



Advanced Router Configuration

This chapter includes advanced configuration procedures.



Note

Every feature described is not necessarily supported on every router model. Where possible and applicable, these feature limitations will be listed.

If you prefer to use network scenarios to build a network, see [Chapter 2, “Network Scenarios.”](#) For basic router configuration topics, see [Chapter 3, “Basic Router Configuration.”](#)

This chapter contains the following sections:

- [Configuring PPP over Ethernet Support, page 4-2](#)
- [Configuring TCP Maximum Segment Size for PPPoE, page 4-4](#)
- [Configuring Low-Latency Queuing and Link Fragmentation and Interleaving, page 4-5](#)
- [Configuring Class-Based Traffic Shaping to Support Low Latency Queuing, page 4-7](#)
- [Configuring the Length of the PVC Transmit Ring, page 4-10](#)
- [Configuring DHCP Server Import, page 4-11](#)
- [Configuring IP Control Protocol Subnet Mask Delivery, page 4-15](#)
- [Configuring the Service Assurance Agent, page 4-21](#)
- [Configuring Secure Shell, page 4-21](#)
- [Configuring IP Named Access Lists, page 4-22](#)
- [Configuring International Phone Support, page 4-22](#)
- [Configuring Committed Access Rate, page 4-27](#)
- [Configuring VPN IPSec Support Through NAT, page 4-27](#)
- [Configuring VoAAL2 ATM Forum Profile 9 Support, page 4-29](#)
- [Configuring ATM OAM F5 Continuity Check Support, page 4-31](#)
- [Configuring RADIUS Support, page 4-36](#)
- [Configuring Cisco Easy VPN Client, page 4-36](#)
- [Configuring Dial-on-Demand Routing for PPPoE Client, page 4-38](#)
- [Configuring Weighted Fair Queuing, page 4-40](#)

- [Configuring DSL Commands, page 4-41](#)
- [Configuring FTP Client, page 4-45](#)

Each section includes a configuration example and verification steps, where available.

Configuring PPP over Ethernet Support

The following sections describe how to configure PPP over Ethernet support:

- [Configuring PPPoE Client Support](#)
- [Configuring TCP Maximum Segment Size for PPP over Ethernet](#)

Configuring PPPoE Client Support

PPPoE is supported on the following Cisco routers:

- Cisco 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, and Cisco 837
- Cisco 828
- Cisco 831
- Cisco SOHO 77, Cisco SOHO 77H, Cisco SOHO 78, Cisco SOHO 96, and Cisco SOHO 97

This feature supports the PPP over Ethernet (PPPoE) client on an ATM permanent virtual circuit (PVC). Only one PPPoE client on a single ATM PVC is supported.

A PPPoE session is initiated on the client side by the network described above. If the session has a timeout or is disconnected, the PPPoE client immediately attempts to reestablish the session.

Follow these steps to configure the router for PPPoE client support:

-
- Step 1** Configure the virtual private dialup network (VPDN) group number.
- Enter the **vpdn enable** command in global configuration mode.
 - Configure the VPDN group by entering the **vpdn group tag** command.
 - Specify the dialing direction by entering the **request-dialin** command in the VPDN group.
 - Specify the type of protocol in the VPDN group by entering the **protocol pppoe** command.
- Step 2** Configure the ATM interface with PPPoE support.
- Configure the ATM interface by entering the **interface atm 0** command.
 - Specify the ATM PVC by entering the **pvc number** command.
 - Configure the PPPoE client and specify the dialer interface to use for cloning by entering the **pppoe-client dial-pool-number number** command.
- Step 3** Configure the dialer interface by entering the **int dialer number** command.
- Configure the IP address as negotiated by entering the **ip address negotiated** command.
 - Configure authentication for your network by entering the **ppp authentication** protocol command. This step is optional.
 - Configure the dialer pool number by entering the **dialer pool number** command.

- d. Configure the dialer-group number by entering the **dialer-group** *number* command.
- e. Configure a dialer list corresponding to the dialer-group by entering the **dialer-list 1 protocol ip permit** command.

**Note**

Multiple PPPoE clients can run on a different PVCs, in which case, each client has to use a separate dialer interface and a separate dialer pool, and the PPP parameters need to be applied on the dialer interface.

If you enter the **clear vpdn tunnel pppoe** command with a PPPoE client session already established, the PPPoE client session terminates and the PPPoE client immediately tries to reestablish the session.

Configuration Example

The following example shows a configuration of a PPPoE client.

```

vpdn enable
vpdn-group 1
    request-dialin
    protocol pppoe

int atm0

pvc 1/100
    pppoe-client dial-pool-number 1

int dialer 1
ip address negotiated
ppp authentication chap
dialer pool 1
dialer-group 1

```

Configuring TCP Maximum Segment Size for PPP over Ethernet

If a Cisco router terminates the PPP over Ethernet (PPPoE) traffic, a computer connected to the Ethernet interface may have problems accessing websites. The solution is to manually reduce the maximum transmission unit (MTU) configured on the computer by constraining the TCP maximum segment size (MSS). Enter the following command on the router's Ethernet 0 interface:

ip tcp adjust-mss *mss*

where *mss* is 1452 or less.

Network address translation (NAT) must be configured for the **ip tcp adjust-mss** command to work.

This feature is not supported on Cisco SOHO 76 routers.

Configuration Example

The following example shows a configuration of a PPPoE client.

```

vpdn enable
no vpdn logging
!

```

```

vpdn-group 1
  request-dialin
  protocol pppoe
!
interface Ethernet0
  ip address 192.168.100.1 255.255.255.0
  ip tcp adjust-mss 1452
  ip nat inside
!
interface ATM0
  no ip address
  no atm ilmi-keepalive
  pvc 8/35
    pppoe-client dial-pool-number 1
!
dsl operating-mode auto
!
interface Dialer1
  ip address negotiated
  ip mtu 1492
  ip nat outside
  encapsulation ppp
  dialer pool 1
  dialer-group 1
  ppp authentication pap callin
  ppp pap sent-username sohodyn password 7 141B1309000528
!
ip nat inside source list 101 interface Dialer1 overload
ip route 0.0.0.0.0.0.0.0 Dialer1
access-list 101 permit ip 192.168.100.0.0.0.0.255 any

```

Configuring TCP Maximum Segment Size for PPPoE

The configuring TCP maximum segment size for PPP over Ethernet feature is supported on the following Cisco routers:

- Cisco 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, and Cisco 837
- Cisco SOHO 77, Cisco SOHO 77H, Cisco SOHO 78, Cisco 96, and Cisco SOHO 97
- Cisco 828

If a Cisco router terminates the PPPoE traffic, a computer connected to the Ethernet interface may have problems accessing websites. The solution is to manually reduce the maximum transmission unit (MTU) configured on the computer by constraining the TCP maximum segment size (MSS). Enter the following command on the router's Ethernet 0 interface:

```
ip tcp adjust-mss mss
```

where *mss* is 1452 or less.

Network address translation (NAT) must be configured in order for the **ip tcp adjust-mss** command to work.

Configuration Example

The following example shows a configuration of a PPPoE client.

```
vpdn enable
no vpdn logging
!
vpdn-group 1
 request-dialin
  protocol pppoe
!
interface Ethernet0
 ip address 192.168.100.1 255.255.255.0
 ip tcp adjust-mss 1452
 ip nat inside
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 8/35
  pppoe-client dial-pool-number 1
!
dsl operating-mode auto
!
interface Dialer1
 ip address negotiated
 ip mtu 1492
 ip nat outside
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication pap callin
 ppp pap sent-username sohodyn password 7 141B1309000528
!
 ip nat inside source list 101 interface Dialer1 overload
 ip route 0.0.0.0.0.0.0.0 Dialer1
 access-list 101 permit ip 192.168.100.0.0.0.0.255 any
```

Configuring Low-Latency Queuing and Link Fragmentation and Interleaving

Low-Latency Queuing (LLQ) provides a low-latency, strict-priority transmit queue for Voice over IP (VoIP) traffic. LLQ is supported on the following routers:

- Cisco 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, Cisco 831, and Cisco 837
- Cisco 828

Link Fragmentation and Interleaving (LFI) reduces voice traffic delay and jitter by fragmenting large data packets and interleaving voice packets within the data fragments.

Configuring LLQ

Follow these steps to configure the router for LLQ:

-
- Step 1** Ensure that the voice and data packets have different IP precedence values so that the router can differentiate between them. Normally, data packets should have an IP precedence of 0, and voice packets should have an IP precedence of 5. If the VoIP packets are generated from within the router, you may set the IP precedence to 5 for these packets by entering the **ip precedence number** command in dial-peer voice configuration mode as follows:
- Enter the global configuration **dial-peer voice 1 voip** command.
 - Enter the **ip precedence 5** command.
- Step 2** Create an access list and a class map for the voice packets.
- Create an access list by entering the **access-list 101 permit ip any any precedence 5** command.
 - Create a class map for the voice packets by entering **class-map match-all voice** command.
 - Link the class map to the access list by entering the **match access-group 101** command.
- Step 3** Create the LLQ for voice traffic.
- Create a policy map by entering the **policy-map mypolicy** command.
 - Define the class by entering the **class voice** command.
 - Assign the priority bandwidth to the voice traffic. The priority bandwidth assigned to the voice traffic depends on the codec used and the number of simultaneous calls that you allow. For example, a G.711 codec call consumes 200 kbps; therefore, to support one G.711 voice call you would enter a **priority 200** command.
- Step 4** Attach LLQ to the dialer interface.
- Enter the global configuration **interface dialer 1** command.
 - Create a service policy by entering the **service-policy out mypolicy** command.



