CHAPTER 5

Configuring the Layer 2 Tunnel Protocol Access Concentrator and Network Server

The Cisco 10000 series router supports the Layer 2 Tunnel Protocol (L2TP) to allow users and telecommuters to connect to their corporate intranets or extranets. The Cisco 10000 series router supports the Layer 2 access concentrator (LAC) and Managed L2TP network server features. These features enable the Cisco 10000 series router to act as either a LAC or an LNS device.

Acting as the LAC, the Cisco 10000 router uses L2TP tunnels to forward packets to the LNS. As the LNS, the Cisco 10000 series router terminates and routes subscriber sessions into the appropriate virtual routing and forwarding (VRF) instance.

This chapter describes the following features:

IP Reassembly

The Cisco 10000 series router supports the IP Reassembly feature on the fastpath. This feature reassembles fragments of IP and L2TP encapsulated packets.

The IP Reassembly feature on the fastpath reassembles IP packets that have two IPv4 non-overlapping no-option fragments and drops two fragment overlapping fragments. The Route Processor (RP) handles packets with options, non-IPv4 packets, and packets with three or more fragments. If input security ACLs are configured, IP Reassembly processes the ACLs on the fragments and also on the reassembled packet.

Intermediate routers fragments an IP datagram if the outgoing maximum transmission unit (MTU) is lower than the packet size. The receiving host is responsible for reassembling the datagram from the fragments. When configured as a LAC, LNS, or tunnel switch, the Cisco 10000 series router is the receiving host for the tunneled packets. If one of the intermediate routers fragments L2TP encapsulated packets in transit through the tunnel, the IP Reassembly feature reassembles the packets.

Feature History for IP Reassembly

Cisco IOS Release	Description	Required PRE
12.3(7)XI1	This feature was integrated into Cisco IOS Release 12.3(7)XI1.	PRE2
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.	PRE2

Layer 2 Access Concentrator

The Cisco 10000 series router supports the Layer 2 access concentrator (LAC) feature. When configured as the LAC, the Cisco 10000 series router functions as the service provider's network access server. Remote subscribers use a local or point-to-point connection to initiate a PPPoA or PPPoE session to the LAC. The LAC terminates the physical connection and forwards the PPP session to the provider's Layer 2 Tunnel Protocol network server (LNS).

The LAC connects to the LNS using a local area network or a wide area network such as public or private ATM. The LAC directs subscriber sessions into Layer 2 Tunnel Protocol (L2TP) tunnels based on the domain of each session. The LAC acts as one side of an L2TP tunnel endpoint and is a peer to the LNS on the other side of the tunnel. The LAC forwards packets to and from the LNS and a remote system.

Acting as the LNS, you can configure the Cisco 10000 series router to terminate the PPP sessions and route the client IP packets onto the ISP or corporate network toward their final destination (Figure 5-1). You can also configure the LNS to place the sessions in VRFs before routing the packets, as shown in Figure 5-2.

The LAC feature is described in the following topics:

Figure 5-1 Terminating and Forwarding Sessions from the LAC

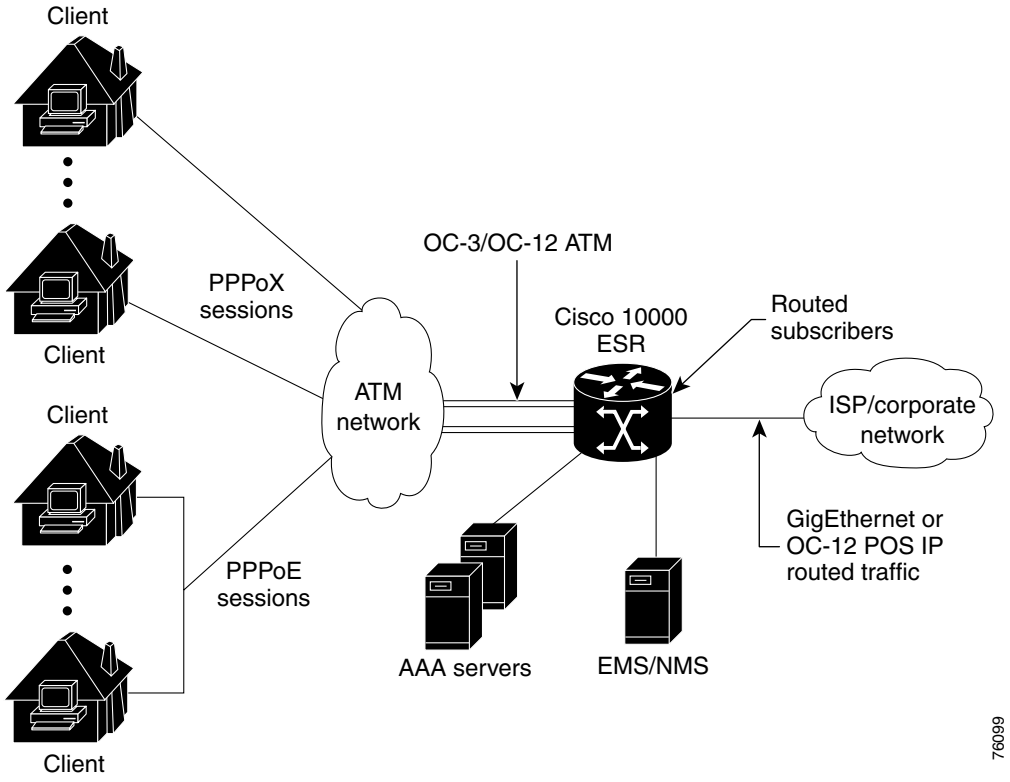
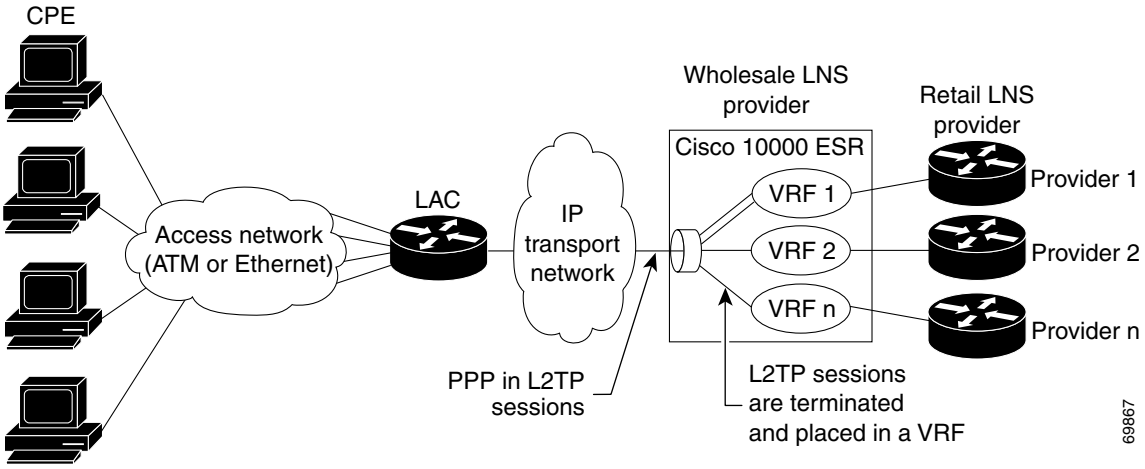


Figure 5-2 Placing Sessions from the LAC in VRFs



Tunnel Sharing

The tunnel sharing feature enables sessions that are authorized with different domains to share the same tunnel. Tunnel sharing reduces the number of tunnels required from the LAC. When used with the L2TP multihop feature, tunnel sharing also reduces the number of tunnels to an LNS. While improving tunnel management, tunnel sharing helps to reduce the number of tunnel establishment messages that are sent after interface dropouts, reducing dropout recovery time.

Note The session per tunnel limiting feature, when configured, limits the number of PPP sessions from multiple domain names that can be forwarded in a single tunnel.

The **domain** *domain-name* command in request-dialin or virtual private dial network (VPDN) group configuration mode requests that the LAC tunnel PPP sessions from a specific *domain-name*. Applying multiple instances of this command in a VPDN group or subgroup enables the LAC to forward PPP sessions from any of the specified domains in the same tunnel.

Tunnel Service Authorization

The tunnel service authorization feature allows the service provider to limit the number of destinations a subscriber can choose and to charge a fee for each destination allowed. The LAC can conduct static or dynamic tunnel service authorization.

A static domain name on an ATM PVC port overrides the domain name that the client session supplies. Static tunnel service authorization does not support switched virtual circuits (SVCs).

If a static domain is not configured, the LAC conducts dynamic tunnel service authorization. During dynamic tunnel service authorization, the LAC performs the following steps:

1. Domain Preauthorization—Checks the client-supplied domain name (in the PPP username) against an authorized list configured on the RADIUS server for each PVC.

   If the domain name is on the authorized list, the LAC proceeds to tunnel service authorization.

   If the domain name is not on the authorized list, the LAC attempts PPP authentication and authorization for local termination. The **vpdn authorize domain** command configures the domain preauthorization feature.
2. Tunnel Service Authorization—Checks the client-supplied domain name against a list of domains provided in the user profile on the RADIUS server to determine the domains accessible to the user. Enables tunnel service authorization and establishes an L2TP tunnel.

The following sections discuss tunnel selection as it relates to tunnel service authorization.

Tunnel Selection

When configured as the LAC, the Cisco 10000 series router selects a tunnel for an incoming PPP session using the following features:

- Static tunnel selection
- Per user tunnel selection
- Dynamic tunnel selection

Static Tunnel Selection

The static tunnel selection feature specifies a domain name for a PVC on an ATM interface. The LAC uses the specified domain name to select a tunnel for all PPP sessions originating from the PVC. This feature ignores the domains subscribers indicate in their usernames and forces the subscribers to a specific destination.

The **vpn service** *domain-name* command in ATM VC configuration mode configures the *domain-name* on the specified PVC. The **vpn service** *domain-name* command in ATM VC class configuration mode configures the *domain-name* on all virtual circuits in the VC class.

Per User Tunnel Selection

The per user tunnel selection feature specifies that the LAC use the entire structured PPP username to select a tunnel for forwarding an incoming session. Instead of sending the domain name, the LAC sends the entire structured PPP username to the authentication, authorization, and accounting (AAA) server. The AAA server provides the VPDN tunnel attributes for the user, indicating which tunnel the LAC can use to forward the session.

The **authen-before-forward** command in VPDN group configuration mode configures the per user tunnel selection feature.

Note When tunneling from a LAC to an LNS using L2TP, when you use the **authen-before-forward** command to configure the LAC to authenticate the user to RADIUS before negotiating a tunnel with the LNS, the user is authenticated and the LAC uses RADIUS information to determine if it should terminate a PPPoX session as PPP terminated aggregation (PTA) or forward the session to the LNS.

Dynamic Tunnel Selection

The dynamic tunnel selection feature enables the LAC to use the client-supplied domain in the PPP username to select a tunnel for forwarding an incoming session. You must configure a VPDN group on the LAC for each possible domain that a user might indicate.

Note You can restrict a user from certain domains by using domain preauthorization and tunnel service authorization. For more information, see the "Tunnel Service Authorization" section on page 5-4.

Sessions per Tunnel Limiting

The sessions per tunnel limiting feature specifies the maximum number of sessions initiated within an L2TP tunnel. The **initiate-to ip** command in VPDN group configuration mode configures the session per tunnel limiting feature. The command syntax is:

```
initiate-to ip ipaddress [limit limit-number] [priority priority-number]
```

Because the sessions per tunnel limiting feature enables you to specify the maximum number of VPDN sessions terminating at any L2TP network server (LNS), you can keep corporate router utilization at a more predictable level.

Session Load Balancing

The session load balancing feature enables the LAC to direct sessions across multiple LNS devices. The LAC retrieves L2TP tunnel (VPDN) information from local configuration or a RADIUS server. Both configuration methods support load balancing, but using RADIUS is more scalable than the local method. When you enable the session load balancing feature using RADIUS, the server sends L2TP tunnel information using multiple Tunnel-Server-Endpoint attributes in one tagged attribute group.

Multiple instances of the **initiate-to ip** command in VPDN group configuration mode configures the session load balancing feature locally. For information on the command syntax, see the "Sessions per Tunnel Limiting" section on page 5-5.

