b>	Sets the maximum number of PPP over Ethernet (PPPoE) sessions that will be permitted on a router, and sets the PPPoE session count threshold at which an SNMP trap will be generated.
	<b>pppoe max-sessions</b>	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session count threshold at which an SNMP trap will be generated.
	<b>snmp-server host</b>	Specifies the recipient of an SNMP notification operation.
	<b>snmp-server trap-source</b>	Specifies the interface that an SNMP trap should originate from.

## snmp-server enable traps atm pvc extension

To enable the sending of extended ATM permanent virtual circuit (PVC) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps atm pvc extension** global configuration command. To disable extended ATM PVC-specific SNMP notifications, use the **no** form of this command.

**snmp-server enable traps atm pvc extension { up | down | oam failure loopback }**

**no snmp-server enable traps atm pvc extension { up | down | oam failure loopback }**

Syntax Description	up	down	oam failure loopback
	Enables ATM PVC UP traps, which are generated when a PVC changes from the DOWN to UP state.	Enables ATM PVC DOWN traps, which are generated when a PVC changes from the UP to DOWN state.	Enables ATM PVC OAM FAILURE traps, which are generated when OAM loopback fails.

**Defaults** SNMP notifications are disabled by default.  
The interval between successive traps is 30 seconds.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(4)T	This command was introduced for those platforms that support ATM PVC Management.
	12.3	This command was integrated into Cisco IOS Release 12.3.

**Usage Guidelines** You cannot use extended ATM PVC traps at the same time as the legacy ATM PVC trap. You must disable the legacy ATM PVC trap by using the **no snmp-server enable traps atm pvc** command before configuring extended ATM PVC traps.

When the ATM PVC OAM failure trap is enabled, the PVC remains in the UP state when OAM loopback fails so that the flow of data is still possible. If the ATM PVC OAM failure trap is not enabled, the PVC is placed in the DOWN state when OAM loopback fails.

OAM management must be enabled on the PVC by using the **oam-pvc manage** command before you can use ATM PVC traps.

Generation of PVC traps is dampened by the notification interval in order to prevent trap storms. No traps are sent until the interval lapses.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. ATM notifications are defined in the CISCO-IETF-ATM2-PVCTRAP-MIB.mib file, available from the Cisco FTP site:



<ftp://www.cisco.com/public/mibs/v2/>

ATM PVC traps are generated at the end of the notification interval. It is possible to generate all three types of ATM PVC traps (the ATM PVC DOWN trap, ATM PVC UP trap, and ATM PVC OAM failure trap) at the end of the same notification interval.

Use the **snmp-server enable traps atm pvc** command with the **snmp-server host** command.

Use the **snmp-server host** command to specify which hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

## Examples

The following example shows all three extended ATM PVC traps enabled on a router. If PVC 0/1 leaves the UP or DOWN state, or has an OAM loopback failure, host 172.16.61.90 receives the SNMP notifications:

```
! Configure SNMP support and an IP routing protocol on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.16.0.0
!
! Enable extended ATM PVC trap support and OAM management:
Router(config)# snmp-server enable traps atm pvc extension down
Router(config)# snmp-server enable traps atm pvc extension up
Router(config)# snmp-server enable traps atm pvc extension oam failure loopback
Router(config)# interface atm 1/0.1
Router(config-if)# pvc 0/1
Router(config-if-atm-vc)# oam-pvc manage
```

## Related Commands

Command	Description
<b>oam-pvc manage</b>	Enables end-to-end F5 Operation, Administration, and Maintenance (OAM) loopback cell generation and OAM management for an ATM PVC or VC class.
<b>show atm pvc</b>	Displays all ATM permanent virtual circuits (PVCs) and traffic information.
<b>snmp-server enable traps</b>	Enables all available SNMP notifications on your system.
<b>snmp-server enable traps atm pvc</b>	Enables the sending of legacy ATM PVC DOWN traps.
<b>snmp-server host</b>	Specifies the recipient of an SNMP notification operation.
<b>snmp-server trap-source</b>	Specifies the interface that an SNMP trap should originate from.

# tunnel share

To enable tunnel sharing for a VPDN group, use the **tunnel share** VPDN group command. To disable tunnel sharing, use the **no** form of this command.

**tunnel share**

**no tunnel share**

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

**Defaults** Disabled.

**Command Modes** VPDN group

Command History	Release	Modification
	12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

**Examples** This example shows all sessions that are locally authorized through VPDN group 1 being sent through the same tunnel to 10.1.1.1.

```
!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain net1.com
  domain net2.com
  initiate-to ip 10.1.1.1
→ tunnel share
!
```

Related Commands	Command	Description
	<b>vpdn-group</b>	Selects the VPDN group.
	<b>request-dialin</b>	Enables a router to request L2TP tunnels for dial-in.
	<b>initiate-to</b>	Specifies the IP address that calls are tunneled to.

# tx-ring-limit

To limit the number of particles that can be used on a transmission ring, use the **tx-ring-limit** ATM VC configuration command. To return to the default, use the **no** form of this command.

**tx-ring-limit** *ring-limit*

**no tx-ring-limit**

Syntax Description	<i>ring-limit</i>	Specifies the maximum number of allowable particles that can be placed on the transmission ring.
--------------------	-------------------	--

Defaults	2 particles on the Cisco 6400 NRP-2SV
----------	---------------------------------------

Command Modes	This command is supported in the following command modes, numbered according to hierarchy: <ol style="list-style-type: none"> <li>1. ATM VC</li> <li>2. PVC-in-range</li> <li>3. PVC range</li> <li>4. VC class</li> <li>5. ATM interface</li> </ol>
---------------	--

When you enter **tx-ring-limit** in a particular command mode, its value takes precedence over any value inherited from a command mode that is lower on the list.