Note

Attach the service policy to the dialer interface only when LFI is used. Else, the service policy must be attached under the PVC itself.

Configuring LFI

Follow these steps to configure the router for LFI.



Note

When you are configuring LFI, the data fragment size must be greater than the voice packet size; otherwise, the voice packets fragment and voice quality deteriorates.

- Step 1** Configure the dialer bandwidth. The dialer interface has a default bandwidth of 56 kbps, which may be less than the upstream bandwidth of your digital subscriber line (DSL) connection. You can find the upstream bandwidth of your DSL connection by entering the **show dsl interface atm0** command in

dialer interface configuration mode. If you have two or more permanent virtual circuits (PVCs) sharing the same DSL connection, the bandwidth configured for the dialer interface must be the same as the bandwidth allocated to its assigned PVC.

Step 2 Enable PPP multilink, and configure fragment delay and interleaving for the dialer interface.

- a. Enter the global configuration **interface dialer 1** command.
- b. Specify the dialer bandwidth by entering the **bandwidth 640** command. The bandwidth is specified in kilobits per second (kbps).
- c. Enter the **ppp multilink** command.
- d. Specify PPP multilink interleaving by entering the **ppp multilink interleave** command.
- e. Define the fragment delay by entering the **ppp multilink fragment-delay 10** command.
- f. Calculate the fragment size using the following formula:

fragment size = (bandwidth in kbps / 8) * fragment-delay in milliseconds (ms)

In this case, the fragment size = (640/8) * 10, resulting in a fragment size of 800. The fragment size is greater than the maximum voice packet size of 200, which is G.711 20 ms. A low fragment delay corresponds to a fragment size that may be smaller than the voice packet size, resulting in reduced voice quality.

Configuring Class-Based Traffic Shaping to Support Low Latency Queuing

Class-based traffic shaping (CBTS) is supported on the Cisco 831 router.

CBTS can be used to control the WAN interface traffic transmission speed to match the speed of the attached broadband modem or of the remote target interface. CBTS ensures that the traffic conforms to the policies configured for it, thereby eliminating topology bottlenecks with data-rate mismatches.

The **shape average kbps** and the **shape peak kbps** commands enable you to define traffic shaping for an interface.



Note

CBTS is supported on the Ethernet 1 interface.

Configuring CBTS for LLQ

Follow the steps below to configure CBTS, beginning in global configuration mode. This procedure shows how to create multiple traffic classes and associate them with policy maps, and then to associate the policy maps with a router interface.

Step 1 Define a traffic classification.

- a. Enter the **class-map map-name** command to define a traffic classification. For example, the name *voice* could be used to specify that this is a class map for voice traffic.

- b. Now in class configuration mode, enter the **match ip precedence 5** command to match all IP voice traffic with a precedence of 5. Cisco Architecture for Voice, Video and Integrated Data (AVVID) documentation specifies a precedence value of 5 for voice-over-IP traffic.
- c. Enter **exit** to leave class configuration mode.

Step 2 Define a policy map and associated classes for low-latency queuing.

- a. Enter the **policy-map map-name** command in global configuration mode to construct policies and to allocate different network resources for the defined traffic classes. The name *LLQ* could be used to specify that this is the policy map for LLQ.
- b. Now in policy-map mode, define a class to handle voice traffic by entering **class QOS-class-name**, using the class-map name you defined using the **class-map** command in [Step 1](#). This command places the router in QOS-class configuration mode.
- c. Enter **priority number**, where number is bandwidth in kilobits per second. A value of 300, as shown in the example configuration, provides enough bandwidth for two G.711 voice ports. Before setting a priority value, see the specification for the CODEC used for voice calls.
- d. Enter **exit** to return to policy-map configuration mode.
- e. Enter **class class-default** to use the default class for all traffic other than voice traffic. The name class-default is well known, and does not have to be predefined using the **class-map** command.
- f. Apply WFQ to non-voice traffic by entering the **fair-queue** command.
- g. Enter **exit** twice to return to global configuration mode.

Step 3 Define a traffic-shaping policy map.

- a. Enter **policy-map map-name** in global configuration mode. The name *shape* should be used to indicate this map defines overall traffic shaping that is compatible with the remote transmission rate bandwidth.
- b. Enter **class class-default** to associate the default class with this policy map.
- c. Set the transmission speed to be used after traffic shaping to match the speed of the broadband modem or remote interface by entering the **shape average kbps** command, where *kbps* is a value in kilobits per second.



Caution

The transmission speed entered must be less than or equal to the TX bandwidth of the DSL or cable modem to which the router is attached. Specifying a value greater than the modem's TX bandwidth will result in the modem's becoming congested, and the benefits of applying QOS might be lost.

- d. Enter **service-policy name** to associate the LLQ policy map with the traffic-shaping policy map. If the map name for the low-latency queue were *LLQ*, then *name* would be *LLQ*.
- e. Enter **exit** twice to return to global configuration mode.

Step 4 Apply these policies to the Ethernet 1 interface.

- a. Enter the **interface Ethernet 1** command.
- b. Apply the service policy to the Ethernet 1 interface by entering **service-policy output name**, where *name* matches the policy defined in the traffic-shaping policy map. If the traffic-shaping policy map name were *shape*, the service-policy name would also be *shape*.

Step 5 Enter **end** to leave router configuration mode.

Configuration Example

The following example shows how a Cisco router can be configured to connect to a broadband modem with limited bandwidth, while ensuring voice line quality. Two policy maps are configured:

- Policy map *LLQ*
- Policy map *shape*

Policy map *LLQ* ensures that voice traffic has a strict priority queue with bandwidth of up to 300 kbps. The policy map *shape* limits the total throughput to 2.2 MBps.

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password encryption
!
hostname 831-uut
!
ip subnet-zero
!
class-map match-all voice
  match ip precedence 5
!
!
policy-map LLQ
  class voice
    priority 300
  class class-default
    fair-queue
policy-map shape
  class class-default
    shape average 2250000
    service-policy LLQ
!
interface Ethernet0
  ip address 1.7.65.11 255.255.0.0
!
interface Ethernet1
  ip address 192.168.1.101 255.255.255.0
  service-policy output shape
!
ip classless
ip http server
ip pim bidir-enable
!
line con 0
  stopbits 1
line vty 0 4
  login
!
!
scheduler max-task-time 5000
end
!
```

Configuring the Length of the PVC Transmit Ring

The length of the PVC transmit ring can be configured on the following Cisco routers:

- Cisco 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, and Cisco 837
- Cisco 828
- Cisco SOHO 77, Cisco SOHO 77H, Cisco SOHO 78, Cisco SOHO 96, and Cisco SOHO 97

If both voice and data packets share the same PVC, it is important to reduce the PVC transmit (TX) ring size. This reduces the maximum number of data packets and fragments that can be in front of a voice packet in the hardware queue, thus reducing latency.

Follow these steps to reduce the PVC TX ring size:

-
- Step 1** Enter the global configuration **int atm 0** command.
- Step 2** Specify the PVC number by entering the **pvc 1/100** command.
- Step 3** Reduce the PVC TX ring size to 3 by entering the **tx-ring-limit 3** command.
-

Configuration Example

The following example combines LFI, LLQ, and the PVC TX ring configurations.

```
class-map match-all voice
match access-group 101
!
policy-map mypolicy
class voice
priority 200
class class-default
fair-queue
!
interface Ethernet0
ip address 70.0.0.1 255.255.255.0
no ip mroute-cache
!
interface ATM0
no ip address
bundle-enable
dsl operating-mode auto
!
interface ATM0.1 point-to-point
no ip mroute-cache
pvc 1/40
encapsulation aal5mux ppp dialer
dialer pool-member 1
tx-ring-limit 3
!
interface Dialer1
bandwidth 640
ip address 60.0.0.1 255.255.255.0
encapsulation ppp
dialer pool 1
service-policy output mypolicy
ppp multilink
```