When you enable the session load balancing feature, the LAC uses a priority or round-robin load balancing algorithm to forward PPP sessions destined to the same domain among multiple tunnels.

Note Load balancing occurs with respect to the load a particular LAC generates. The LAC is not aware of the true load on a set of LNS devices. The true load on the LNS devices is an aggregation of all LAC devices using the LNS devices.

Session Load Failover

The session load failover feature works with the session load balancing feature to enable the LAC to direct sessions across multiple LNS devices. If the primary set of LNS devices fails, the session load failover feature enables the LAC to direct sessions to a set of failover LNS devices. The LAC uses the failover LNS devices only if *all* of the primary set of devices are unavailable. Failover occurs if the LAC:

- Sends an excessive number of Start-Control-Connection-Requests (SCCRQs) (no response from peer)
- Receives a Stop Control Channel (StopCNN) message from its peer during tunnel establishment
- Receives a Call-Disconnect-Notify (CDN) message during session establishment
- Receives vendor-specific attributes (VSAs) or standard RADIUS AV pairs indicating failover

The RADIUS Tunnel-Preference attribute is used to form load failover groups. When the values of the Tunnel-Preference attributes for different tagged attribute groups are the same, the Tunnel-Server-Endpoint for each of those attribute groups has the same failover priority.

Feature History for LAC

Cisco IOS Release	Description	Required PRE
12.2(15)BX	This feature was introduced on the Cisco 10000 series router.	PRE2
12.3(7)XI1	This feature was integrated into Cisco IOS Release 12.3(7)XI1.	PRE2
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.	PRE2

Restrictions for LAC

When configured as a LAC device, the Cisco 10000 series router has the following restrictions:

- The L2TP LAC per session features do not support PPP quality of service (QoS) and security access control lists (ACLs).
- The Cisco 10000 series router does not support the configuration of L2TP tunnels over the management Fast Ethernet interface. Do not set up L2TP tunnels over this interface.

Required Configuration Tasks for LAC

To configure the Cisco 10000 series router to act as a LAC, perform the following required configuration task:

- Enabling the LAC to Look for Tunnel Definitions, page 5-7

Enabling the LAC to Look for Tunnel Definitions

To enable the LAC to look for tunnel definitions, you must enable the VPDN feature on the LAC. To enable VPDN, enter the following commands:

	Command	Purpose
Step 1	`Router> enable`	Enters privileged EXEC mode.
Step 1	`Router# config terminal`	Enters global configuration mode.
Step 1	`Router(config)# vpdn enable`	Enables VPDN networking on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
Step 2	`Router(config)# vpdn-group` *group-name*	Defines a local group name for which you can assign other VPDN variables. Enters VPDN group configuration mode.
Step 3	`Router(config-vpdn)# request-dialin`	Enables the LAC to request L2TP tunnels to the Cisco 10000 router and enters VPDN request-dialin group mode.
Step 4	`Router(config-vpdn-req-in)# protocol l2tp`	Specifies the Layer 2 Tunnel Protocol.
Step 5	`Router(config-vpdn-req-in)# exit`	Returns to VPDN group configuration mode.
Step 6	`Router(config-vpdn)# initiate-to ip` *ip-address* [`priority` *priority-number*]	Specifies the LNS IP address and optionally the priority of the IP address (1 is the highest).

Optional Configuration Tasks for LAC

To configure the Cisco 10000 series router as a LAC, perform any of the following optional tasks:

- Enabling Sessions with Different Domains to Share the Same Tunnel, page 5-8
- Enabling the LAC to Conduct Tunnel Service Authorization, page 5-8
- Configuring Sessions Per Tunnel Limiting on the LAC, page 5-12

Enabling Sessions with Different Domains to Share the Same Tunnel

To enable sessions authorized with different domains to share the same tunnel, enter the following commands:

	Command	Purpose
Step 1	`Router> enable`	Enters privileged EXEC mode.
Step 2	`Router# config terminal`	Enters global configuration mode.
Step 3	`Router(config)# vpdn-group group-name`	Defines a local group name for which you can assign other VPDN variables. Enters VPDN group configuration mode.
Step 4	`Router(config-vpdn)# request-dialin`	Enables the LAC to request L2TP tunnels to the Cisco 10000 series router and enters VPDN request-dialin group mode.
Step 5	`Router(config-vpdn-req-in)# protocol l2tp`	Specifies the Layer 2 Tunnel Protocol.
Step 6	`Router(config-vpdn-req-in)# domain domain-name`	Requests that PPP calls from the specified domain be tunneled. **Note** For multiple domains over the same tunnel, repeat this step to list all of the domains you want that tunnel to support. To configure the same domain over multiple tunnels, you must configure load balancing and sharing between the tunnels by using the **loadsharing ip** *ip-address* [**limit** *session-limit*] command in VPDN group configuration mode.
Step 7	`Router(config-vpdn-req-in)# exit`	Returns to VPDN group configuration mode.
Step 8	`Router(config-vpdn)# initiate-to ip ip-address [priority priority-number]`	Specifies the LNS IP address and optionally the priority of the IP address (1 is the highest).

Verifying Tunnel Sharing Configuration on the LAC

To verify tunnel sharing configuration on the LAC, enter the following command in privileged EXEC mode:

Command	Purpose
`Router# show running-config`	Displays the running configuration and allows you to check that you successfully enabled the tunnel sharing feature.

Enabling the LAC to Conduct Tunnel Service Authorization

To enable the LAC to conduct static or dynamic tunnel service authorization, perform the following tasks:

- Configuring a Static Domain Name on a Permanent Virtual Circuit, page 5-8 or Configuring a Static Domain Name on a Virtual Circuit Class, page 5-10
- Enabling Domain Preauthorization, page 5-11
- Configuring the LAC to Communicate with the RADIUS Server, page 5-11

Configuring a Static Domain Name on a Permanent Virtual Circuit

To configure a static domain name on a permanent virtual circuit (PVC), enter the following commands:

	Command	Purpose
Step 1	`Router> enable`	Enters privileged EXEC mode.
Step 2	`Router# config terminal`	Enters global configuration mode.
Step 3	`Router(config)# interface atm 0/0/0[.subinterface-number] {multipoint | point-to-point | tag-switching}`	Specifies the ATM interface and optional subinterface.
Step 4	`Router(config-subif)# atm pppatm passive`	Places the sessions on the subinterface in passive (listening) mode.
Step 5	`Router(config-subif)# no ip directed-broadcast`	Disables forwarding of directed broadcasts.
Step 6	`Router(config-subif)# pvc [name] vpi/vci`	Configures a PVC on the ATM interface or subinterface.
Step 7	`Router(config-if-atm-vc)# encapsulation aal5mux ppp Virtual-Template number`	Configures the ATM adaptation layer (AAL) and encapsulation type for an ATM PVC, SVC, VC class, or VC bundle. **mux ppp** is for a MUX-type VC running IETF-compliant PPP over ATM. You must use the **Virtual-Template** *number* argument to identify the virtual template. The **mux ppp** keyword applies to ATM PVCs only.
Step 8	`Router(config-if-atm-vc)# vpn service domain-name`	Configures the static domain name on the PVC.

Example 5-1 shows the static domain names *net1.com* and *net2.com* assigned to PVCs on an ATM interface. All PPP sessions originating from PVC 30/33 are sent to the *net1.com* L2TP tunnel. All PPP sessions originating from PVC 30/34 are sent to the *net2.com* tunnel.

Example 5-1 Configuring a Static Domain Name on a Permanent Virtual Circuit

```
!
interface ATM 0/0/0.33 multipoint
    atm pppatm passive
    pvc 30/33
        encapsulation aa15ciscoppp Virtual-Template1
        vpn service net1.com
    !
    pvc 30/34
        encapsulation aa15ciscoppp Virtual-Template1
        vpn service net2.com
    !
```

Configuring a Static Domain Name on a Virtual Circuit Class

To configure a static domain name on a VC class, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router> enable`	Enters privileged EXEC mode.
Step 2	`Router# config terminal`	Enters global configuration mode.
Step 3	`Router(config)# vc-class atm` *vc-class-name*	Creates and names a map class.
Step 4	`Router(config-vc-class)# encapsulation aal5mux ppp Virtual-Template` *number*	Configures the ATM adaptation layer (AAL) and encapsulation type for an ATM PVC, SVC, VC class, or VC bundle. **mux ppp** is for a MUX-type VC running IETF-compliant PPP over ATM. You must use the **Virtual-Template** *number* argument to identify the virtual template. The **mux ppp** keyword applies to ATM PVCs only.
Step 5	`Router(config-vc-class)# vpn service` *domain-name*	Configures the static domain name on the VC class.
Step 6	`Router(config-vc-class)# exit`	Returns to global configuration mode.
Step 7	`Router(config)# interface atm 0/0/0`[*.subinterface-number*] {**multipoint** | **point-to-point** | **tag-switching**}	Specifies the ATM interface and optional subinterface.
Step 8	`Router(config-subif)# atm pppatm passive`	Places the sessions on the subinterface in passive (listening) mode.
Step 9	`Router(config-subif)# class-int` *vc-class-name*	Applies the VC class to all VCs on the ATM interface or subinterface.

In Example 5-2, the static domain name *net.com* is assigned to a VC class. The VC class is then assigned to the VCs on an ATM subinterface.

Example 5-2 Configuring a Static Domain Name on a VC Class

```
!
vc-class ATM MyClass
    encapsulation aal5ciscoppp Virtual-Template1
    vpn service net.com
    !
interface ATM 0/0/0.99 multipoint
    atm pppatm passive
    class-int MyClass
    no ip directed-broadcast
    pvc 20/40
    pvc 30/33
    !
```

Verifying the Static Domain Name

To verify that you successfully configured the static domain name, enter the **show running-config** command in privileged EXEC mode.

Enabling Domain Preauthorization

To enable the LAC to perform domain authorization before tunneling, enter the following commands:

	Command	Purpose
Step 1	`Router> enable`	Enters privileged EXEC mode.
Step 2	`Router# config terminal`	Enters global configuration mode.
Step 3	`Router(config)# vpdn authorize domain`	Enables domain preauthorization.

Example 5-3 Enabling Domain Preauthorization

```
!
aaa new-model
aaa authorization network default local group radius
!
vpdn authorize domain
!
radius-server host 10.16.9.9 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
radius-server key MyKey
radius-server vsa send authentication
!
```

Verifying Domain Preauthorization

To verify that you successfully enabled domain preauthorization, enter the following commands:

Command	Purpose
`Router# show running-config`	Verifies that you successfully configured the maximum number of sessions per tunnel.
`Router# show vpdn tunnel`	Verifies active L2TP tunnel information in a VPDN environment.
`Router# show vpdn session`	Verifies active L2TP sessions in a VPDN environment.

Configuring the LAC to Communicate with the RADIUS Server

To enable the LAC to communicate properly with the RADIUS server for tunnel service authorization, enter the following commands:

	Command	Purpose
Step 1	`Router> enable`	Enters privileged EXEC mode.
Step 2	`Router# config terminal`	Enters global configuration mode.
Step 3	`Router(config)# radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number]`	Specifies the RADIUS server host.
Step 4	`Router(config)# radius-server retransmit retries`	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up. The default number of retries is 3 attempts.

	Command	Purpose
Step 5	`Router(config)# radius-server attribute 44 include-in-access-req vrf` *vrf-name*	Sends RADIUS attribute 44 (Accounting Session ID) in access request packets before user authentication (including requests for preauthentication).
Step 6	`Router(config)# radius-server domain-stripping vrf` *vrf-name*	(Optional) Enables VRF-aware domain-stripping. The **vrf** *vrf-name* argument specifies the per VRF configuration.
Step 7	`Router(config)# radius-server attribute list` *list-name*	Defines the list name given to the set of attributes defined using the **attribute** command.
Step 8	`Router(config)# radius-server key` *string*	Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
Step 9	`Router(config)# radius-server vsa send authentication`	Configures the LAC to recognize and use vendor-specific attributes.

Example 5-4 Configuring Communication with the RADIUS Server

```
!
aaa new-model
aaa authorization network default local group radius
!
radius-server host 10.16.9.9 auth-port 1645 acct-port 1646
radius-server attribute 44 include-in-access-req vrf vrf1
radius-server key MyKey
radius-server vsa send authentication
```

Verifying Communication with the RADIUS Server

To verify that you successfully configured the LAC to communicate properly with the RADIUS server for tunnel service authorization, enter the **show running-config** command in privileged EXEC mode.