Command History	Release	Modification
	12.0(7)XE1	This command was introduced.
	12.0(9)S	This command was integrated into Cisco IOS Release 12.0 S for the Cisco 7500/RSP series.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
	12.2(2)B	This command was modified for the Cisco 6400 NRP-2SV: <ul style="list-style-type: none"> <li>• New default of 2 particles</li> <li>• Added command to PVC range and PVC-in-range command modes</li> </ul>
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines	The <b>tx-ring-limit</b> command is not supported on the Cisco 6400 NRP-1. The entered transmission ring limit is limited to values from 3 to 6000 particles. On the Cisco 6400 NRP-2SV, the particle size is 2048 bytes.
------------------	---

### What is a Transmitting Ring?

The transmission ring, a hardware first-in, first-out (FIFO) queue on the NRP-2SV ATM port adapter, stores packets before they are segmented into cells for transmission. When the queue is full, the NRP-2SV stops sending packets to the transmission ring and stores the packets in the Cisco IOS software until the transmission ring is no longer congested.

### Choosing the Transmission Ring Limit

There is no ideal value for the transmission ring limit, so you must experiment to find the best value:

- A low transmission ring limit accelerates the traffic shaping performance in the IOS software and reduces latency for packets waiting to be segmented and transmitted. A lower transmission ring limit has a faster rate of dropped packets.
- A high transmission ring limit provides more buffering space and time for packets on that VC, but can cause performance problems for delay-sensitive traffic. A higher transmission ring limit has a slower rate of dropped packets.

### Examples

In the following example, a transmission ring limit of seven particles is configured on the main ATM interface:

```
!
interface atm 0/0/0
atm pvc 32 0 32 aal5snap 10000 8000 2000 tx-ring-limit 7
!
```

In the following example, a transmission ring limit of ten particles is configured directly on the PVC:

```
!
interface ATM0/0/0.1 point-to-point
pvc 2/200
tx-ring-limit 10
!
```

In the following example, a transmission ring limit of five particles is configured for the PVC range from 6/32 to 6/4032:

```
!
interface atm 0/0/0
range pvc 6/32 6/4032
tx-ring-limit 5
!
```

In the following example, a transmission ring limit of six particles is configured for PVC 4/33 in the range 4/32 to 4/128:

```
!
interface atm 0/0/0
range pvc 4/32 4/128
!
pvc-in-range 4/33
!
tx-ring-limit 6
!
```

In the following example, a transmission ring limit of five particles is configured for VC class pppoa-1:

```
!
vc-class atm pppoa-1
tx-ring-limit 5
!
```

Related Commands	Command	Description
	<b>show atm vc</b>	Displays information about ATM PVCs and SVCs.

## virtual-template pre-clone

To specify the number of virtual-access interfaces to be created and cloned from a specific virtual template, use the **virtual-template pre-clone** global configuration command.

**virtual-template** *template-number* **pre-clone** *number*

<b>Syntax Description</b>	<b>virtual-template</b> <i>template-number</i>	The virtual template interface from which the new virtual-access interfaces are created.
	<b>pre-clone</b> <i>number</i>	The number of virtual-access interfaces created.

**Defaults** None

**Command Modes** Global configuration

**Usage Guidelines** This command applies to PPPoE only.  
The number of pre-cloned virtual-access interfaces should be set to the number of expected PPPoE sessions.

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

**Examples** This example shows how to create 1200 pre-cloned virtual-access interfaces on virtual template 1:  
virtual-template 1 pre-clone 1200

# vpdn authorize domain

To enable domain preauthorization on a NAS, use the **vpdn authorize domain** global configuration command. To disable domain preauthorization, use the **no** form of this command.

**vpdn authorize domain**

**no vpdn authorize domain**

---

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

---

**Defaults** Domain preauthorization is disabled by default.

---

**Command Modes** Global configuration

---

Command History	Release	Modification
	12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

---

---

**Examples** This example shows how to enable domain preauthorization:  
vpdn authorize domain

## vpdn search-order

To specify how the service provider's network access server is to perform VPDN tunnel authorization searches, use the **vpdn search-order** global configuration command. To remove a prior specification, use the no form of the command.

**vpdn search-order {dnis domain multihop-hostname}**

**no vpdn search-order**

### Syntax Description

<b>multihop-hostname</b>	Specifies a search on LAC host name or ingress tunnel ID.
<b>domain</b>	Specifies a search on the domain name.
<b>dnis</b>	Specifies a search on the DNIS information.

### Defaults

The default vpdn search order is:

**vpdn search-order {dnis domain}**

If authorization based on the multihop hostname is required, you will have to explicitly configure it as follows:

**vpdn search-order {multihop-hostname dns domain}**

### Command Modes

Global configuration

### Command History

Release	Modification
11.3	This command was introduced.
12.1(1) DC1	The <b>multihop-hostname</b> keyword was added for the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

### Usage Guidelines

VPDN authorization searches are performed only as specified.

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

### Examples

This example shows how to configure an L2TP tunnel switch to perform each VPDN authorization search by the multihop-hostname, and if unsuccessful, search by the domain name.

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



## vpn service

To configure a static domain name, use the **vpn service** ATM VC or VC class configuration command. To remove a static domain name, use the **no** form of this command.

**vpn service** *domain-name*

**no vpn service** *domain-name*

Syntax Description	<i>domain-name</i>	Static domain name.
--------------------	--------------------	---------------------

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

Command Modes	ATM VC or VC class
---------------	--------------------

Command History	Release	Modification
	12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Examples	This example shows how to configure the static domain name of net.com: vpn service net.com
----------	---