```
ppp multilink fragment-delay 10
ppp multilink interleave
!
ip classless
no ip http server
!
access-list 101 permit ip any any precedence 5
!
voice-port 1
!
voice-port 2
!
voice-port 3
!
voice-port 4
dial-peer voice 110 pots
    destination-pattern 110555
    port 1
!
dial-peer voice 210 voip
    destination-pattern 210555
    session target ipv4:60.0.0.2
    codec g711ulaw
    ip precedence 5
```

Configuring DHCP Server Import

This feature is supported on the following Cisco routers:

- Cisco 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, and Cisco 837
- Cisco 828
- Cisco 831
- Cisco SOHO 77, Cisco SOHO 77H, Cisco SOHO 78, Cisco SOHO 91, Cisco SOHO 96, and Cisco SOHO 97

Before Cisco IOS Release 12.1(5), the only way to configure the DHCP options on the Cisco IOS DHCP server was through the command-line interface (CLI). However, you may not want to configure the same DHCP options on multiple DHCP servers if you can, instead, configure a remote master DHCP server located on the corporate backbone. In this case, all the local DHCP servers will have the same DHCP options as those configured on the remote DHCP server.

The Cisco IOS DHCP server has been enhanced to allow configuration information to be updated automatically by PPP. You can enable PPP to automatically configure the Domain Name System (DNS) server, the Windows Information Name Server (WINS), or the NetB Cisco IOS Name Service (NBNS), and the server IP address information within a Cisco IOS DHCP server pool.

Follow these steps to configure the Cisco router for DHCP server import:

-
- Step 1** Configure the asynchronous transfer mode (ATM) interface and the asymmetric digital subscriber line (ADSL) operating mode.
- Step 2** Create an ATM PVC for data traffic, enter virtual circuit configuration mode, and specify the virtual path identifier/virtual channel identifier (VPI /VCI) values, the encapsulation type, and the dial-pool member.

- Step 3** Create a dialer interface.
- Enter configuration mode for the dialer interface.
 - Specify the MTU size as 1492.
 - Assign *ip address negotiated* to the dialer interface.
 - Configure the dialer group number.
 - Configure PPP encapsulation and (if needed) Challenge Handshake Authentication Protocol (CHAP).
 - Configure IP negotiation of DNS and WINS requests.
- Step 4** Define an IP DHCP pool name.
- Configure the network and domain name (if needed) for the DHCP pool.
 - Enter the **import all** command.
- Step 5** Configure a dialer list and a static route for the dialer interface.
-

Configuration Examples

The following example shows configuration of the DHCP server import on the Cisco router:

```

router-820#show run
Building configuration...
Current configuration :1510 bytes
version 12.1
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router-820
logging rate-limit console 10 except errors
!
username 3620-4 password 0 lab
mmi polling-interval 60
mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip finger
no ip domain-lookup
!
ip dhcp pool 2
import all
network 192.150.2.0 255.255.255.0
domain-name devtest.com
default-router 192.150.2.100
lease 0 0 3
!
no ip dhcp-client network-discovery
vpdn enable
no vpdn logging
vpdn-group 1
request-dialin
protocol pppoe

```

```

call rsvp-sync
!
interface Ethernet0
ip address 192.150.2.100 255.255.255.0
ip nat inside
!
interface ATM0
no ip address
no atm ilmi-keepalive
pvc 0/16 ilmi
!
pvc 1/40
protocol pppoe
pppoe-client dial-pool-number 1
!
bundle-enable
dsl operating-mode auto
!
interface Dialer0
ip address negotiated
ip mtu 1492
ip nat outside
encapsulation ppp
dialer pool 1
dialer-group 1
ppp authentication chap
ppp ipcp dns request
ppp ipcp wins request
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer0
no ip http server
!
ip nat inside source list 101 interface Dialer0 overload
access-list 101 permit ip any any
dialer-list 1 protocol ip list 101
snmp-server manager
!
voice-port 1
voice-port 2
voice-port 3
voice-port 4
!
line con 0
transport input none
stopbits 1
line vty 0 4
scheduler max-task-time 5000
end

```

The following example shows DHCP proxy client configuration:

```

3620-4#show run
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3620-4
logging rate-limit console 10 except errors
!
username 820-uit1 password 0 lab
username 820-uit4 password 0 lab

```

```

memory-size iomem 10
ip subnet-zero
!
no ip finger
!
ip address-pool dhcp-proxy-client
ip dhcp-server 192.150.1.101
vpdn enable
no vpdn logging
!
vpdn-group 1
accept-dialin
protocol pppoe
virtual-template 1
!
call rsvp-sync
cns event-service server
!
interface Ethernet0/0
ip address 192.150.1.100 255.255.255.0
half-duplex
!
interface Ethernet0/1
no ip address
shutdown
half-duplex
!
interface ATM1/0
no ip address
no atm scrambling cell-payload
no atm ilmi-keepalive
pvc 1/40
encapsulation aal5snap
protocol pppoe
!
interface Virtual-Template1
ip address 2.2.2.1 255.255.255.0
ip mtu 1492
peer default ip address dhcp
ppp authentication chap
!
ip kerberos source-interface any
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet0/0
no ip http server
!
dialer-list 1 protocol ip permit
dial-peer cor custom
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
login
end

```

The following example shows configuration on the remote DHCP server:

```

2500ref-4#show run
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption

```

```
service udp-small-servers
service tcp-small-servers
!
hostname 2500ref-4
!
no logging console
!
ip subnet-zero
no ip domain-lookup
ip host PAGENT-SECURITY-V3 45.41.44.82 13.15.0.0
ip dhcp excluded-address 2.2.2.1
!
ip dhcp pool 1
network 2.2.2.0 255.255.255.0
dns-server 53.26.25.23
netbios-name-server 66.22.66.22
domain-name ribu.com
lease 0 0 5
!
cns event-service server
!
interface Ethernet0
ip address 192.150.1.101 255.255.255.0
interface Ethernet1
ip address 192.168.254.165 255.255.255.0
interface Serial0
no ip address
shutdown
no fair-queue
interface Serial1
no ip address
shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 1.1.1.1
ip route 0.0.0.0 0.0.0.0 Ethernet0
no ip http server
!
dialer-list 1 protocol ip permit
line con 0
exec-timeout 0 0
transport input none
line aux 0
transport input all
line vty 0 4
login
no scheduler max-task-time
end
```

Configuring IP Control Protocol Subnet Mask Delivery

The IP control protocol subnet mask delivery feature is supported on the following Cisco routers:

- Cisco 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, Cisco 831, and Cisco 837
- Cisco 828
- Cisco SOHO 77, Cisco SOHO 77H, Cisco SOHO 78, Cisco SOHO 91, Cisco SOHO 96, and Cisco SOHO 97

The IP Control Protocol (IPCP) feature assigns IP address pools to customer premises equipment (CPE) devices. These devices then assign IP addresses to the CPE and to a DHCP pool.

The IPCP feature provides the following functions:

- The Cisco IOS CPE device requests and uses the subnet.
- The Authentication, Authorization, and Accounting (AAA) Remote Authentication Dial-In User Service (RADIUS) provides the subnet and inserts the framed route into the proper virtual route forwarding (VRF) table.
- The provider edge or the edge router helps in providing the subnet through IPCP.

DHCP support is no longer on the client side because the CPE can now receive both the IP address and the subnet mask during the PPP setup negotiation. If the CPE uses the DHCP servers to allocate addresses for its own network, subnets can be assigned through the node route processor (NRP) on the network access server (NAS) and distributed to the remote CPE DHCP servers.

Follow these steps to configure the Cisco router (CPE) for IPCP:

-
- Step 1** Configure the ATM interface, and enter the ADSL operating mode.
- Step 2** Configure the ATM subinterface.
- a. Create an ATM PVC for data traffic, enter virtual circuit configuration mode, and specify the VPI and VCI values.
 - b. Set the encapsulation of the PVC as *aal5mux ppp* to support data traffic.
- Step 3** Create a dialer interface.
- a. Enter configuration mode for the dialer interface.
 - b. Specify the PPP encapsulation type for the PVC.
 - c. Enter the **ip unnumbered Ethernet 0** command to assign the Ethernet interface to the dialer interface.
 - d. Configure the dialer group number.
 - e. Configure CHAP.
 - f. Enter the **ppp ipcp mask request** command.
 - g. Assign a dialer list to this dialer interface.
- Step 4** Define an IP DHCP pool name.
- a. Enter the **import all** command.
 - b. Enter the **origin ipcp** command.
- Step 5** Configure the Ethernet interface, and assign an IP address pool. Enter the pool name that you defined in Step 4.
- Step 6** Configure a dialer list and a static route for the dialer interface.
-

Configuration Examples

The following example shows IPCP configuration on the Cisco router (CPE):

```
router-8274v-1# show run
Building configuration...
Current configuration :1247 bytes
version 12.2
no service single-slot-reload-enable
no service pad
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname router-8274v-1
!
no logging buffered
logging rate-limit console 10 except errors
!
username 6400-nrp2 password 0 lab
ip subnet-zero
ip dhcp smart-relay
!
ip dhcp pool IPPOOLTEST
import all
origin ipcp
lease 0 0 1
!
no ip dhcp-client network-discovery
!
interface Ethernet0
ip address pool IPPOOLTEST
no shutdown
hold-queue 32 in
!
interface ATM0
no ip address
atm ilmi-keepalive
bundle-enable
dsl operating-mode auto
hold-queue 224 in
!
interface ATM0.1 point-to-point
pvc 1/40
no ilmi manage
encapsulation aal5mux ppp dialer
dialer pool-member 1
!
interface Dialer0
ip unnumbered Ethernet0
encapsulation ppp
dialer pool 1
dialer-group 1
no cdp enable
ppp authentication chap callin
ppp chap hostname router-8274v-1
ppp chap password 7 12150415
ppp ipcp accept-address
ppp ipcp dns request
ppp ipcp wins request
ppp ipcp mask request
!
ip classless
```

```

ip route 0.0.0.0 0.0.0.0 Dialer0
no ip http server
!
dialer-list 1 protocol ip permit
!
line con 0
exec-timeout 0 0
stopbits 1
line vty 0 4
login
!
scheduler max-task-time 5000
end

```

The following example shows IPCP configuration on the remote server:

```

6400-nrp2#show run
Building configuration...
Current configuration :1654 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 6400-nrp2
!
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa nas port extended
enable password lab
!
username router-8274v-1 password 0 lab
username TB2-8274v-2 password 0 lab
!
redundancy
main-cpu
auto-sync standard
no secondary console enable
ip subnet-zero
no ip finger
!
interface ATM0/0/0
no ip address
no atm ilmi-keepalive
hold-queue 500 in
!
interface ATM0/0/0.4 point-to-point
pvc 6/40
encapsulation aal5mux ppp Virtual-Template5
!
!interface ATM0/0/0.5 point-to-point
pvc 5/46
protocol ip 7.0.0.60 broadcast
encapsulation aal5mux ppp Virtual-Template6
!
interface Ethernet0/0/1
no ip address
shutdown
!
interface Ethernet0/0/0
description admin IP address 192.168.254.201 255.255.255.0
ip address 192.168.254.240 255.255.255.0

```

```

!
interface FastEthernet0/0/0
ip address 192.168.100.101 255.255.255.0
half-duplex
!
interface Virtual-Template5
ip unnumbered FastEthernet0/0/0
no keepalive
no peer default ip address
ppp authentication chap
!
interface Virtual-Template6
ip unnumbered FastEthernet0/0/0
no peer default ip address
ppp authentication chap
!
ip classless
no ip http server
!
ip radius source-interface FastEthernet0/0/0
!
radius-server host 192.168.100.100 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute nas-port format d
radius-server key foo
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
  password lab
!
end

```

The following example shows IPCP configuration on the RADIUS server (Cisco Access Registrar 1.5):

```

/opt/AICar1/usrbin-4 % ./aregcmd
Access Registrar Configuration Utility Version 1.5
Copyright (C) 1995-1998 by American Internet Corporation, and 1998-2000 by
  Cisco Systems, Inc. All rights reserved.
Cluster:localhost
User:admin
Password:
Logging in to localhost
400 Login failed/opt/AICar1/usrbin-5 % ./aregcmd
Access Registrar Configuration Utility Version 1.5
Copyright (C) 1995-1998 by American Internet Corporation, and 1998-2000 by
  Cisco Systems, Inc. All rights reserved.
Cluster:localhost
User:admin
Password:
Logging in to localhost

[ //localhost ]
  LicenseKey = SBUC-7DQF-PM1E-5HPC (expires in 51 days)
  Radius/
  Administrators/

Server 'Radius' is Running, its health is 10 out of 10
--> cd radius

[ //localhost/Radius ]
  Name = Radius

```

```

Description =
Version = 1.6R1
IncomingScript~ =
OutgoingScript~ =
DefaultAuthenticationService~ = local-users
DefaultAuthorizationService~ = local-users
DefaultAccountingService~ = local-file
DefaultSessionService~ =
DefaultSessionManager~ =
UserLists/
UserGroups/
Policies/
Clients/
Vendors/
Scripts/
Services/
SessionManagers/
ResourceManagers/
Profiles/
Rules/
Translations/
TranslationGroups/
RemoteServers/
Advanced/
Replication/

--> cd profile

[ //localhost/Radius/Profiles ]
ls
  Entries 1 to 6 from 6 total entries
  Current filter:<all>

  default-PPP-users/
  default-SLIP-users/
  default-Telnet-users/
  StaticIP/
  router-8274v-1/
  TB2-8274v-2/

--> ls

[ //localhost/Radius/Profiles ]
  Entries 1 to 6 from 6 total entries
  Current filter:<all>

  default-PPP-users/
  default-SLIP-users/
  default-Telnet-users/
  StaticIP/
  router-8274v-1/
  TB2-8274v-2/

--> cd router-8274v-1

[ //localhost/Radius/Profiles/router-8274v-1 ]
  Name = router-8274v-1
  Description =
  Attributes/

--> ls

[ //localhost/Radius/Profiles/router-8274v-1 ]
  Name = router-8274v-1

```

```
Description =
Attributes/

--> cd attribute

[ //localhost/Radius/Profiles/router-8274v-1/Attributes ]
cisco-avpair = "ip:wins-servers=100.100.100.100 200.200.200.200"
cisco-avpair = "ip:dns-servers=60.60.60.60 70.70.70.70"
Framed-Compression = none
Framed-IP-Address = 40.1.2.30
Framed-IP-Netmask = 255.255.255.0
Framed-MTU = 1500
Framed-Protoc
l = ppp
Framed-Routing = None
Service-Type = Framed
```

Configuring the Service Assurance Agent

The Service Assurance Agent (SAA) can be configured on the following Cisco routers:

- Cisco 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, Cisco 831, and Cisco 837
- Cisco 828
- Cisco SOHO 77, Cisco SOHO 77H, Cisco SOHO 78, Cisco SOHO 96, and Cisco SOHO 97

The Service Assurance Agent (SAA) is an agent that monitors network performance by measuring key factors such as response time, availability, jitter, connect time, throughput, and packet loss.

The SA agent is a new name and an enhancement for the Response Time Reporter (RTR) feature introduced in Cisco IOS Release 11.2.

For configuration information on this command, see the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt3/fcd301d.htm#xtocid135130

Configuring Secure Shell

Secure Shell (SSH) is supported on the following Cisco routers:

- Cisco 826 and 836
- Cisco 827, 827H, 827-4V, 831, and 837
- Cisco 828
- Cisco SOHO 91, SOHO 96, and SOHO 97

SSH is a protocol that provides a secure and remote connection to a router. SSH is available in two versions, SSH Version 1 and SSH Version 2. Only SSH Version 1 is available in the Cisco IOS software.

For configuration information on this command, see the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s5/sshv1.htm>

Configuring IP Named Access Lists

IP named access lists are supported on the following Cisco routers:

- Cisco 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, Cisco 831, and Cisco 837
- Cisco 828
- Cisco SOHO 77, Cisco SOHO 77H, Cisco SOHO 78, Cisco SOHO 96, and Cisco SOHO 97

You can identify IP access lists with an alphanumeric string (name) instead of a number. When you use named access lists, you can configure more IP access lists in a router.

For configuration information on this command, see the following URL:

http://cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipeprt1/1cdip.htm#xtocid2299616

Configuring International Phone Support

Cisco 827-4V routers provide international phone support (H.323 only) for the following countries:

- Italy
- Denmark
- Australia

International phone support commands configure voice port settings and caller ID settings.

H.323 international phone support has been tested and verified to work with the following equipment identified for Italy and Denmark.

The following devices are supported in Italy:

- Telephones:
 - Siemens Gigaset 3015 Class Model
 - Telecom Italia MASTER s.p. LUPO VIEW
 - Alcatel Dial Face Mod. SIRIO 2000 Basic A
- Caller-ID Devices:
 - BRONDI INDOVINO
- Fax equipment:
 - Canon FAX-B155

The following devices are supported in Denmark:

- Telephones:
 - Tele Danmark dana classic
 - Tele Danmark Danafon Topas
- Caller-ID Devices:
 - DORO Danmark DOROX5

Use the following procedure to configure a voice port to support caller ID, international cadence, impedance, and ring frequency, starting in global configuration mode:

-
- Step 1** Enter the **voice-port** *number* command to enter voice-port configuration mode.
- Step 2** Enter the **cptone** *country-code* command to specify settings for call-progress tone, ring cadence, line impedance, and ring frequency.
- Step 3** Enter one of the following commands to enable caller ID:
- Enter the **caller-id enable** command to enable caller ID support.
 - Enter the **caller-id alerting** *alerting-method* command to enable caller ID support and to specify the alerting method.
- Step 4** Enter the **caller-id block** command to request blocking of the display of caller ID information at the far end of the call.
- Step 5** Enter **end** to exit router configuration mode.
-

Configuration Example

The following voice-port configuration example shows two voice ports configured for the progress tone and line characteristics for Denmark. Caller ID is enabled on both ports, and port 1 requests that caller ID information be blocked at the other end when a phone call originates from this port. The second port uses the line-reversal alerting method.

```
!
voice-port 1
cptone dk
caller-id enable
caller-id block
timeouts call-disconnect 0
!
voice-port 2
cptone dk
caller-id alerting line-reversal
timeouts call-disconnect 0
```

International Tone, Cadence, Ring Frequency, and Impedance Support

The default voice-port configuration for all voice ports specifies the U.S. country code, 600-ohm impedance, and 25-Hz ring frequency. Cisco IOS software supports commands for setting ring tone, cadence, frequency, and line impedance.

cptone Command

Use the voice-port configuration mode **cptone** command to specify a regional analog voice interface-related tone. Use the **no** form of this command to disable the selected tone.

```
cptone { dk | it | au }
no cptone { dk | it | au }
```

The following table shows what each code specifies.

Code	Country	Parameters
dk	Denmark	POTS line type 2 (complex impedance), a-law encoding, OSI disconnect supervision, 25-Hz ringing frequency, 0 guard time
it	Italy	POTS line type 2 (complex impedance), a-law encoding, OSI disconnect supervision, 25-Hz ringing frequency, 0 guard time
au	Australia	POTS line type 2 (complex impedance), a-law encoding, OSI disconnect supervision, 20-Hz ringing frequency, 0 guard time

ring cadence Command

To specify the ring cadence for a Foreign Exchange Station (FXS) voice port, use the **ring cadence** command in voice-port configuration mode. Use the **no** form of this command to restore the default value for this command.