Configuring Sessions Per Tunnel Limiting on the LAC

To limit the number of sessions per tunnel without using a RADIUS server, enter the following commands.

Note You can configure the LAC or the RADIUS server to limit the number of sessions per tunnel. For information on using the RADIUS server for sessions per tunnel limiting, see the "Configuring Sessions Per Tunnel Limiting in the RADIUS Service Profile" section on page 5-16.

	Command	Purpose
Step 1	`Router> enable`	Enters privileged EXEC mode.
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# vpdn-group` *group-name*	Defines a local group name for which you can assign other VPDN variables. Enters VPDN group configuration mode.
Step 4	`Router(config-vpdn)# request-dialin`	Enables the LAC to request L2TP tunnels to the LNS and enters VPDN request-dialin group mode.
Step 5	`Router(config-vpdn-req-in)# protocol l2tp`	Specifies the Layer 2 Tunnel Protocol.

	Command	Purpose
Step 6	`Router(config-vpdn-req-in)# domain domain-name`	Initiates a tunnel based on the client-supplied domain name.
Step 7	`Router(config-vpdn-req-in)# exit`	Returns to VPDN group mode.
Step 8	`Router(config-vpdn)# initiate-to ip ip-address limit limit-number [priority priority-number]`	Specifies the LNS IP address, the maximum number of sessions per tunnel, and optionally the priority of the IP address (1 is the highest).

Verifying Sessions Per Tunnel Limiting on the LAC

To verify sessions per tunnel limiting on the LAC, enter the following commands:

Command	Purpose
`Router# show running-config`	Verifies that you successfully configured the maximum number of sessions per tunnel.
`Router# show vpdn tunnel`	Verifies that the number of displayed sessions does not exceed your configured limit.

Example 5-5 Verifying Sessions Per Tunnel Limiting on the LAC

```
Router> enable
Router# show vpdn tunnel

L2TP Tunnel Information (Total tunnels 50 sessions 2000)

LocIDRemIDRemote NameStateRemote AddressPortSessions
412347811LNS1est10.16.1.1170140
200222323LNS1est10.16.1.1170140
412347811LNS2est10.16.2.2170140
597653477LNS2est10.16.3.3170140
!
!
```

RADIUS Server Optional Configuration Tasks for LAC

To configure the optional RADIUS server for the LAC, perform any of the following optional tasks:

- Enabling Tunnel Sharing for RADIUS Services, page 5-13
- Enabling the RADIUS Server to Conduct Tunnel Service Authorization, page 5-14
- Configuring Sessions Per Tunnel Limiting in the RADIUS Service Profile, page 5-16

Enabling Tunnel Sharing for RADIUS Services

To configure tunnel sharing in the RADIUS service profile, enter the following Cisco-AV pair attributes in the profile:

- vpdn-group
- tunnel-share

VPDN Group

The vpdn-group attribute specifies the group to which the service belongs. All services with matching group names are considered members of the same VPDN group. This attribute has the following syntax:

```
Cisco-AVpair="vpdn:vpdn-group=group-name"
```

group-name is the group to which the service belongs.

Example 5-6 VPDN Group—RADIUS Freeware Format

```
Cisco-AVpair="vpdn:vpdn-group=group1"
```

Tunnel Share

The tunnel-share attribute indicates that the tunnel sharing feature is enabled for the service.

Example 5-7 Tunnel Share—RADIUS Freeware Format

```
Cisco-AVpair="vpdn:tunnel-share=yes"
```

Verifying the Tunnel Sharing Configuration in the RADIUS Service Profile

To verify the RADIUS service profile, see the user documentation for your RADIUS server.

Enabling the RADIUS Server to Conduct Tunnel Service Authorization

To enable the RADIUS server to conduct dynamic tunnel service authorization, perform the following tasks:

- Configuring the RADIUS User Profile for Domain Preauthorization, page 5-14
- Configuring the RADIUS Service Profile for Tunnel Service Authorization, page 5-15

Configuring the RADIUS User Profile for Domain Preauthorization

To enable domain preauthorization, enter the following configuration parameters in the user profile on the RADIUS server:

RADIUS Entry	Purpose
nas-port:*ip-address*:*slot*/*subslot*/*port*/*vpi*.*vci*	Configures the NAS port username for domain preauthorization. The *ip-address* argument is the management IP address of the network service provider (NSP). The *slot*/*subslot*/*port* argument specifies the ATM interface. The *vpi*.*vci* arguments are the VPI and VCI values for the PVC.
`Password = "cisco"`	Sets the fixed password.
`User-Service-Type = Outbound-User`	Configures the service-type as outbound.
Cisco-AVpair = "vpdn:vpn-domain-list=domain1, domain2,..."	Specifies the domains accessible to the user.

Example 5-8 Configuring the RADIUS User Profile for Domain Preauthorization

```
user = nas-port:10.16.9.9:0/0/0/30.33{
    profile_id = 826
    profile_cycle = 1
    radius=Cisco {
    check_items = {
    2=cisco
    }
    reply_attributes= {
    9, 1="vpdn:vpd-domain-list=net1.com,net2.com"
```

Verifying the RADIUS User Profile for Domain Preauthorization

To verify the RADIUS user profile, see your RADIUS server user documentation.

Configuring the RADIUS Service Profile for Tunnel Service Authorization

To enable tunnel service authorization, enter the following configuration parameters in the service profile on the RADIUS server:

RADIUS Entry	Purpose
`domain` **`Password "cisco"`**	Sets the fixed password.
`User-Service-Type = Outbound-User`	Configures the service-type as outbound.
`Cisco-AVpair = "vpdn:tunnel-id=`*`name`***`"`**	Specifies the name of the tunnel that must match the LNS's VPDN terminate-from hostname.
`Cisco-AVpair = "vpdn:12tp-tunnel-password=`*`secret`***`"`**	Specifies the secret (password) for L2TP tunnel authentication.
`Cisco-AVpair = "vpdn:tunnel-type=12tp"`	Specifies Layer 2 Tunnel Protocol.
`Cisco-AVpair = "vpdn:ip-addresses=`*`ip-address`***`"`**	Specifies the IP address of the LNS.

Example 5-9 Configuring the RADIUS Service Profile for Tunnel Service Authorization

```
user = net1.com{
profile_id = 45
profile_cycle = 18
member = me
radius=Cisco {
check_items= [
2=cisco
}
reply_attributes= {
9,1="vpdn:tunnel-id=LAC-1"
9,1="vpdn:12tp-tunnel_password=MySecret"
9,1="vpdn:tunnel-type=12tp"
9,1="vpdn:ip-addresses=10.16.10.10"
6=5
}
}
}
```

Verifying the RADIUS Service Profile for Tunnel Service Authorization

To verify the RADIUS service profile, see your RADIUS server user documentation.

Configuring Sessions Per Tunnel Limiting in the RADIUS Service Profile

To use a RADIUS server to limit the number of sessions per tunnel, enter the following Cisco-AVpair attributes in the RADIUS service profile:

- vpdn:ip-addresses
- vpdn:ip-address-limits

Note You can configure the RADIUS server or the LAC to limit the number of sessions per tunnel. For information on using the LAC for sessions per tunnel limiting, see the "Configuring Sessions Per Tunnel Limiting on the LAC" section on page 5-12.

VPDN IP Addresses

The vpdn:ip-addresses attribute specifies the IP addresses of the LNS devices to receive the L2TP connections. It has the following syntax:

Cisco-AVpair = "vpdn:ip-addresses=*address1*[<*delimiter*>*address2*][<*delimiter*>*address3*]...**"**

The *address* argument is the IP address of the LNS.

The <*delimiter*>**,** (comma) and <*delimiter*> (space) arguments select load sharing among IP addresses.

The <*delimiter*>**/** (slash) argument groups IP addresses on the left side in higher priority than the right side.

Example 5-10 VPDN IP Addresses—RADIUS Freeware Format

In the following example, the LAC sends the:

- First PPP session through a tunnel to 10.16.1.1
- Second PPP session to 10.16.2.2
- Third PPP session to 10.16.3.3
- Fourth PPP session to 10.16.1.1

If the LAC fails to establish a tunnel with any of the IP addresses in the first group, it attempts to connect to the IP addresses in the second group (10.16.4.4 and 10.16.5.5).

```
Cisco-AVpair="vpdn:ip-addresses=10.16.1.1,10.16.2.2,10.16.3.3/10.16.4.4,10.16.5.5"
```

VPDN IP Address Limits

The vpdn:ip-address-limits attribute specifies the maximum number of sessions in each tunnel to the IP addresses listed with the attribute. It has the following syntax:

Cisco-AVpair = "vpdn:ip-address-limits=*limit1*[*limit2*][*limit3*]...**"**

The *limit* argument is the maximum number of sessions per tunnel to the corresponding IP address.

Example 5-11 VPDN IP Address Limits—RADIUS Freeware Format

```
Cisco-AVpair="vpdn:ip-address-limits=10 20 30 40 50 "
.1.1.1,10.2.2.2,10.3.3.3/10.4.4.4,10.5.5.5"
```

Note You must enter a space between the final *limit* entry and the end quotation marks.

Verifying Sessions Per Tunnel Limiting in the RADIUS Service Profile

To verify the RADIUS service profile, see the user documentation for your RADIUS server.

Configuration Example for LAC

The following example is a basic LAC configuration in which the LNS authenticates the PPP sessions.

```
Current configuration : 4882 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c10k_mc_10005_1
!
no logging console
aaa new-model
!
!
aaa session-id common
enable password lab
!
username LAC1-1 nopassword
username LNS1-1 nopassword
no spd enable
facility-alarm intake-temperature major 49
facility-alarm intake-temperature minor 40
facility-alarm core-temperature major 53
facility-alarm core-temperature minor 45
card 1/0 1gigethernet-1
card 2/0 1oc12atm-1
card 3/0 1oc12atm-1
card 4/0 4oc3atm-1
card 5/0 1gigethernet-1
ip subnet-zero
no ip gratuitous-arps
ip host zeppelin-2 1.0.0.253
ip host zeppelin-3 1.0.0.253
!
vpdn enable
!
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
 pppoe limit per-mac 32000
 pppoe limit per-vc 32000
!
vpdn-group LAC_1
 request-dialin
  protocol l2tp
  domain hello1
 initiate-to ip 103.1.1.2
 local name LAC1-1
 l2tp tunnel password 7 06121A2F424B05
!
!
```

```
buffers small permanent 15000
buffers middle permanent 12000
buffers large permanent 1000
!
interface Loopback1
 no ip address
!
interface FastEthernet0/0/0
 ip address 23.3.6.3 255.255.0.0
 full-duplex
!
interface GigabitEthernet1/0/0
 no ip address
 no ip mroute-cache
 negotiation auto
 hold-queue 4096 in
 hold-queue 4096 out
!
interface GigabitEthernet1/0/0.101
 encapsulation dot1Q 101
 ip address 103.1.1.1 255.255.255.0
!
interface ATM2/0/0
 no ip address
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-4
 no atm auto-configuration
 no atm ilmi-keepalive
 no atm address-registration
 no atm ilmi-enable
!
interface ATM3/0/0
 atm pppatm passive
 no ip address
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-4
 no atm auto-configuration
 no atm ilmi-keepalive
 no atm address-registration
 no atm ilmi-enable
!
interface ATM3/0/0.41101 point-to-point
 atm pppatm passive
 pvc 41/101
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41102 point-to-point
 pvc 41/102
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41103 point-to-point
 pvc 41/103
  encapsulation aal5snap
  protocol pppoe
 !
!
```

```
interface ATM3/0/0.41104 point-to-point
 pvc 41/104
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41105 point-to-point
 pvc 41/105
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41106 point-to-point
 pvc 41/106
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41107 point-to-point
 pvc 41/107
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41108 point-to-point
 pvc 41/108
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41109 point-to-point
 pvc 41/109
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41110 point-to-point
 pvc 41/110
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41111 point-to-point
 pvc 41/111
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41112 point-to-point
 pvc 41/112
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41113 point-to-point
 pvc 41/113
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41114 point-to-point
 pvc 41/114
  encapsulation aal5snap
  protocol pppoe
```

```
 !
!
interface ATM3/0/0.41115 point-to-point
 pvc 41/115
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41116 point-to-point
 pvc 41/116
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41117 point-to-point
 pvc 41/117
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41118 point-to-point
 pvc 41/118
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41119 point-to-point
 pvc 41/119
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41120 point-to-point
 pvc 41/120
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41121 point-to-point
 pvc 41/121
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41122 point-to-point
 pvc 41/122
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41123 point-to-point
 pvc 41/123
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/0/0.41124 point-to-point
 pvc 41/124
  encapsulation aal5snap
  protocol pppoe
 !
!
```

```
interface ATM4/0/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM4/0/1
 no ip address
 no atm ilmi-keepalive
!
interface ATM4/0/2
 no ip address
 no atm ilmi-keepalive
!
interface ATM4/0/3
 no ip address
 no atm ilmi-keepalive
!
interface GigabitEthernet5/0/0
 no ip address
 negotiation auto
!
interface Virtual-Template1
 ip unnumbered Loopback1
 keepalive 30
 no peer default ip address
 ppp authentication pap
!
ip default-gateway 23.3.0.4
ip classless
ip route 1.0.0.253 255.255.255.255 23.3.0.4
no ip http server
ip pim bidir-enable
!
no cdp run
!
radius-server retransmit 3
radius-server authorization permit missing Service-Type
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
end
```