```
ring cadence cadence
no ring cadence
```

The **ring cadence** command can take the following values.

Value	Meaning
define	User-defined cadence
pattern01	2 seconds on, 4 seconds off
pattern02	1 second on, 4 seconds off
pattern03	1.5 seconds on, 3.5 seconds off
pattern04	1 second on, 2 seconds off
pattern05	1 second on, 5 seconds off
pattern06	1 second on, 3 seconds off
pattern07	.8 second on, 3.2 seconds off
pattern08	1.5 seconds on, 3 seconds off
pattern09	1.2 seconds on, 3.7 seconds off
pattern10	1.2 seconds on, 4.7 seconds off
pattern11	0.4 second on, 0.2 second off, then 0.4 second on, 2 seconds off
pattern12	0.4 second on, 0.2 second off, then 0.4 second on, 2.6 seconds off

ring frequency Command

To specify the ring frequency for a specified FXS voice port, use the **ring frequency** command in voice-port configuration mode. Use the **no** form of this command to restore the default value for this command.

```
ring frequency frequency
no ring frequency
```

To select the ring frequency, use the commands as follows.

25	Specify a 25-Hz ring frequency.
50	Specify a 50-Hz ring frequency.

impedance Command

To specify the terminating impedance of a voice port interface, use the **impedance** command in voice-port configuration mode. Use the **no** form of this command to restore the default value.

```
impedance {600c | 600r | 900c | 900r | complex1 | complex2 }
no impedance {600c | 600r | 900c | 900r | complex1 | complex2 }
```

The following table shows what each code specifies.

Code	Impedance
600c	600-ohm complex
600r	600-ohm real
900c	900-ohm complex
900r	900-ohm real
complex1	complex 1
complex2	complex 2

When using the **impedance** command, be aware of the following constraints:

- The **c600r** option selects the current POTS line type 0 implementation.
- The **900r** option selects the current POTS line type 1 implementation.
- The **600c**, **900c**, **complex1**, and **complex2** options select the current POTS line type 2 implementation.

Configuring International Caller ID

Caller ID (CLID) is an analog service that displays the number of the calling line to the receiving line's terminal device when it receives a call. In some countries, CLID is called Calling Line Identity Presentation (CLIP). The Cisco router receives CLID data as a part of the H.225 Setup Message and transmits it to the terminal device, which can either be a CLID device or a telephone capable of showing CLID messages.

There are two types of CLID: Type I and Type II. Type I transmits the CLID information when the receiving phone is on hook. Type II transmits the CLID information when the receiving phone is off hook. Only type I CLID is supported in this release.

caller-id enable Command

To allow the sending of caller ID information to the FXS voice port, use the **caller-id enable** voice-port configuration command. To disable the sending of caller ID information, use the **no** form of this command, which also clears all other caller ID configuration settings for the voice port.

```
caller-id enable
no caller-id enable
```

The country code specified in the **cptone** command must represent one of the countries for which caller ID is supported. Caller ID is disabled by default.

caller-id alerting Command

Specify the caller ID alerting method and enable caller ID support by using the **caller-id alerting** voice-port configuration command. The **no** form of this command sets the caller ID alerting type to caller ID alerting ring type 1.

```
caller-id alerting { line-reversal | pre-ring | ring < 1 | 2 > }
no caller-id alerting { line-reversal | pre-ring | ring < 1 | 2 > }
```

Alerting methods are described in the following table.

Alerting Method	Description
line-reversal	Use line-reversal alerting method.
pre-ring	Set a 250-millisecond pre-ring alerting method for caller ID information for on-hook (Type 1) caller ID at an FXS voice port.
ring < 1 2 >	Set the ring-cycle method for receiving caller ID information for on-hook (Type 1) caller ID at an FXS voice port. 1—If your telephone service provider specifies it, use this setting to provide caller ID alerting (display) after the first ring at the receiving station. 2—If your telephone service provider specifies it, use this setting to provide caller ID alerting (display) after the second ring.

The default alerting method is **ring 1**. If the country in which the router is installed uses a different alerting method, the appropriate alerting method must be configured. The **caller-id alerting ring** command can be used in countries using the BellCore/Telcordia standard. The **caller-id alerting line-reversal**, the **caller-id alerting pre-ring**, and **caller-id alerting ring** commands can be used in countries that do not use the BellCore/Telcordia standard.

The **caller-id alerting** command automatically enables caller ID support for the specific voice port.

caller-id block Command

To request the blocking of the display of caller ID information at the far end of a call for calls originated at an FXS port, use the **caller-id block** voice-port configuration command at the originating Foreign FXS voice port. To allow the display of caller ID information, use the **no** form of this command.

```
caller-id block
no caller-id block
```

The default is no blocking of caller ID information.



Note

The calling party information is included in the routed on-net call, as this information is often required for other purposes, such as billing and call blocking. The request to block display of the calling party information on terminating FXS ports is normally accepted by Cisco routers, but no guarantee can be made regarding the acceptance of the request by other equipment.

Configuring Committed Access Rate

This feature is available on the following Cisco routers:

- Cisco 826 and 836
- Cisco 827, 827H, 827-4V, 831, and 837
- Cisco 828

Use the committed access rate (CAR) to limit bandwidth transmission rates to traffic sources and destinations and to specify policies for handling traffic that breaches the specified bandwidth allocations. To enable CAR, enter the **rate-limit** command while in ATM interface configuration mode.

Configuration Example

The following example shows a CAR configuration:

```
interface ATM0.1 point-to-point
  mtu 576
  ip address 10.0.0.10 255.255.255.0
  rate-limit output 368000 2000 2000 conform-action set-dscp-transmit 40 exceed-action
  set-dscp-transmit 48
  pvc 0/33
    protocol ip 10.0.0.9 broadcast
    vbr-nrt 142 142 1
    encapsulation aal5snap
  !
```

Configuring VPN IPSec Support Through NAT

This feature is available on the following Cisco routers:

- Cisco 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, Cisco 831, and Cisco 837

- Cisco 828
- Cisco SOHO 77, Cisco SOHO 78, Cisco SOHO 96, and Cisco SOHO 97

Cisco IOS Release 12.2(2)XI NAT supports IP Security (IPsec) client software that does not use Transmission Control Protocol (TCP) wrapping or User Datagram Protocol (UDP) wrapping. On Cisco routers, this feature allows the simultaneous use of multiple, PC-based IPsec clients on which IPsec packet wrapping is disabled or is not supported. When PCs connected to the router create an IPsec tunnel, network address translation (NAT) on the router translates the private IP addresses in these packets to public IP addresses. This NAT feature also supports multiple Point-to-Point Tunnel Protocol (PPTP) sessions, which may be initiated by PCs with PPTP client software.

You must enter the following command in global configuration mode for this feature to work:

```
ip nat inside source list number interface BVI number overload
```

NAT Default Inside Server Enhancement

This feature is supported on the following Cisco routers:

- Cisco 831, Cisco 836, and Cisco 837
- Cisco SOHO 91, Cisco SOHO 96, and Cisco SOHO 97

The NAT command has been extended to allow you to specify an inside local address to receive packets that do not match criteria in other NAT statements in the configuration.

The syntax is as follows:

```
ip nat inside source static inside_local interface interface_name
```

Configuration Example

Several NAT statements direct traffic to the address 20.0.0.14. All packets not matching those NAT statements will be routed to 20.0.0.16.

```
Current configuration :942 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c836-1
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto mib ipsec flowmib history tunnel size 200
crypto mib ipsec flowmib history failure size 200
!
interface Ethernet0
 ip address 20.0.0.1 255.0.0.0
 ip nat inside
 hold-queue 100 out
!
interface Ethernet1
 ip address 10.0.0.1 255.0.0.0
```