Monitoring and Maintaining LAC

To monitor and maintain the LAC, enter the following commands in privileged EXEC mode:

Command	Purpose
`Router# show running-config`	Displays the current configuration of the Cisco 10000 series router, acting as the LAC device. This command is useful in verifying that you successfully configured the LAC features, such as the maximum number of sessions per tunnel, the static domain name, and the LAC to RADIUS communication for tunnel service authorization

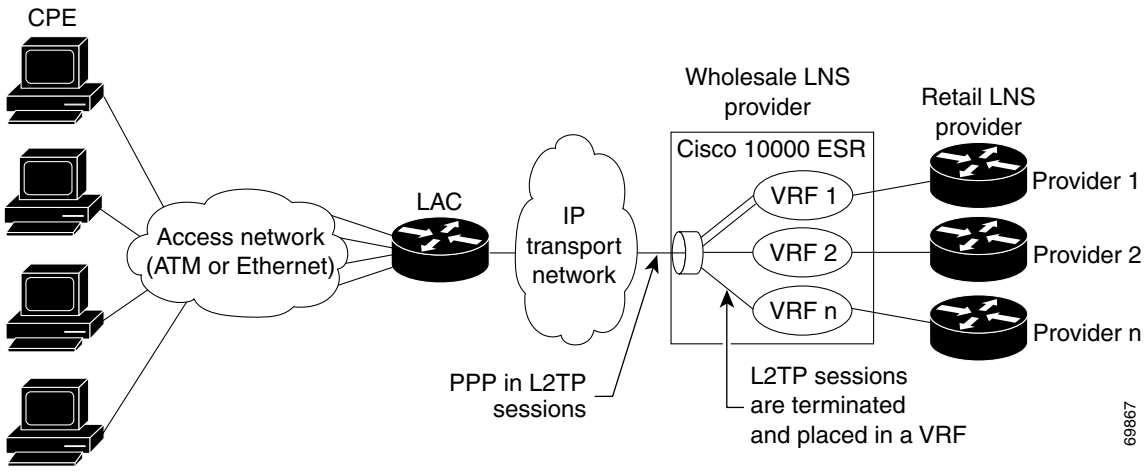
Command	Purpose
`Router# show vpdn session`	Verifies active L2TP sessions in a VPDN environment.
`Router# show vpdn tunnel`	Verifies active L2TP tunnel information in a VPDN environment.

L2TP Network Server

The Cisco 10000 series router can function as an L2TP network server (LNS). By using the managed LNS features introduced in Cisco IOS Release 12.2(4)BZ1, the Cisco 10000 series router terminates L2TP sessions from the LAC and places each session into the appropriate VRF instance based on the L2TP tunnel the session arrived in. The Cisco 10000 router then routes each session within the VRF to the destination network.

The LNS is a peer to the LAC and sits on one side of an L2TP tunnel. The LNS routes packets to and from the LAC and a destination network. Acting as the LNS, you can configure the Cisco 10000 series router to terminate the PPP sessions and route the client IP packets onto the ISP or corporate network toward their final destination (see Figure 1-1 on page 1-3). You can also configure the LNS to place the sessions in VRFs before routing the packets, as shown in Figure 5-3.

Figure 5-3 Managed LNS Topology



All of a service provider's subscribers do not share the same L2TP trunk interface. Typically, the Cisco 10000 router uses virtual local area networks (VLANs) to separate a service provider's subscriber traffic. The Cisco 10000 series router can also use permanent virtual circuits (PVCs) or a separate physical interface for each provider to separate traffic. A virtual template interface configures the user sessions in a tunnel and applies to all users in the same VRF.

The LNS feature is described in the following topics:

- Virtual Template Interface, page 5-23
- Virtual Routing and Forwarding Instance, page 5-23
- Per VRF AAA, page 5-23
- Private Servers, page 5-24
- RADIUS Attribute Screening, page 5-24
- Packet Fragmentation, page 5-24

Virtual Template Interface

The virtual template interface is a logical entity that the Cisco 10000 series router applies dynamically as needed to a connection. It is a configuration for an interface, but it is not tied to the physical interface. It is used to create and configure a virtual interface known as a virtual access interface (VAI). The VAI is cloned from the virtual template interface, used on demand, and then freed when no longer needed.

For example, when a remote user initiates a PPP session to the Cisco 10000 series router, the predefined configuration template is used to configure a VAI. The VAI is created and configured dynamically using the virtual template interface. Using AAA, RADIUS attributes can further define the VAI configuration.

The VAI uses the attributes of the virtual template to create the session, which results in a VAI that is uniquely configured for a specific user. When the user is done, the VAI goes down and the resources are freed for other client uses.

Virtual Routing and Forwarding Instance

A virtual routing and forwarding (VRF) instance includes the routing information that defines a customer VPN site that is attached to a provider edge (PE) router, such as the Cisco 10000 series router. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table.

To configure a VRF instance, enter the **rd** command in VRF configuration submode to specify the correct route distinguisher (RD) used for the VPN. The RD extends the IP address so that you can identify the VPN to which it belongs.

Per VRF AAA

The per VRF AAA feature enables you to partition authentication, authorization, and accounting (AAA) services based on a VRF instance. To support the per VRF AAA feature, the RADIUS server must be VRF aware.

To be VRF aware, ISPs must define multiple instances of the same operational parameters and secure them to the VRF partitions. Securing AAA parameters to a VRF can be accomplished from one or more of the following sources:

- Virtual template—Used as a generic interface configuration.
- Service provider AAA server—Used to associate a remote user with a specific VPN based on the domain name. The server then provides the VPN-specific configuration for the virtual access interface that includes the IP address and port number of the customer AAA server.
- Customer VPN AAA server—Used to authenticate the remote user and to provide user-specific configurations for the virtual access interface.

For more information on the per VRF AAA feature, see the "Configuring per VRF AAA Services" section on page 5-31 and the "RADIUS Attribute Screening" section on page 16-39.

Private Servers

Private servers are servers defined within a server group. These servers have private addresses within the default server group containing all the servers. Private servers remain hidden from other groups. If you do not specify private server parameters, global configurations are used. If you do not specify global configurations, default values are used.

You configure all server operational parameters per host, per server group, or globally. Per host configurations have precedence over per server group configurations. Per server group configurations have precedence over global configurations.

RADIUS Attribute Screening

The RADIUS Attribute Screening feature allows you to configure a list of "accept" or "reject" RADIUS attributes on the Cisco 10000 series router for authorization and accounting purposes. Based on the accept or reject list you configure for a particular purpose, the Cisco 10000 series router:

- Accepts and processes all standard RADIUS attributes
- Rejects all standard RADIUS attributes

Before you configure a RADIUS accept or reject list, you must enable AAA using the **aaa new-model** command in global configuration mode. For more information, see the "Configuring RADIUS Attribute Accept or Reject Lists" section on page 5-37, the "RADIUS Attribute Screening" section on page 16-39, or see the *Cisco IOS Command Summary, Volume 2 of 3, Release 12.2*.

Packet Fragmentation

The setting of the Don't Fragment (DF) bit determines if a packet is eligible for fragmentation. If the DF bit is clear, a packet is fragmented only if it exceeds the maximum transfer unit (MTU) size. If the DF bit is set, a packet is not fragmented and instead is dropped. For packets entering an L2TP tunnel that exceed the MTU size, enter the following command in global configuration mode to configure the Cisco 10000 series router to ignore the setting of the DF bit and to fragment the packets:

```
Router(config)# [no] ip pxf ignore l2tp df-bit
```

When you activate packet fragmentation, the router clears the DF bit of packets entering all L2TP tunnels and fragments the packets, but only if the packets exceed the session MTU. Clearing the DF bit allows packets to be fragmented. If a packet enters an L2TP tunnel, but it does not exceed the MTU, the router does not clear the DF bit. Instead, the DF bit is left untouched and the router does not fragment the packet.

Tunnel Accounting

The tunnel accounting feature enhances AAA accounting by adding the ability to include tunnel-related statistics in the RADIUS information. To collect tunnel usage information, RADIUS accounting includes tunnel accounting attributes and additional tunnel accounting values for the Acct-Status-Type RADIUS attribute.

Note For more information about the RADIUS tunnel accounting attributes or the Acct-Status-Type values that support RADIUS tunnel accounting, see the "Configuring Vendor-Specific Attributes on RADIUS" section on page 5-44 or see RFC 2867.

By using the tunnel accounting feature, you can track the services that users are accessing and the amount of network resources that they are consuming. In L2TP dial-up networks, tunneling of user sessions can be done automatically as a service of the Internet service provider (ISP). This service is used to provide remote intranet access to the employees of a corporation. ISPs collect usage information about the service, which they then can use for billing purposes and for managing the network. Tunnel accounting allows dial-up usage information to be collected and stored at a central location.

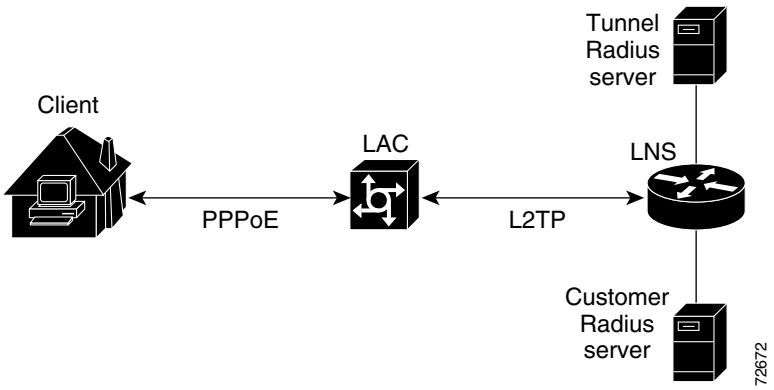
When you enable tunnel accounting on the Cisco 10000 series router, the router reports user activity to the RADIUS server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs. Accounting records are stored on the RADIUS server and can be analyzed for network management, client billing, and auditing. Corporations contracting with ISPs also receive a record of a user's resource consumption, which enables the corporation to audit its ISP billing statements.

Note For more information about AAA accounting, see the "Configuring Accounting" chapter in the *Cisco IOS Security Configuration Guide, Release 12.2*.

Tunnel Authentication

The tunnel authentication feature verifies users before they are allowed access to the network and the network services. On the LNS, L2TP tunnel authorization and authentication can occur by using the **vpdn-group** commands configured in the local configuration. If a large number of VPDN groups is configured, maintaining the local configuration across a number of LNS devices can be difficult. To alleviate this, the Cisco 10000 series router supports the capability to do tunnel authentication using a RADIUS server.

Figure 5-4 Tunnel Authorization and Authentication



As shown in Figure 5-4, typically, a tunnel RADIUS server is used for tunnel authorization and a separate user RADIUS server is used for RADIUS tunnel authentication. The following describes the sequence of events that occur for tunnel authorization and authentication:

1. The LNS gets a Start-Control-Connection-Request (SCCRQ) and starts tunnel initialization and authorization.
2. The LNS makes an authorization request to the RADIUS server. This request includes the name of the LAC device that initiated the tunnel. The RADIUS server uses the LAC name in determining user authorization.
3. The RADIUS server determines if local or RADIUS authorization should be done. If authorization is done locally, the LNS searches the VPDN groups. If RADIUS authorization is to be done, the RADIUS server makes a RADIUS request to the LNS. This request includes the LAC host name and a hardwired password.
4. The LNS checks RADIUS attributes 90 (Tunnel-Client-Auth-ID) and 69 (Tunnel-Password). If the value in attribute 90 is inconsistent with the LAC host name or the value in attribute 69 does not match the shared secret received in the SCCRQ, the tunnel is dropped.
5. The LNS terminates the L2TP tunnel.
6. User authentication occurs either locally or by using the RADIUS server.

Note

- The Cisco 10000 series router implements tunnel authentication by using Cisco-specific RADIUS attributes. For more information about the tunnel authentication vendor-specific attributes (VSAs), see the "Configuring Vendor-Specific Attributes on RADIUS" section on page 5-44.
- For more information about AAA authentication, see the "Configuring Authentication" chapter in the *Cisco IOS Security Configuration Guide, Release 12.2*.

Named Method Lists

To configure authentication, authorization, and accounting (AAA), you first define a named list of methods and then apply that list to various interfaces. The named method list defines the types of authentication or accounting to be performed and the sequence in which they will be performed. You must apply the method list to a specific interface before any defined authentication methods are performed. The only exception is the default method list, which is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

An authentication method list lists the methods to be queried to authenticate users. An accounting method list lists the methods used to support accounting. Method lists enable you to designate one or more security protocols to be used for authentication or accounting, thus ensuring a backup system for authentication or accounting in case the initial method fails. Cisco IOS software uses the first listed method to authenticate users or to support accounting. If that method fails to respond, the Cisco IOS software selects the next authentication or accounting method listed in the method list. This process continues until successful communication with a listed authentication or accounting method occurs, or all methods defined in the method list are exhausted.

The Cisco IOS software attempts authentication with the next listed authentication method only when there is no response from the previous method. If authentication fails at any point in this cycle (for example, the RADIUS server responds by denying user access), the authentication process stops and no other authentication methods are attempted.

For more information, see the "Configuring Authentication" chapter in the *Cisco IOS Security Configuration Guide, Release 12.2*.

Framed-Route VRF Aware

The Framed-Route VRF aware feature allows you to apply static IP routes to a specific VRF table instead of the global routing table. This feature makes RADIUS Attribute 22 (Framed-Route) and a combination of Attribute 8 (Framed-IP-Address) and Attribute 9 (Framed-IP-Netmask) aware of VRF instances.

You can configure a per-user static route by using the Framed-Route attribute in any of the following ways:

- Using the Cisco **route** command
- Using the RADIUS Framed-Route attribute

Note When the PE router receives a Framed-Route attribute from the RADIUS server, the PE determines if the user is a VPN customer. If so, then the static route is implemented in the VRF routing table to which the user belongs.

- Using the RADIUS Framed-IP-Address or Framed-IP-Netmask attribute

Note The Framed-IP-Netmask attribute has the same function as the Framed-Route attribute.

Feature History for LNS

Cisco IOS Release	Description	Required PRE
12.2(4)BZ1	This feature was introduced on the Cisco 10000 series router.	PRE1
12.3(7)XI1	This feature was integrated into Cisco IOS Release 12.3(7)XI1.	PRE2
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.	PRE2

Restrictions for the LNS

To function as a LNS, the Cisco 10000 series router has the following restrictions:

- The Cisco 10000 series router does not support the configuration of L2TP tunnels over the management Fast Ethernet interface. Do not set up L2TP tunnels over this interface.
- In Cisco IOS Release 12.3(7)XI1, the output rate limited traffic on an L2TP VAI can be lower than than in previous releases due to increases in the overhead included in the policed bps rate.

  The configured police bps rate when applied to an L2TP virtual access interface includes the following 40 bytes of per packet overhead:

  - L2TP (8 bytes)
  - PPP (4 bytes)
  - Outer IP (20 bytes)
  - UDP (8 bytes)

Prerequisites for LNS

To function as an LNS, the Cisco 10000 series router has the following requirements:

- Before you configure RADIUS tunnel accounting or authentication, you must first:
  - Enable AAA on the LNS and the LAC by using the **aaa new-model** global configuration command. For more information, see the "AAA Overview" chapter in the *Cisco IOS Security Configuration Guide, Release 12.2*.
  - Configure the LNS and LAC to communicate with the RADIUS server. For more information, see the "Configuring the LAC to Communicate with the RADIUS Server" section on page 5-11 and see the "Configuring RADIUS" chapter in the *Cisco IOS Security Configuration Guide, Release 12.2*.

Note For more information, see the "Configuring Accounting," "Configuring Authentication," and "Configuring RADIUS" chapters in the *Cisco IOS Security Configuration Guide, Release 12.2*.

Required Configuration Tasks for LNS

To configure the Cisco 10000 series router as an LNS, perform the following required configuration tasks:

- Configuring the Virtual Template Interface, page 5-29
- Configuring the LNS to Initiate and Receive L2TP Traffic, page 5-29

Note You must also configure the LAC and RADIUS server to communicate with the LNS. For more information, see the "Required Configuration Tasks for LAC" section on page 5-7 or see your RADIUS documentation.

Configuring the Virtual Template Interface

To configure a virtual template interface, enter the following commands:

	Command	Purpose
Step 1	`Router> enable`	Enters privileged EXEC mode.
Step 2	`Router# config terminal`	Enters global configuration mode.
Step 3	`Router(config)# interface virtual-template` *number*	Creates a virtual template interface and enters interface configuration mode.
Step 4	`Router(config-if)# ip vrf forwarding` <*name*>	Maps the virtual template interface to a VRF routing table.
Step 5	`Router(config-if)# ip unnumbered loopback` <*number*>	Enables IP without assigning a specific IP address on the LAN.
Step 6	`Router(config-if)# ppp authentication` {**pap** | **chap** | **ms-chap**}	Enables PAP or CHAP authentication on the virtual template interface, which is applied to VAIs.

Configuring the LNS to Initiate and Receive L2TP Traffic

To configure the Cisco 10000 router, acting as the LNS, to initiate and receive L2TP traffic, enter the following commands:

	Command	Purpose
Step 1	`Router> enable`	Enters privileged EXEC mode.
Step 2	`Router# config terminal`	Enters global configuration mode.
Step 3	`Router(config)# vpdn enable`	Enables VPDN networking on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway) if one is present.
Step 4	`Router(config)# vpdn-group` *group-name*	Defines a local group name for which you can assign other VPDN variables. Enters VPDN group configuration mode.
Step 5	`Router(config-vpdn)# accept-dialin`	Configures the LNS to accept tunneled PPP connections from the LAC and creates an accept-dialin VPDN subgroup.

	Command	Purpose
Step 6	`Router(config-vpdn-acc-in)# protocol l2tp`	Specifies the Layer 2 Tunnel Protocol.
Step 7	`Router(config-vpdn-acc-in)# virtual-template` *template-number*	Specifies the virtual template to be used to clone virtual access interfaces.
Step 8	`Router(config-vpdn-acc-in)# exit`	Returns to VPDN group configuration mode.
Step 9	`Router(config-vpdn)# terminate-from hostname` *host-name*	Specifies the host name of the remote L2TP access concentrator (LAC) that will be required when accepting a VPDN tunnel.

Example 5-12 Configuring the LNS

```
!Configures the VRF.
ip vrf vpn-1
    rd 1100:1
!
!Configures the virtual template interface and associates the VRF to it.
interface virtual-template 1
    ip vrf forwarding vpn-1
    ip unnumbered loopback
    ppp authentication chap
!
!Configures a VPDN group to ensure that all the sessions for a particular tunnel get the
same virtual template and thus the same VRF.
vpdn enable
vpdn-group 1
    accept-dialin
    protocol l2tp
    virtual-template 1
    terminate-from hostname lac1-vpn1
    local name r4-1
    l2tp tunnel password 7 1511021F0725
    l2tp tunnel receive-window 100
    l2tp tunnel retransmit retries 7
    l2tp tunnel retransmit timeout min 2
```

Optional Configuration Tasks for LNS

To configure the Cisco 10000 series router as an LNS, perform as many of the following configuration tasks as desired. All of these configuration tasks are optional.

- Configuring per VRF AAA Services, page 5-31
- Configuring a VRF on the LNS, page 5-36
- Configuring Sessions per Tunnel Limiting on the LNS, page 5-36
- Configuring RADIUS Attribute Accept or Reject Lists, page 5-37
- Configuring the LNS for RADIUS Tunnel Accounting, page 5-39
- Configuring the LNS for RADIUS Tunnel Authentication, page 5-42

Configuring per VRF AAA Services

To configure per VRF AAA services, perform the following tasks:

- Enabling AAA, page 5-31
- Configuring Private Server Parameters, page 5-31
- Configuring AAA for the VRF, page 5-32
- Configuring RADIUS-Specific Commands for the VRF, page 5-34

Note For more information about configuring AAA parameters, see the *Cisco IOS Security Configuration Guide, Release 12.2*.

Enabling AAA

To enable AAA, enter the following commands.

Note For more information, see the *Cisco IOS Command Summary, Volume 2 of 3, Release 12.2*.

	Command	Purpose
Step 1	`Router> enable`	Enters privileged EXEC mode.
Step 2	`Router# config terminal`	Enters global configuration mode.
Step 3	`Router(config)# aaa new model`	Enables AAA.

Configuring Private Server Parameters

To configure private server operational parameters, enter the following commands:

	Command	Purpose
Step 1	`Router> enable`	Enters privileged EXEC mode.
Step 2	`Router# config terminal`	Enters global configuration mode.

Step 3	`Router(config)# aaa group server radius` *group-name*	Groups different RADIUS server hosts into distinct lists and distinct methods.
		The *group-name* argument is the character string used to name the group.
		Note When RADIUS servers are configured in a group and the first server fails to respond, the L2TP tunnel request from the LAC might time out before the LNS fails over to the second server. To avoid this, configure the LAC with the following commands in VPDN group configuration mode:
		`l2tp tunnel retransmit initial retries 5`
		`l2tp tunnel retransmit initial timeout min 2`

	Command	Purpose
Step 4	`Router(config-sg-radius)# server-private` *ip-address* `timeout` *seconds* `retransmit` *retries* `key` *string*	Configures the IP address of the private RADIUS server for the group server. The *ip-address* argument specifies the IP address of the private RADIUS server host. (Optional) The *seconds* argument specifies the timeout value (1 to 1000). The *string* argument specifies the authentication and encryption key for all RADIUS communications between the Cisco 10000 series router and the RADIUS server.
Step 5	`Router(config-sg-radius)# ip vrf forwarding` *vrf-name*	Configures the VRF reference of the AAA RADIUS server group. The *vrf-name* argument is the name assigned to a VRF instance.

Configuring AAA for the VRF

To configure AAA for the VRF, enter the following commands:

	Command	Purpose
Step 1	`Router> enable`	Enters privileged EXEC mode.
Step 2	`Router# config terminal`	Enters global configuration mode.
Step 3	`Router(config)# aaa authentication ppp` *list-name method1* [*method2...*]	Specifies one or more AAA authentication methods for use on serial interfaces running PPP. The *list-name* argument is a character string used to name the list of authentication methods tried when a user logs in. The *method1*[*method2...*] argument is at least one of the following keywords: • **if-needed**—Does not authenticate if user has already been authenticated on a TTY line. • **local**—Uses the local username database for authentication. • **local-case**—Uses case-sensitive local username authentication. • **none**—Uses no authentication. • **group radius**—Uses the list of all RADIUS servers for authentication. • **group** *group-name*—Uses a subset of RADIUS servers for authentication as defined by the **aaa group server radius** command.