```
ip nat outside
!
ip nat inside source static tcp 20.0.0.14 80 interface Ethernet1 80
ip nat inside source static udp 20.0.0.14 161 interface Ethernet1 161
!
ip nat inside source static 20.0.0.16 interface Ethernet1
! 20.0.0.16 is defined as the catch-all address
!
ip nat inside source static udp 20.0.0.14 1000 interface Ethernet1 1000
! udp port 1000 traffic will be routed to 20.0.0.14
!
ip nat inside source static tcp 20.0.0.14 23 interface Ethernet1 23
! telnet traffic will be routed to 20.0.0.14
!
ip classless
no ip http server
!
!
line con 0
  stopbits 1
line vty 0 4
  password lab
  login
```

Configuring VoAAL2 ATM Forum Profile 9 Support

The Cisco 827-4V router supports voice over ATM Adaptation Layer 2 (VoAAL2) ATM Forum Profile 9. ATM Forum Profile 9 supports a 44-byte payload, optimizing voice transport efficiency, and makes interoperability with TdSoft gateways possible.

This feature enables the Cisco router to interoperate with GR.303 and V5.2 gateways that communicate with Class 5 switches. The voice PVC is routed to a VoAAL2 gateway that supports either the General Recommendation 303 (GR.303) or the V5.2 protocol. This gateway converts the AAL2-encoded voice cells to a format that can be sent over a time division multiplexed connection to a Class 5 switch. The data PVC can be routed through the digital subscriber line access multiplexer (DSLAM) or aggregator to the data network.

Configuring ATM Forum Profile 9

Follow these steps to configure ATM Forum Profile 9 support for a voice port, beginning in global configuration mode.

-
- Step 1** Enter the **voice class permanent 1** command to configure a voice class.
 - Step 2** Enter the **signal timing oos timeout disabled** command to disable the assertion of the receive Out-of-Service (OOS) pattern to the PBX when signaling packets are lost.
 - Step 3** Enter **exit** to exit voice class configuration mode.
 - Step 4** Enter **voice service voatm** to enter voice service configuration mode.
 - Step 5** Enter the **session protocol aal2** command.
 - Step 6** Enter **mode bles** to indicate that VOATM is to be used in broadband loop emulation service (BLES) mode.

- Step 7** Enter **exit** to leave session protocol mode, and then enter **exit** again to leave voice service configuration mode.
- Step 8** Enter **interface atm0** to enter ATM 0 interface configuration mode.
- Step 9** Enter **pvc vpi vci** to specify the virtual path identifier and the virtual channel identifier of the PVC.
- Step 10** Enter **vbr-rt pcr acr bcs** to specify the variable bit rate-real time peak cell rate and average cell rate in kbps, and the burst cell size in number of cells.



Note One phone line requires a minimum setting of 78 kbps for both PCR and ACR values.

- Step 11** Enter **encapsulation aal2** to specify that ATM adaptation layer 2 type encapsulation be used.
- Step 12** Enter **no atm cell-clumping-disable** to ensure that sufficient bandwidth is allocated for data packets when voice calls are in progress.
- Step 13** Enter **exit** to leave ATM 0 interface configuration mode.
- Step 14** Enter the **dial-peer voice tag voatm** command. This command places the router in dial-peer voice configuration mode.
- Step 15** Enter the **session protocol aal2-trunk** command.
- Step 16** Enter the **session target atm0 pvc vpi/vci cid cid** command.
- This command has the following parameters:
- *vpi*—Virtual path identifier
 - *vci*—Virtual channel identifier
 - *cid*—AAL2 channel identifier
- Step 17** To specify which codec profile the voice dial peer will use, enter one of these **codec aal2 profile** commands, as appropriate:
- Enter **codec aal2-profile atmf 9 g711alaw** to specify that only G.711 a-law be used.
 - Enter **codec aal2-profile atmf 9 g711ulaw** to specify that only G.711 mu-law be used.
- Step 18** Enter the **destination-pattern destination string** command. The *destination string* is the phone number in E.164 format that must match the destination string configured for the voice-port in order to associate a dial-peer with a voice port.
- Step 19** Enter the **voice-class permanent 1** command to associate this dial peer with the configured voice class.
- Step 20** Enter **no vad** to specify no voice activity detection (VAD).
- Step 21** Enter **exit** to leave dial peer voice configuration mode.
- Step 22** Enter the **voice port #** command to enter voice port configuration mode.
- Step 23** Enter the **connection trunk destination-pattern** command. The destination pattern must match the *destination-string* configured for the dial peer.
- Step 24** Enter the **playout-delay mode fixed no-timestamps** command. This command causes the AAL2 packet to be played at a fixed rate, and the timestamps carried in the packet to be ignored.
- Step 25** Enter **end** to exit router configuration mode.
-

Configuration Example

The following example shows the configuration for two voice ports using Profile 9, and the G.711 a-law codec. VBR-RT, PCR, and ACR values are 312 to accommodate 4 phone lines, although only 2 phone lines are currently configured.

```
voice service voatm
!
 session protocol aal2
 mode bles
!
!
voice class permanent 1
 signal timing oos timeout disabled
!
interface atm 0
 no atm cell-clumping-disable
 pvc 1/100
 vbr-rt 312 312 32
 encapsulation aal2
!
voice-port 1
 playout-delay mode fixed no-timestamps
 cptone DK
 timeouts wait-release 3
 connection trunk 8881052
 caller-id enable
!
voice-port 2
 playout-delay mode fixed no-timestamps
 cptone DK
 timeouts wait-release 3
 connection trunk 8881053
 caller-id enable
!
!dial-peer voice 1000 voatm
 destination-pattern 8881052
 voice-class permanent 1
 session protocol aal2-trunk
 session target ATM0 pvc 1/100 16
 codec aal2-profile ATMF 9 g711alaw
 no vad
!
dial-peer voice 1001 voatm
 destination-pattern 8881053
 voice-class permanent 1
 session protocol aal2-trunk
 session target ATM0 pvc 1/100 17
 codec aal2-profile ATMF 9 g711alaw
 no vad
!
```

Configuring ATM OAM F5 Continuity Check Support

This feature is available on the following Cisco routers:

- Cisco 826 and Cisco 836
- Cisco 827, Cisco 827H, and Cisco 837
- Cisco SOHO 77, Cisco SOHO 96, and Cisco SOHO 97

ATM operation administration and maintenance (OAM) F5 continuity check (CC) cells enable network administrators to detect misconfigurations in the ATM layer. Such misconfigurations can cause misdelivery of a cell stream to a third party or can cause unintended merging of cells from multiple sources.

CC cells provide an in-service tool optimized to detect connectivity problems at the ATM layer. CC cells are sent between a router designated as the source location and a router designated as the sink location. The local router can be configured as the source, as the sink, or as both the source and the sink. It is not necessary to enter a CC configuration on the router at the other end of the segment, because the router on which CC has been configured sends a CC activation request to the router at the other end of the segment, directing it to act as either a source or a sink.

oam-pvc manage cc Command

The **oam-pvc manage cc** command configures continuity checking on a PVC. Use the **no** form of this command to disable continuity checking on the segment.

```
oam-pvc manage cc segment direction [ source | sink | both ]
no oam-pvc manage cc segment direction [ source | sink | both ]
```

Syntax Description

segment direction specifies the CC cell transmission direction.

source	The router is to act as the source of CC cells.
sink	The router is to act as the sink, or destination, for transmitted CC cells.
both	The router is to act as both source and sink.

Default

The default segment direction is sink.

Command Mode

PVC configuration mode.

Message Guidelines

Using **no oam-pvc manage cc** deactivates continuity checking regardless of the direction in which it is being performed, and regardless of which router initiated continuity checking.

Configuration Examples

The following configuration activates CC over the segment and causes the router to function as the source.

```
interface ATM0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/33
  oam-pvc manage cc segment direction source
 !
end
```

The following configuration activates CC over the segment and causes the router to function as the sink.

```
interface ATM0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/33
  oam-pvc manage cc segment direction sink
 !
end
```

The following configuration activates CC over the segment and causes the router to function both as the source of CC cells and as the sink:

```
interface ATM0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/33
  oam-pvc manage cc segment direction both
 !
end
```

The following configuration deactivates segment CC:

```
interface ATM0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/33
  no oam-pvc manage cc
 !
end
```

oam retry cc activation-count deactivation-count retry-frequency Command

The **oam retry cc activation-count deactivation-count retry-frequency** command sets the frequency at which CC activation and deactivation requests are sent to the router at the other end of the segment. The **no** form of this command removes these settings.

```
oam retry cc activation-count number deactivation-count number retry-frequency seconds
no oam retry cc activation-count number deactivation-count number retry-frequency seconds
```

Syntax Description

activation-count	Specifies the maximum number of times the activation message will be sent before receiving an acknowledgement.
deactivation-count	Specifies the maximum number of times the deactivation message will be sent before receiving an acknowledgement.
retry-frequency	Specifies the interval between retries.

Default

No default.

Command Mode

PVC configuration.

Example Configuration

The following configuration sets the CC activation and deactivation counts, as well as the retry frequency:

```
interface ATM0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/33
  oam-pvc manage cc segment direction source
  retry activation-count 10 deactivation-count 10 retry-frequency 3
!
```

```
end
```

oam-pvc manage cc deny Command

The **oam-pvc manage cc deny** command disables CC support on the virtual circuit (VC) under which the command has been entered. A PVC on which CC support has been disabled will deny CC activation requests. The **no** form of this command reenables CC support on the VC.

```
oam-pvc manage cc deny
no oam-pvc manage cc deny
```

Default

CC is supported by default.

Command Mode

PVC configuration mode.

Example Configuration

The following configuration denies segment CC:

```
interface ATM0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/33
  oam-pvc manage cc deny
!
```

```
end
```

debug atm oam cc Command

You see the results of continuity checking by using the **debug atm oam cc** command. The **no** form of this command disables continuity checking debugging.

```
debug atm oam cc interface atm number
no debug atm oam cc interface atm number
```

Syntax Description

<i>number</i>	ATM interface number.
---------------	-----------------------

Default

Disabled.

Command Mode

Privileged EXEC.

Example Output

The following example output of the debug **atm oam cc** command records activity beginning with the entry of the **oam-pvc manage cc** command, and ending with the entry of the **no oam-pvc manage cc** command. The ATM 0 interface was specified, and the “both” segment direction was specified. The output shows an activation request sent and confirmed, a series of CC cells sent by the routers on each end of the segment, and a deactivation request and confirmation.