	Command	Purpose
Step 4	`Router(config)# aaa authorization network list-name method1 [method2...]`	Sets parameters that restrict user access to a network. The *list-name* argument is a character string used to name the list of authentication methods tried when a user logs in. The *method1*[*method2...*] argument is at least one of the following keywords: • **group radius**—Uses the list of all RADIUS servers for authentication. • **group** *group-name*—Uses a subset of RADIUS servers for authentication as defined by the **aaa group server radius** command. • **if-authenticated**—Succeeds if user has been successfully authenticated. • **local**—Uses the local username database for authentication. • **none**—Uses no authentication.
Step 5	`Router(config)# aaa accounting {system default [vrf vrf-name] | network {default | none | start-stop | stop-only | wait-start} group group-name`	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS. The **system default** keyword performs accounting for all system-level events not associated with users, such as reloads. The **vrf** *vrf-name* keyword and argument specify a VRF configuration. The **network** keyword runs accounting for all network-related service requests. The **default** keyword specifies the default accounting list: • **none**—No accounting. • **start-stop**—Record stop and start without waiting. • **stop-only**—Record stop when service terminates. • **wait-start**—Record stop and start after start-record commit. The **group** *group-name* keyword and argument use a subset of RADIUS servers for accounting as defined by the server **group** *group-name*.
Step 6	`Router(config)# aaa accounting delay-start vrf vrf-name`	Delays generation of the start accounting records until the user IP address is established. The **vrf** *vrf-name* keyword and argument enables the specification on a per VRF basis.
Step 7	`Router(config)# aaa accounting send stop-record authentication failure vrf vrf-name`	Generates accounting stop records for users who fail to authenticate at login or during session negotiation. The **vrf** *vrf-name* keyword and argument enables the specification on a per VRF basis.

Configuring RADIUS-Specific Commands for the VRF

To configure AAA global RADIUS-specific commands for the VRF definition, enter the following commands:

	Command	Purpose
Step 1	`Router> enable`	Enters privileged EXEC mode.
Step 2	`Router# config terminal`	Enters global configuration mode.
Step 3	`Router(config)# interface virtual-template number`	Configures a virtual template interface and enters interface configuration mode.
Step 4	`Router(config-if)# ip vrf forwarding vrf-name`	Associates a VRF instance with a virtual template interface. The *vrf-name* argument is the name assigned to a VRF.
Step 5	`Router(config-if)# ppp authentication {protocol1 [protocol2...]} list-name`	Enables Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) or both and specifies the order in which CHAP and PAP authentication are selected on the interface. The *protocol1*[*protocol2...*] argument specifies at least one of the following keywords: • **chap**—Enables CHAP on a serial interface. • **ms-chap**—Enables Microsoft's version of CHAP (MS-CHAP) on a serial interface. • **pap**—Enables PAP on a serial interface. The *list-name* argument (optional) specifies the name of a list of methods of authentication to use. This is the same name you specified in step 4 of the "Configuring AAA for the VRF" section on page 5-32. If no list name is specified, the system uses the default. Create the list by using the **aaa authentication ppp** command.
Step 6	`Router(config-if)# ppp authorization list-name`	Enables AAA authorization on the selected interface. The *list-name* argument (optional) specifies the name of a list of authorization methods to use. If no list name is specified, the system uses the default. Create the list by using the **aaa authorization** command.
Step 7	`Router(config-if)# ppp accounting list-name`	Enables AAA accounting services on the selected interface.
Step 8	`Router(config-if)# exit`	Exits interface configuration mode.
Step 9	`Router(config)# ip radius source-interface subinterface-name vrf vrf-name`	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets and enables the specification on a per VRF basis. The *subinterface-name* argument specifies the name of the interface that RADIUS uses for all of its outgoing packets. The **vrf** *vrf-name* keyword and argument specify the per VRF configuration.

	Command	Purpose
Step 10	`Router(config)# radius-server attribute 44 include-in-access-req vrf` *vrf-name*	Sends RADIUS attribute 44 in access request packets before user authentication and enables the specification on a per VRF basis. The **vrf** *vrf-name* keyword and argument specify the per VRF configuration.
Step 11	`Router(config)# radius-server domain-stripping vrf` *vrf-name*	(Optional) Enables VRF-aware domain-stripping. The **vrf** *vrf-name* keyword and argument specify the per VRF configuration.

Verifying and Troubleshooting per VRF AAA

To verify and troubleshoot the per VRF AAA feature, enter the following commands in privileged EXEC mode.

Note Due to the large output of some of the commands, many events are not displayed on the console. Instead, the messages are logged to a console log file. To limit the rate that the Cisco 10000 series router logs system messages, enter the **logging rate-limit** command. For more information, see the "Troubleshooting and Fault Management Commands in the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*.

Command	Purpose
`Router# show ip route vrf` *vrf-name*	Displays the IP routing table associated with a VRF.
`Router# debug aaa accounting`	Displays information on accountable events as they occur.
`Router# debug aaa authorization`	Displays information on AAA authorization.
`Router# debug ppp negotiation`	Displays information on traffic and exchanges in an internetwork implementing PPP.
`Router# debug radius`	Displays information associated with RADIUS.
`Router# debug vpdn event`	Displays L2TP errors and events that are a part of normal tunnel establishment or shutdown for VPNs.
`Router# debug vpdn error`	Displays debug traces for VPN.

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco Systems technical support personnel. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

Configuring a VRF on the LNS

To configure a VRF, enter the following commands:

	Command	Purpose
Step 1	`Router> enable`	Enters privileged EXEC mode.
Step 2	`Router# config terminal`	Enters global configuration mode.
Step 3	`Router(config)# ip vrf vrf-name`	Enters VRF configuration mode and defines the VPN routing instance by assigning a VRF name.
Step 4	`Router(config-vrf)# rd route-distinguisher`	Creates routing and forwarding tables.

For more information about configuring a VRF, see the "Configuring Multiprotocol Label Switching chapter in the *Cisco IOS Switching Services Configuration Guide, Release 12.2*.

Configuring Sessions per Tunnel Limiting on the LNS

To limit the number of sessions per tunnel without using a RADIUS server, enter the following commands:

	Command	Purpose
Step 1	`Router> enable`	Enters privileged EXEC mode.
Step 2	`Router# config terminal`	Enters global configuration mode.
Step 3	`Router(config)# vpdn-group group-name`	Defines a local group name for which you can assign other VPDN variables. Enters VPDN group configuration mode.
Step 4	`Router(config-vpdn)# accept-dialin`	Configures the LNS to accept tunneled PPP connections from the LAC and creates an accept-dialin VPDN subgroup.
Step 5	`Router(config-vpdn-acc-in)# protocol l2tp`	Specifies the Layer 2 Tunnel Protocol.
Step 6	`Router(config-vpdn-acc-in)# virtual-template template-number`	Specifies the virtual template to be used to clone virtual access interfaces.
Step 7	`Router(config-vpdn-acc-in)# exit`	Returns to VPDN group configuration mode.
Step 8	`Router(config-vpdn)# terminate-from hostname host-name`	Specifies the host name of the remote L2TP access concentrator (LAC) that is required when accepting a VPDN tunnel.
Step 9	`Router(config-vpdn)# session-limit limit-number`	Specifies the maximum number of sessions per tunnel.

Verifying Sessions per Tunnel Limiting on the LNS

To verify sessions per tunnel limiting on the LNS, enter the following commands:

Command	Purpose
`Router# show running-config`	Displays the current router configuration. Check the output to verify that you successfully configured the maximum number of sessions per tunnel.
`Router# show vpdn tunnel`	Displays information about all active L2TP tunnels in summary-style format. Check the output to verify that the number of displayed sessions does not exceed your configured limit.

Configuring RADIUS Attribute Accept or Reject Lists

To configure a RADIUS attribute accept or reject list for authorization or accounting, enter the following commands:

	Command	Purpose
Step 1	`Router> enable`	Enters privileged EXEC mode.
Step 2	`Router# config terminal`	Enters global configuration mode.
Step 3	`Router(config)# aaa authentication ppp default group group-name`	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
Step 4	`Router(config)# aaa authorization network default group group-name`	Sets parameters that restrict network access to the user.
Step 5	`Router(config)# aaa group server radius group-name`	Groups different RADIUS server hosts into distinct lists and distinct methods and enters server group configuration mode.
Step 6	`Router(config-sg-radius)# server-private ip-address timeout seconds retransmit retries key string`	Configures the IP address of the private RADIUS server for the group server. The *ip-address* argument specifies the IP address of the private RADIUS server host. (Optional) The *seconds* argument specifies the timeout value (1 to 1000). The *string* argument specifies the authentication and encryption key for all RADIUS communications between the Cisco 10000 series router and the RADIUS server.

Step 7	`Router(config-sg-radius)# authorization [accept | reject] listname`
	and/or
	`Router(config-sg-radius)# accounting [accept | reject] listname`
		Specifies a filter for the attributes that are returned in an Access-Accept packet from the RADIUS server.
		Specifies a filter for the attributes that are to be sent to the RADIUS server in an accounting request.
		The **accept** keyword indicates that all attributes will be rejected except the attributes specified in the *listname* argument.
		The **reject** keyword indicates that all attributes will be accepted except for the attributes specified in the *listname* argument and all standard attributes.

	Command	Purpose
Step 8	`Router(config-sg-radius)# exit`	Exits server-group configuration mode.
Step 9	`Router(config)# radius-server attribute list` *listname*	Defines the list name given to the set of attributes defined using the **attribute** command. Define the *listname* argument to be the same as you defined it in step 5.
Step 10	`Router(config-sg-radius)# attribute` *value1* [*value2* [*value3...*]]	Adds attributes to the configured accept or reject list. You can use this command multiple times to add attributes to an accept or reject list.

Verifying RADIUS Attribute Accept or Reject Lists

To verify an accept or reject list, enter any of the following commands in privileged EXEC mode:

Command	Purpose
`Router# debug aaa accounting`	Displays information on accountable events as they occur.
`Router# debug aaa authentication`	Displays information on AAA authentication.
`Router# show radius statistics`	Displays the RADIUS statistics for accounting and authentication packets.

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco Systems technical support personnel. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

Configuring the LNS for RADIUS Tunnel Accounting

To configure the LNS for RADIUS tunnel accounting, perform the following required configuration tasks:

- Configuring AAA Accounting Using Named Method Lists, page 5-39
- Configuring RADIUS for Tunnel Accounting, page 5-39

Configuring AAA Accounting Using Named Method Lists

To configure AAA accounting using named method lists, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa accounting {system | network | exec | connection | commands level} {default | list-name} {start-stop | stop-only | none} [method1 [method2...]]`	Creates an accounting method list and enables accounting. The *list-name* argument is a character string used to name the list you are creating.

Step 2	`Router(config)# line [aux | console | tty | vty] line-number [ending-line-number]`
	or
	`Router(config)# interface interface-type interface-number`
		Enters the line configuration mode for the line to which you want to apply the accounting method list.
		Enters the interface configuration mode for the interface to which you want to apply the accounting method list.

Step 3	`Router(config-line)# accounting {arap | commands level | connection | exec} {default | list-name}`
	or
	`Router(config-if)# ppp accounting {default | list-name}`
		Applies the accounting method list to a line or a set of lines.
		Applies the accounting method list to an interface.

Note System accounting does not use named method lists. For system accounting you can define only the default method list. For more information, see the "Configuring Accounting" chapter in the *Cisco IOS Security Configuration Guide, Release 12.2*.

Configuring RADIUS for Tunnel Accounting

Cisco IOS Release 12.2(15)BX enhances the AAA accounting feature by adding the ability to include tunnel-related statistics in the RADIUS information. To collect tunnel usage information, you must configure the following attributes on the RADIUS server:

- Acct-Tunnel-Connection—Specifies the identifier assigned to the tunnel session. This attribute and the Tunnel-Client-Endpoint and Tunnel-Server-Endpoint attributes provide a way to uniquely identify a tunnel session for auditing purposes.
- Acct-Tunnel-Packets-Lost—Specifies the number of packets lost on a given link.

Table 5-1 describes the values for the Acct-Status-Type attribute that support tunnel accounting on the RADIUS server.

Table 5-1 Acct-Status-Type Values for RADIUS Tunnel Accounting

Acct-Status-Type Values	Value	Description
Tunnel-Start	9	Marks the establishment of a tunnel with another device.
Tunnel-Stop	10	Marks the destruction of a tunnel to or from another device.
Tunnel-Reject	11	Marks the rejection of the establishment of a tunnel with another device.
Tunnel-Link-Start	12	Marks the creation of a tunnel link within an L2TP tunnel that carries multiple links.
Tunnel-Link-Stop	13	Marks the destruction of a tunnel link within an L2TP tunnel that carries multiple links.
Tunnel-Link-Reject	14	Marks the rejection of the establishment of a new link in an existing tunnel.

Example 5-13 is an example of Tunnel-Start accounting record sent by the LNS to the RADIUS server.

Example 5-13 Tunnel-Start Accounting Record

```
User-Name = LNS1/LAC1
NAS-IP-Address = 23.1.2.10
Service-Type = Framed
Framed-Protocol = PPP
Tunnel-Type_tag0 = L2TP
Tunnel-Medium-Type_tag0 = IPv4
Tunnel-Client-Endpoint_tag0 = 10.2.2.1
Tunnel-Server-Endpoint_tag0 = 10.2.2.2
Acct-Status-Type = Tunnel-Start
Acct-Delay-Time = 0
Acct-Session-Id = 00000B3D
Acct-Authentic = RADIUS
Tunnel-Client-Auth-ID_tag0 = LAC1
Tunnel-Server-Auth-ID_tag0 = LNS1
Acct-Tunnel-Connection = 63708/13441
```

Example 5-14 is an example of a Tunnel-Stop accounting record sent by the LNS to the RADIUS server.

Example 5-14 Tunnel-Stop Accounting Record

```
User-Name = LNS1/LAC1
NAS-IP-Address = 23.1.2.10
Service-Type = Framed
Framed-Protocol = PPP
Ascend-Multilink-ID = 2877
Ascend-PreSession-Time = 0
Tunnel-Type_tag0 = L2TP
Tunnel-Medium-Type_tag0 = IPv4
Tunnel-Client-Endpoint_tag0 = 10.2.2.1
Tunnel-Server-Endpoint_tag0 = 10.2.2.2
Ascend-Pre-Input-Packets = 0
Ascend-Pre-Input-Octets = 0
```

```
Acct-Status-Type = Tunnel-Stop
Acct-Delay-Time = 0
Acct-Input-Octets = 108276
Acct-Output-Octets = 65986
Acct-Session-Id = 00000B3D
Acct-Authentic = RADIUS
Acct-Session-Time = 57
Acct-Input-Packets = 2578
Acct-Output-Packets = 2823
Acct-Terminate-Cause = NAS Error
Acct-Multi-Session-Id = 00000B3D
Tunnel-Client-Auth-ID_tag0 = LAC1
Tunnel-Server-Auth-ID_tag0 = LNS1
Ascend-Connect-Progress = Call-Up
Acct-Tunnel-Connection = 63708/13441
Ascend-Disconnect-Cause = No-Reason
Acct-Tunnel-Packets-Lost = 0
Ascend-Pre-Output-Octets = 0
Ascend-Pre-Output-Packets = 0
```

For more information about the RADIUS tunnel accounting attributes or the Acct-Status-Type values that support RADIUS tunnel accounting, see RFC 2867, *RADIUS Accounting Modifications for Tunnel Protocol Support*.

For information about RADIUS accounting attributes supported on the Cisco 10000 series router, see Appendix A, "RADIUS Attributes".

For information about RADIUS attributes, see the "RADIUS Attributes" appendix in the *Cisco IOS Security Configuration Guide, Release 12.2*.

For more information on configuring RADIUS, see your RADIUS user documentation.

Configuring Optional RADIUS Tunnel Accounting Features

To configure RADIUS tunnel accounting, you can also perform any of the following optional configuration tasks:

- Suppressing Generation of Accounting Records for Null Username Sessions
- Generating Interim Accounting Records
- Generating Accounting Records for Failed Login or Session
- Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records
- Configuring AAA Resource Failure Stop Accounting
- Configuring AAA Resource Accounting for Start-Stop Records
- Configuring AAA Broadcast Accounting
- Configuring AAA Resource Failure Stop Accounting
- Configuring AAA Session MIB
- Monitoring Accounting
- Troubleshooting Accounting

Note For more information, see the "Configuring Accounting" chapter in the *Cisco IOS Security Configuration Guide, Release 12.2*.

Configuring the LNS for RADIUS Tunnel Authentication

To configure the LNS for RADIUS tunnel authentication, perform the following required configuration tasks:

- Configuring RADIUS Tunnel Authentication Method Lists on the LNS, page 5-42
- Configuring AAA Authentication Methods, page 5-43
- Configuring Vendor-Specific Attributes on RADIUS, page 5-44

Note Cisco 10000 series router supports L2TP tunnel authorization, however, RADIUS does not provide attributes for such parameter values as L2TP tunnel timeouts, L2TP tunnel hello intervals, and L2TP tunnel receive window size. When the Cisco 10000 series router does not receive a RADIUS attribute for a parameter, the router uses the default value.

Configuring RADIUS Tunnel Authentication Method Lists on the LNS

To configure method lists on the LNS for RADIUS tunnel authentication, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa authorization network list-name method1 [method2...]`	Sets parameters that restrict user access to a network. The *list-name* argument is a character string used to name the list of authentication methods tried when a user logs in. The *method1*[*method2...*] argument is at least one of the following keywords: • **group radius**—Uses the list of all RADIUS servers for authentication. • **group** *group-name*—Uses a subset of RADIUS servers for authentication as defined by the **aaa group server radius** command. • **if-authenticated**—Succeeds if the user has been successfully authenticated. • **local**—Uses the local username database for authentication. • **none**—Uses no authentication. **Note** The method list is only for VPDN tunnel authorization and termination, not for domain and DNIS authorization. Therefore, the method list applies only on the tunnel terminator device: the LAC for dialout sessions and the LNS for dialin sessions.
Step 2	`Router(config)# vpdn tunnel authorization network <method list name>`	Specifies the AAA method list to use for VPDN remote tunnel hostname-based authorization. If you do not specify a method list (including a default method list) by using the **vpdn tunnel authorization network** command, local authorization occurs by using the local VPDN group configuration.

	Command	Purpose
Step 3	`Router(config)# vpdn tunnel authorization virtual-template <vtemplate num>`	Specifies the default virtual template interface used to clone a virtual access interface (VAI). If you do not specify a virtual template interface in the local VPDN group configuration or in a remote RADIUS configuration, then this default virtual template interface is used. **Note** The **vpdn tunnel authorization virtual-template** command is only applicable on the LNS.
Step 4	`Router(config)# vpdn tunnel authorization password <dummy password>`	Specifies the password to use for the RADIUS authorization request to retrieve the tunnel configuration based on the remote tunnel hostname. By default, the password is *cisco*, but you can configure a different password. **Note** The **vpdn tunnel authorization password** command is applicable on both the LAC and LNS.

Configuring AAA Authentication Methods

To configure AAA authentication methods, do the following:

Step 1 Enable AAA using the **aaa new-model** global configuration command. For more information, see the "AAA Overview" chapter in the *Cisco IOS Security Configuration Guide, Release 12.2*.

Step 2 Configure RADIUS security protocol parameters. For more information about RADIUS, see the "Configuring RADIUS" chapter in the *Cisco IOS Security Configuration Guide, Release 12.2*.

Step 3 Define the authentication method lists using the **aaa authentication** command.

Step 4 Apply the authentication method lists to an interface, a line, or a set of lines as required.

The Configuring Authentication" chapter in the *Cisco IOS Security Configuration Guide, Release 12.2* describes how to configure the following authentication methods:

- Configuring Login Authentication Using AAA
- Configuring PPP Authentication Using AAA
- Configuring AAA Scalability for PPP Requests
- Configuring ARAP Authentication Using AAA
- Configuring NASI Authentication Using AAA
- Specifying the Amount of Time for Login Input
- Enabling Password Protection at the Privileged Level
- Changing the Text Displayed at the Password Prompt
- Configuring Message Banners for AAA Authentication
- Configuring AAA Packet of Disconnect
- Enabling Double Authentication
- Enabling Automated Double Authentication

Configuring Vendor-Specific Attributes on RADIUS

Cisco IOS Release 12.2(15)BX adds Cisco-specific VPDN RADIUS attributes to support RADIUS tunnel authentication. To configure the RADIUS server for tunnel authentication, you must configure the following vendor-specific attributes (VSAs) on the RADIUS server:

- vpdn-vtemplate—Specifies the virtual template number to use for cloning on the LNS. This attribute corresponds to the virtual template associated with the local VPDN group on the LNS. This attribute is not required if you used the **vpdn tunnel authorization virtual-template** <*vtemplate num*> command on the LNS to configure a default virtual template to use for cloning.

  ```
  Cisco:Cisco-Avpair = "vpdn:vpdn-vtemplate = <vtemplate number>"
  ```

- dout-dialer—Specifies the LAC dialer to use on the LAC for a dialout configuration.

  ```
  Cisco:Cisco-Avpair = "vpdn:dout-dialer = <LAC dialer number>"
  ```

- Service-Type—Specifies an outbound or inbound service type. In the tunnel authorization request, the LNS sets the Service-Type attribute to Outbound. Therefore, in the RADIUS configuration you must also configure an Outbound Service-Type.

  ```
  Service-Type = Outbound
  ```

Note

- For information about RADIUS attributes supported on the Cisco 10000 series router, see Appendix A, "RADIUS Attributes" or see the "RADIUS Attributes" appendix in the *Cisco IOS Security Configuration Guide, Release 12.2*.
- For more information about configuring RADIUS, see your RADIUS user documentation.

Example 5-15 is a RADIUS configuration that allows the LNS to terminate L2TP tunnels from a LAC. In this configuration, VirtualTemplate10 is used to clone a virtual access interface (VAI) on the LNS.

Example 5-15 Configuring RADIUS for LNS Termination of L2TP Tunnels from a LAC

```
myLACname       Password = "cisco"
    Service-Type = Outbound,
    Tunnel-Type = :0:1@TP,
    Tunnel-Medium-Type = :o:IP,
    Tunnel-Client-Auth-ID = :0:"myLACname",
    Tunnel-Password = :0:"mytunnelpassword",
    Cisco:Cisco-Avpair = "vpdn:vpdn-vtemplate=10"
```

Example 5-16 is an LNS configuration that supports RADIUS tunnel authentication. In this configuration, a RADIUS server group is defined using the **aaa group server radius VPDN-Group** command. The **aaa authorization network mymethodlist group VPDN-Group** command queries RADIUS for network authorization.

Example 5-16 Configuring the LNS to Support RADIUS Tunnel Authentication

```
aaa group server radius VPDN-Group
    server 64.102.48.91 auth-port 1645 acct-port 1646
aaa authorization network mymethodlist group VPDN-Group
vpdn tunnel authorization network mymethodlist
vpdn tunnel authorization virtual-template 10
```

Configuration Examples for LNS

This section provides example configurations for the following features:

Managed LNS Configuration Example

Example 5-17 is an example of how to configure the Managed LNS features on the Cisco 10000 series router. In this example, the Cisco 10000 series router terminates the tunnel from the LAC and associates the VRFs with the interfaces and the virtual template interfaces. This configuration also configures RADIUS attribute screening and AAA accounting for the VRFs.