```
router# debug atm oam cc interface atm0
Generic ATM:
  ATM OAM CC cells debugging is on
router#
00:15:05: CC ACTIVATE MSG (ATM0) I:VCD#1 VC 1/40 OAM Cell Type:4 OAM
Type:8 OAM Func:1 Direction:3 CTag:5
00:15:05: CC ACTIVATE CONFIRM MSG (ATM0) O:VCD#1 VC 1/40 OAM Cell
Type:4 OAM Type:8 OAM Func:1 Direction:3 CTag:5
00:15:06: CC CELL (ATM0) O:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1
00:15:07: CC CELL (ATM0) I:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:08: CC CELL (ATM0) O:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:09: CC CELL (ATM0) I:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:10: CC CELL (ATM0) O:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:11: CC CELL (ATM0) I:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:12: CC CELL (ATM0) O:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:13: CC CELL (ATM0) I:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:14: CC CELL (ATM0) O:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:15: CC CELL (ATM0) I:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:16: CC CELL (ATM0) O:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:17: CC CELL (ATM0) I:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:18: CC CELL (ATM0) O:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:19: CC CELL (ATM0) I:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:19: CC DEACTIVATE MSG (ATM0) I:VCD#1 VC 1/40 OAM Cell Type:4 OAM
Type:8 OAM Func:1 Direction:3 CTag:6
00:15:19: CC DEACTIVATE CONFIRM MSG (ATM0) O:VCD#1 VC 1/40 OAM Cell
Type:4 OAM Type:8 OAM Func:1 Direction:3 CTag:6
```

The following table describes significant fields.

Field	Description
00:15:05	Time stamp.
CC ACTIVATE MSG (ATM0)	Message type and interface.
0	Source.
1	Sink.
VC 1/40	Virtual circuit identifier.
Direction:3	Indication of the direction in which the cells are traveling. 1 indicates local router is sink. 2 indicates local router is source. 3 indicates both routers operate as source and sink.

Configuring RADIUS Support

Remote Authentication Dial-In User Service (RADIUS) is supported on the following Cisco routers:

- Cisco 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, Cisco 831, and Cisco 837
- Cisco 828

RADIUS enables you to secure your network against unauthorized access. A RADIUS server must be configured in the service provider or corporate network in order for the router to use RADIUS client features.

Configuring Cisco Easy VPN Client

Routers and other forms of broadband access provide high-performance connections to the Internet. However, many applications also require the security of Virtual Private Network (VPN) connections that perform a high level of authentication and that encrypt the data between two particular endpoints. Establishing a VPN connection between two routers can be complicated, and it typically requires tedious coordination between network administrators to configure the two routers' VPN parameters.

The Cisco Easy VPN client feature eliminates much of this tedious work by implementing Cisco's Unity Client protocol, which allows most VPN parameters to be defined at a VPN 3000 concentrator acting as an IPsec server.

After the IPsec server has been configured, a VPN connection can be created with minimal configuration on an IPsec client, such as a supported Cisco 800 series router. When the IPsec client then initiates the VPN tunnel connection, the IPsec server pushes the IPsec policies to the IPsec client and creates the corresponding VPN tunnel connection.

The Cisco Easy VPN client feature supports two modes of operation:

- **Client**—Specifies that Network Address Translation/Port Address Translation (NAT/PAT) be done, so that the PCs and other hosts at the client end of the VPN tunnel form a private network that does not use any IP addresses in the destination server's IP address space.
- **Network Extension**—Specifies that the PCs and other hosts at the client end of the VPN tunnel should be given IP addresses in the destination enterprise network's IP address space, so that they form one logical network.

Both modes of operation also optionally support split tunneling, which allows secure access to corporate resources through the VPN tunnel while also allowing Internet access through a connection to an ISP or other service (thereby eliminating the corporate network from the path for Web access). This configuration is enabled by a simple access list implemented on the IPsec server.

**Note**

Cisco 800-series routers are supported as IPsec clients of VPN 3000 concentrators. Support for other IPsec servers will be available in a future release. Be sure to see the Cisco IOS release notes for the current release to determine if there are any other limitations on the use of Cisco Easy VPN Client.

Easy VPN Documentation

The release note “[Cisco EZVPN Client for the Cisco uBR905/uBR925 Cable Access Routers](#)” contains instructions for configuring the DHCP server pool, the Easy VPN client profile required to implement Easy VPN, contains example configurations for the IPSec server, and descriptions of **commands available to manage Easy Virtual Private Networking**.

Configuration Example

This section provides a client mode configuration example for the Cisco 827 router.

The following example configures a Cisco 827 router as an IPSec client, using the Cisco Easy VPN feature in the client mode of operation. This example shows the following components of the Cisco Easy VPN client configuration:

- DHCP server pool—The **ip dhcp pool** command creates a pool of IP addresses to be assigned to the PCs connected to the router’s Ethernet1 interface. The pool assigns addresses in the class C private address space (192.168.100.0) and configures each PC so that its default route is 192.168.100.1, which is the IP address assigned to the router’s Ethernet interface.
- EzVPN client configuration—The first **crypto ipsec client ezvpn hw-client** command (global configuration mode) creates an EzVPN client configuration named *hw-client*. This configuration specifies a group name of *hw-client-groupname* and a shared key value of *hw-client-password*, and it sets the peer destination to the IP address **188.185.0.5** (which is the address assigned to the interface connected to the Internet on the destination peer router). The EzVPN configuration is configured for the default operations mode **client**.



Note If DNS is also configured on the router, the **peer** option also supports a host name instead of an IP address.

- The second **crypto ipsec client ezvpn hw-client** command (ATM 0 interface configuration mode) assigns the EzVPN client configuration to the ATM 0 interface, so that all traffic received and transmitted on that interface is sent through the VPN tunnel.

The output of the **show running-config** command follows:

```
Current configuration :1040 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c827-18
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip dhcp excluded-address 192.168.100.1
!
ip dhcp pool CLIENT
import all
```

```

network 192.168.100.0 255.255.255.0
default-router 192.168.100.1
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto ipsec client ezvpn hw-client
group hw-client-groupname key hw-client-password
mode client
peer 188.185.0.5
!
interface Ethernet0
ip address 192.168.100.1 255.255.255.0
hold-queue 100 out
!
interface ATM0
ip address 192.168.101.18 255.255.255.0
no atm ilmi-keepalive
protocol ip 192.168.101.19 broadcast
encapsulation aal5snap
!
dsl operating-mode auto
crypto ipsec client ezvpn hw-client
!
ip classless
ip route 0.0.0.0 0.0.0.0 ATM0
ip route 50.0.0.0 255.0.0.0 40.0.0.19
ip http server
ip pim bidir-enable
!
line con 0
stopbits 1
line vty 0 4
login
!

```

Configuring Dial-on-Demand Routing for PPPoE Client

Dial-on-demand routing (DDR) for PPPoE client is supported on the following Cisco routers:

- Cisco 826 and Cisco 836
- Cisco 827, 827H, Cisco 827-4V, Cisco 831, and Cisco 837
- Cisco 828
- Cisco SOHO 77, Cisco SOHO 77H, Cisco SOHO 78, Cisco SOHO 91, Cisco SOHO 96, and Cisco SOHO 97

The DDR for PPPoE client feature provides flexibility for subscribers whose ISP charges are based on the amount of time they are connected to the network (non-flat-rate services). With the DDR for PPPoE feature, you can designate a type of traffic as traffic of interest. You can then configure the router so that it will bring up the PPPoE connection when any interesting traffic arrives from the LAN interface and will bring down the connection when the dialer idle timer expires.

DDR is configured in Ethernet 1 configuration mode, using the **pppoe-client dial-pool-number** command with the **dial-on demand** keyword. The syntax is shown below.


```
pppoe-client dial-pool-number number [dial-on-demand]
```

Syntax Descriptions

dial-pool-number	Create a dial pool.
dial-on-demand	Activate DDR.

Configuring DDR for a PPPoE Client

Complete the following tasks to configure DDR for a PPPoE client, beginning in global configuration mode:

-
- Step 1** Enable vpdn.
- Enter the global configuration mode **vpdn enable** command.
 - Enter **no vpdn logging** command to disable vpdn logging.
- Step 2** Configure a virtual private dial-up network (VPDN) group.
- Enter the global configuration mode **vpdn-group number** command, to enter vpdn group configuration mode.
 - Enter **request-dialin** to specify the dial-in dialing mode.
- Step 3** Configure the Ethernet 1 interface.
- Enter **interface Ethernet 1** to enter Ethernet 1 interface configuration mode.
 - Enter **pppoe enable** to enable PPPoE for this interface.
 - Activate DDR and create a dial pool by entering **pppoe-client dial-pool-number number dial-on-demand**. The *number* value must match the vpdn group number.
- Step 4** Configure the dialer interface.
- Enter **interface dialer 1** to enter dialer interface configuration mode.
 - Enter **ip address negotiated** to indicate that the ip address will be negotiated with the DHCP server.
 - Specify the maximum transmission unit size by entering **ip mtu 1492**.
 - Set the encapsulation type by entering **encapsulation ppp**.
 - Enter the **dialer pool number** command to associate the dialer interface with the dialer pool created for the Ethernet 1 interface.
 - Set the idle timer interval by entering **dialer idle-timeout 180 either**. The **either** keyword specifies that either inbound or outbound traffic can reset the idle timer.
-  **Note** A value of 0 specifies that the timer will never expire and that the connection will always be up.
- Enter **dialer hold-queue 100** to set the queue to a size that will hold packets of interest before the connection is established.
 - Enter **dialer-group 1** to specify the dialer list that defines traffic of interest.
 - Leave Dialer 1 interface configuration mode by entering **exit**.
- Step 5** Enter the global interface configuration **dialer-list 1 protocol ip permit** command to define IP traffic as the traffic of interest.

- Step 6** Create a static route for the Dialer 1 interface by entering the **ip route 0.0.0.0 0.0.0.0 dialer 1 permanent** command.
- Step 7** Enter **end** to leave router configuration mode.
-

Configuring Weighted Fair Queuing

Weighted fair queuing (WFQ) is supported on the following Cisco routers:

- Cisco 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, Cisco 831, and Cisco 837
- Cisco 828

WFQ enables slow-speed links, such as serial links, to provide fair treatment for all types of traffic. In order to do this, WFQ classifies the traffic into different flows (also known as conversations) based on layer three and layer four information, such as IP addresses and TCP ports. It does this without requiring you to define access lists. This means that low-bandwidth traffic effectively has priority over high-bandwidth traffic because high-bandwidth traffic shares the transmission media in proportion to its assigned weight. WFQ is now available on IP Base and IP Firewall Cisco IOS images.

WFQ has certain limitations: it is not scalable if the flow amount increases considerably, and native WFQ is not available on high-speed interfaces such as ATM interfaces. Class-based WFQ, available on Cisco IOS Plus images, overcomes these limitations.

Configuring Weighted Fair Queuing

The following procedure shows how to apply WFQ to the ATM interface of a Cisco router.

- Step 1** Create a policy map for WFQ.
- a. Enter the **policy-map map-name** command in global configuration mode to construct a WFQ policy. The map name *wfq* could be used to specify that this is the policy map for WFQ.
 - b. Enter **class class-default** to use the default class for all traffic.
 - c. Apply WFQ to all traffic by entering the **fair-queue** command.
 - d. Enter **exit** twice to return to global configuration mode.
- Step 2** Apply the policy map to the router interface.
- a. Enter **interface atm number**, where *number* is the ATM interface number.
 - b. Enter **pvc vpi/vci** to specify which PVC you are applying the policy map to.
 - c. Enter **service-policy output map-name** to apply the policy to this PVC. If you named the policy map *wfq*, you would enter the command **service-policy output wfq**.
- Step 3** Enter **end** to leave router configuration mode.
-

Example Configuration

The following configuration applies WFQ to PVC 0/33 on the ATM 0.1 interface. The policy map named *wfq* is created, and WFQ is applied to the default class referenced in that policy map. Then, *wfq* is referenced in the ATM 0.1 interface configuration.