Example 5-17 Configuring Managed LNS on the Cisco 10000 Series Router

```
!Enables AAA.
aaa new-model
!
!Configures private server parameters.
aaa group server radius vpn1
 server-private 192.168.1.128 auth-port 1645 acct-port 1646 key cisco
 server-private 192.168.2.128 auth-port 1645 acct-port 1646 timeout 10 retransmit 3 key
!Configures RADIUS attribute screening.
cisco1
 authorization reject vpn1-autho-list
 accounting reject vpn1-account-list
 ip vrf forwarding vpn1
!
!Configures private server parameters.
aaa group server radius vpn2
 server-private 192.168.1.128 auth-port 1645 acct-port 1646 key cisco
 server-private 192.168.2.128 auth-port 1645 acct-port 1646 timeout 10 retransmit 3 key
cisco1
 ip vrf forwarding vpn2
!
!Configures AAA accounting for the VRFs.
aaa authentication ppp vpn1 group vpn1
aaa authentication ppp vpn2 group vpn2
aaa authorization network vpn1 group vpn1
aaa authorization network vpn2 group vpn2
aaa accounting update periodic 1
aaa accounting network vpn1 start-stop group vpn1
aaa accounting network vpn2 start-stop group vpn2
aaa accounting system default vrf vpn1 start-stop group vpn1
aaa accounting system default vrf vpn2 start-stop group vpn2
aaa session-id common
!
!Configures the VRFs.
ip vrf vpn1
 rd 1100:1
!
ip vrf vpn2
 rd 1100:2
vpdn enable
!
!Terminates the tunnel from the LAC.
vpdn-group 1
```

```
 accept-dialin
 protocol l2tp
 virtual-template 1
 terminate-from hostname lac1-vpn1
 local name r4-1
 lcp renegotiation on-mismatch
 l2tp tunnel password 7 1511021F0725
 l2tp tunnel receive-window 100
 l2tp tunnel retransmit retries 7
 l2tp tunnel retransmit timeout min 2
!
!Terminates the tunnel from the LAC.
vpdn-group 2
 accept-dialin
  protocol l2tp
  virtual-template 2
 terminate-from hostname lac1-vpn2
 local name r4-2
 lcp renegotiation on-mismatch
 l2tp tunnel password 7 121A0C041104
 l2tp tunnel receive-window 100
 l2tp tunnel retransmit retries 7
 l2tp tunnel retransmit timeout min 2
!
!
!Associates the VRF with the interface.
interface Loopback1
 ip vrf forwarding vpn1
 ip address 10.1.1.1 255.255.255.255
!
interface Loopback2
 ip vrf forwarding vpn2
 ip address 10.1.2.1 255.255.255.255
!
interface FastEthernet0/0/0
 no ip address
 shutdown
!
!Configures the interface used to connect to the LAC.
interface GigabitEthernet6/0/0
 ip address 10.1.1.45 255.255.255.0
 negotiation auto
!
interface GigabitEthernet7/0/0
 no ip address
 negotiation auto
!
!Associates the VRF with the interface.
interface GigabitEthernet7/0/0.1
 encapsulation dot1Q 11
 ip vrf forwarding vpn1
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet7/0/0.2
 encapsulation dot1Q 12
 ip vrf forwarding vpn2
 ip address 192.168.2.1 255.255.255.0
!
!Associates the VRF with the virtual template interface.
interface Virtual-Template1
 ip vrf forwarding vpn1
 ip unnumbered Loopback1
 no peer default ip address
 ppp authentication chap vpn1
```

```
 ppp authorization vpn1
 ppp accounting vpn1
!
!Associates the VRF with the virtual template interface.
interface Virtual-Template2
 ip vrf forwarding vpn2
 ip unnumbered Loopback2
 no peer default ip address
 ppp authentication chap vpn2
 ppp authorization vpn2
 ppp accounting vpn2
!
!Enters the VRFs in the routing table.
ip classless
ip route vrf vpn1 192.168.4.2 255.255.255.0 192.168.5.3
ip route vrf vpn2 192.168.4.2 255.255.255.0 192.168.5.4
no ip http server
ip pim bidir-enable
!
!Configures RADIUS-specific command for the VRF to force RADIUS to use the IP address of a
!specified interface for all outgoing RADIUS packets.
ip radius source-interface GigabitEthernet7/0/0.1 vrf vpn1
ip radius source-interface GigabitEthernet7/0/0.2 vrf vpn2
no cdp run
!
!radius-server retransmit is on by default and cannot be removed.
radius-server retransmit 3
!Configures optional features such as domain-name stripping and RADIUS attribute filter.
radius-server domain-stripping vrf vpn1
radius-server domain-stripping vrf vpn2
radius-server attribute 44 include-in-access-req vrf vpn1
radius-server attribute 44 include-in-access-req vrf vpn2
radius-server attribute list vpn1-autho-list
 attribute 26,200-220
!
radius-server attribute list vpn1-account-list
 attribute 60-70
!
```

Tunnel Accounting Configuration Examples

This section provides the following configuration examples:

- LNS Tunnel Accounting Configuration Example, page 5-48
- RADIUS Tunnel Accounting Records, page 5-49

LNS Tunnel Accounting Configuration Example

Example 5-18 shows how to configure the LNS to send tunnel accounting records to the RADIUS server.

Example 5-18 Configuring the LNS for Tunnel Accounting

```
aaa new-model
!
!
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$ftf.$wE6Q5Yv6hmQiwL9pizPCg1
!
username ENT_LNS password 0 tunnelpass
username user1@cisco.com password 0 lab
username user2@cisco.com password 0 lab
spe 1/0 1/7
firmware location system:/ucode/mica_port_firmware
spe 2/0 2/9
firmware location system:/ucode/mica_port_firmware
!
!
resource-pool disable
clock timezone est 2
!
ip subnet-zero
no ip domain-lookup
ip host CALLGEN-SECURITY-V2 10.24.80.28 10.47.0.0
ip host dirt 172.16.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
!
vpdn-group 1
accept-dialin
protocol l2tp
virtual-template 1
terminate-from hostname ISP_LAC
local name ENT_LNS
!
isdn switch-type primary-5ess
!
!
fax interface-type modem
mta receive maximum-recipients 0
!
interface Loopback0
ip address 172.16.0.101 255.255.255.0
!
interface Loopback1
ip address 192.168.0.101 255.255.255.0
!
interface Ethernet0
ip address 10.1.26.71 255.255.255.0
no ip mroute-cache
no cdp enable
!
interface Virtual-Template1
ip unnumbered Loopback0
peer default ip address pool vpdn-pool1
ppp authentication chap
```

```
!
interface Virtual-Template2
ip unnumbered Loopback1
peer default ip address pool vpdn-pool2
ppp authentication chap
!
interface FastEthernet0
no ip address
no ip mroute-cache
shutdown
duplex auto
speed auto
no cdp enable
!
ip local pool vpdn-pool1 172.16.5.1 172.16.128.100
ip local pool vpdn-pool2 10.0.0.1 10.0.0.100
ip default-gateway 10.1.26.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.26.254
ip route 192.168.1.2 255.255.255.255 10.1.26.254
no ip http server
ip pim bidir-enable
!
!
dialer-list 1 protocol ip permit
no cdp run
!
!
radius-server host 172.16.192.80 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
call rsvp-sync
```

RADIUS Tunnel Accounting Records

Example 5-19 and Example 5-20 show RADIUS tunnel accounting record types.

Example 5-19 RADIUS Tunnel Accounting Record

```
User-Name = gomer1@hello101
NAS-IP-Address = 23.1.2.10
NAS-Port = 550
Service-Type = Framed
Framed-Protocol = PPP
Ascend-Multilink-ID = 2877
Tunnel-Type_tag0 = L2TP
Tunnel-Medium-Type_tag0 = IPv4
Tunnel-Client-Endpoint_tag0 = 10.2.2.1
Tunnel-Server-Endpoint_tag0 = 10.2.2.2
Acct-Status-Type = Tunnel-Link-Start
Acct-Delay-Time = 0
Acct-Session-Id = 00000B42
Acct-Authentic = RADIUS
Acct-Multi-Session-Id = 00000B3D
Tunnel-Client-Auth-ID_tag0 = LAC1
Tunnel-Server-Auth-ID_tag0 = LNS1
NAS-Port-Type = Virtual
Acct-Tunnel-Connection = 1088401809
```

Example 5-20 RADIUS Tunnel Accounting Record

```
Wed, 15 Jan 2003 16:34:27
User-Name = gomer1@hello101
NAS-IP-Address = 23.1.2.10
NAS-Port = 550
Service-Type = Framed
Framed-Protocol = PPP
Ascend-Multilink-ID = 2877
Ascend-PreSession-Time = 0
Tunnel-Type_tag0 = L2TP
Tunnel-Medium-Type_tag0 = IPv4
Tunnel-Client-Endpoint_tag0 = 10.2.2.1
Tunnel-Server-Endpoint_tag0 = 10.2.2.2
Ascend-Pre-Input-Packets = 0
Ascend-Pre-Input-Octets = 0
Acct-Status-Type = Tunnel-Link-Stop
Acct-Delay-Time = 0
Acct-Input-Octets = 462
Acct-Output-Octets = 293
Acct-Session-Id = 00000B42
Acct-Authentic = RADIUS
Acct-Session-Time = 45
Acct-Input-Packets = 11
Acct-Output-Packets = 12
Acct-Terminate-Cause = User Request
Acct-Multi-Session-Id = 00000B3D
Acct-Link-Count = 250
Tunnel-Client-Auth-ID_tag0 = LAC1
Tunnel-Server-Auth-ID_tag0 = LNS1
Ascend-Connect-Progress = LAN-Session-Up
NAS-Port-Type = Virtual
Acct-Tunnel-Connection = 1088401809
Ascend-Disconnect-Cause = PPP-Rcv-Terminate-Req
Ascend-Num-In-Multilink = 250
Acct-Tunnel-Packets-Lost = 0
Ascend-Pre-Output-Octets = 0
Ascend-Pre-Output-Packets = 0
```

Note For additional accounting examples, see the "Configuring Accounting" chapter in the *Cisco IOS Security Configuration Guide, Release 12.2*.

Tunnel Authentication Configuration Examples

This section provides the following tunnel authentication configuration examples:

- LNS Configuration to Support RADIUS Tunnel Authentication, page 5-51
- RADIUS Configuration to Support Tunnel Authentication, page 5-51

LNS Configuration to Support RADIUS Tunnel Authentication

The following example is an LNS configuration that supports RADIUS tunnel authentication. In this configuration, a RADIUS server group is defined by using the **aaa group server radius VPDN-Group** command. The **aaa authorization network mymethodlist group VPDN-Group** command queries RADIUS for network authorization.

```
aaa group server radius VPDN-Group
server 64.102.48.91 auth-port 1645 acct-port 1646
aaa authorization network mymethodlist group VPDN-Group
vpdn tunnel authorization network mymethodlist
vpdn tunnel authorization virtual-template 10
```

RADIUS Configuration to Support Tunnel Authentication

The following example is a RADIUS configuration that allows the LNS to terminate L2TP tunnels from a LAC. In this configuration, *VirtualTemplate10* is used to clone a VAI on the LNS.

```
myLACname Password = "cisco"
Service-Type = Outbound,
Tunnel-Type = :0:1@TP,
Tunnel-Medium-Type = :o:IP,
Tunnel-Client-Auth-ID = :0:"myLACname",
Tunnel-Password = :0:"mytunnelpassword",
Cisco:Cisco-Avpair = "vpdn:vpdn-vtemplate=10"
```

Note For additional authentication examples, see the "Configuring Authentication" chapter in the *Cisco IOS Security Configure Guide, Release 12.2*.

Monitoring and Maintaining LNS

To monitor and maintain the features configured on the LNS, enter the following commands in privileged EXEC mode:

Command	Purpose
`Router# show accounting`	Displays accounting records for users currently logged in. Displays active accountable events on the network and helps collect information in the event of a data loss on the accounting server.
`Router# show interfaces virtual-access` *number* [**configuration**]	Displays status, traffic data, and configuration information about the virtual access interface you specify.
`Router# show ip route vrf` *vrf-name*	Displays the IP routing table associated with a VRF.
`Router# show radius statistics`	Displays the RADIUS statistics for accounting and authentication packets.
`Router# show vpdn`	Displays all tunnel and session information for all active sessions and tunnels.
`Router# show vpdn session`	Displays information about active L2TP sessions in a virtual private dialup network (VPDN).
`Router# show vpdn session all username` *username*	Displays statistics about all active L2TP tunnels for the username you specify.

Command	Purpose
`Router# show vpdn tunnel`	Displays information about all active L2TP tunnels in a VPDN.
`Router# show vpdn tunnel all`	Displays information about all active L2TP tunnels.
`Router# debug aaa accounting`	Displays information on accountable events as they occur.
`Router# debug aaa authorization`	Displays information on AAA authorization.
`Router# debug ppp chap`	Displays authentication protocol messages for Challenge Authentication Protocol (CHAP) packet exchanges. This command is useful when a CHAP authentication failure occurs due to a configuration mismatch between devices. Verifying and correcting any username and password mismatch resolves the problem.
`Router# debug ppp negotiation`	Displays information on traffic and exchanges in an internetwork implementing PPP.
`Router# debug ppp negotiation chap`	Used to decipher a CHAP negotiation problem due to a connectivity problem between a Cisco and non-Cisco device.
`Router# debug radius`	Displays information associated with RADIUS.
`Router# debug vpdn events`	Displays L2TP errors and events that are a part of normal tunnel establishment or shutdown for VPNs.
`Router# debug vpdn errors`	Displays errors that prevent a tunnel from being established or errors that cause an established tunnel to be closed.

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco Systems technical support personnel. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.