```

version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password encryption
!
hostname 806-uut
!
ip subnet-zero
!
policy-map wfq
  class class-default
    fair-queue
!
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
!
interface atm0.1
  no ip address
  pvc 0/33
    service-policy output wfq
!
ip classless
ip http server
ip pim bidir-enable
!
line con 0
  stopbits 1
line vty 0 4
  login
!
scheduler max-task-time 5000
end
!
```

Configuring DSL Commands

The sections below describe the supported DSL commands.

Follow the steps below to configure DSL command-line interface (CLI) commands.

	Command	Purpose
Step 1	dsl noise-margin	Sets the noise margin offset.
Step 2	max-tone-bits	Sets the maximum bits per tone limit.
Step 3	gain-setting rx-offset	Sets the receive gain offset.
Step 4	gain-setting tx-offset	Sets the transmit gain offset.

Configuration Example

The following is a configuration example for the **dsl** command.

```
interface ATM0
  no ip address
  no atm ilmi-keepalive
  dsl operating-mode auto
  dsl noise-margin 0
  dsl max-tone-bits 14
  dsl gain-setting tx-offset 0
  dsl gain-setting rx-offset 1
```

Enabling the DSL Training Log

The DSL training log feature is available on the following Cisco routers:

- Cisco 826 and 836
- Cisco 827, 827H, 827-4V, and 837
- Cisco 828

By default, a DSL training log is retrieved each time the Cisco router establishes contact with the DSLAM. The training log is a record of the events that occur when the router *trains*, or negotiates communication parameters, with the DSLAM at the central office. However, retrieving this log adds significant time to the training process, and retrieval is not always necessary after the router has successfully trained. You must use the **dsl enable-training-log** command to enable the retrieval of this log. The **no** form of this command disables retrieval of the DSL training log.

```
dsl enable-training-log
no dsl enable-training-log
```

Retrieving the DSL Training Log and Then Disabling Further Retrieval of the Training Log

Complete the following tasks to retrieve the training log, examine it, and then disable the router from retrieving the training log the next time it trains with the DSLAM.

-
- Step 1** Configure the router to retrieve the training log.
- Enter the global configuration mode **interface ATM *number*** command, where *number* is the number of the ATM interface.
 - Enter **dsl enable-training-log** to enable the retrieval of the training log.
 - Enter **end** to leave router configuration mode.
- Step 2** Unplug the DSL cable from the DSL socket on the back of the router, wait a few seconds, and then plug the cable back in.
- Step 3** When the “DSL line up” message appears, issue the **show dsl int atm *number*** command, where *number* is the number of the ATM interface, to display the retrieved log.
- Step 4** When you decide that it is no longer necessary for the router to retrieve the training log, reconfigure the router to disable the retrieval of the log by completing the following tasks:
- Enter the global configuration mode **interface ATM *number*** command, where *number* is the number of the ATM interface.

- b. Enter **no dsl enable-training-log** to disable the retrieval of the training log.
- c. Enter **end** to leave router configuration mode.

Selecting Secondary DSL Firmware

This command is available on the following routers:

- Cisco 827, 827H, and 827-4V
- Cisco 837 routers.

The ATM interface mode **dsl firmware secondary** command enables you to select the secondary DSL firmware.

```
dsl firmware secondary
```

To revert to using the primary firmware, enter the **no** form of this command.

```
no dsl firmware secondary
```



Note

The router must retrain in order for the configuration changes to take effect. To retrain the line, you can unplug the DSL cable from the DSL socket on the back of the router and then plug the DSL cable back in again.

You can use the **show dsl interface atm number** command to compare firmware versions in use before retraining the DSL line, and after retraining.

Output Example

The following example output contains **show dsl interface atm** command output before the **dsl secondary firmware** command is added to the configuration.

```
827-sus2#sh dsl int atm0
                ATU-R (DS)                ATU-C (US)
Modem Status:   Showtime (DMTDSL_SHOWTIME)
DSL Mode:       ITU G.992.1 (G.DMT)
ITU STD NUM:    0x01                        0x01
Vendor ID:      'ALCB'                      'GSPN'
Vendor Specific:0x0000                      0x0002
Vendor Country: 0x00                        0x00
Capacity Used:  66%                         74%
Noise Margin:   16.5 dB                      17.0 dB
Output Power:   8.0 dBm                      12.0 dBm
Attenuation:    0.0 dB                       4.0 dB
Defect Status:  None                         None
Last Fail Code: None
Selftest Result:0x49
Subfunction:    0x02
Interrupts:     652 (1 spurious)
Activations:    1
SW Version:     3.8129
FW Version:     0x1A04
```

After the **dsl firmware secondary** command is added to the configuration and retraining, the **show dsl interface ATM0** output shows that the software version has changed to 3.7123.

```
827-sus2#sh dsl int atm0
                ATU-R (DS)                ATU-C (US)
Modem Status:   Showtime (DMTDSL_SHOWTIME)
DSL Mode:       ITU G.992.1 (G.DMT)
ITU STD NUM:    0x01                      0x01
Vendor ID:      'ALCB'                    'GSPN'
Vendor Specific:0x0000                    0x0002
Vendor Country: 0x00                      0x00
Capacity Used:  71%                       74%
Noise Margin:   18.0 dB                    17.0 dB
Output Power:   7.5 dBm                    12.0 dBm
Attenuation:    0.0 dB                     4.0 dB
Defect Status:  None                      None
Last Fail Code: None
Selftest Result:0x00
Subfunction:    0x02
Interrupts:     1206 (2 spurious)
Activations:    2
SW Version:     3.7123
FW Version:     0x1A04
```

Configuration Example

The following example shows configuration of a Cisco 827 router using secondary DSL firmware.

```
827-sus2#sh run
Building configuration...

Current configuration :738 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
no service dhcp
!
hostname 827-sus2
!
ip subnet-zero
no ip domain-lookup
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
interface Ethernet0
 ip address 192.168.5.23 255.255.255.0
 no cdp enable
 hold-queue 100 out
!
interface Virtual-Template1
 ip address 2.2.3.4 255.255.255.0
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 1/40
  encapsulation aal5mux ppp Virtual-Template1
!
dsl operating-mode itu-dmt
```

```
ds1 firmware secondary =====> New CLI
!
ip classless
ip http server
ip pim bidir-enable
!
line con 0
  exec-timeout 0 0
  stopbits 1
line vty 0 4
  login
!
scheduler max-task-time 5000
end

827-sus2#
```

Configuring FTP Client

The File Transfer Protocol (FTP) is an application protocol in the Internet protocol suite. It supports file transfers among unlike hosts in diverse internetworking environments. Using FTP, you can move a file from one computer to another, even if each computer runs a different operating system and uses a different file storage format. Cisco routers that can function as FTP clients can copy files from FTP servers into Flash memory.

When Cisco Router Web Setup (CRWS) software is installed on the router, it uses FTP to update the Cisco IOS image in Flash memory, and it configures the router with the FTP username and password that it requires.

**Caution**

CRWS is unable to perform automatic updates if the FTP username and password values it places in the configuration file are changed.

If you need to use FTP to manually copy system images to Flash memory, see the instructions for adding an FTP username and password to the configuration file at the following URL:

http://www.cisco.com/en/US/docs/ios/12_3/configfun/command/reference/cfr_1g04.html#wp1081630

