



RFC-2867 RADIUS Tunnel Accounting

The RFC-2867 RADIUS Tunnel Accounting introduces six new RADIUS accounting types that are used with the RADIUS accounting attribute Acct-Status-Type (attribute 40), which indicates whether an accounting request marks the beginning of user service (start) or the end (stop).

This feature also introduces two new virtual private virtual private dialup network (VPDN) commands that help users better troubleshoot VPDN session events.

History for RFC-2867 RADIUS Tunnel Accounting

Release	Modification
12.2(15)B	This feature was introduced on the Cisco 6400 series, Cisco 7200 series, and the Cisco 7400 series routers.
12.3(4)T	This feature was integrated into Cisco IOS Release 12.3(4)T.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for RFC-2867 RADIUS Tunnel Accounting, page 2](#)
- [Information About RFC-2867 RADIUS Tunnel Accounting, page 2](#)
- [How to Configure RADIUS Tunnel Accounting, page 6](#)
- [Configuration Examples for RADIUS Tunnel Accounting, page 8](#)
- [Additional References, page 12](#)
- [Command Reference, page 13](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2002, 2003, 2005 Cisco Systems, Inc. All rights reserved.

Restrictions for RFC-2867 RADIUS Tunnel Accounting

RADIUS tunnel accounting works only with L2TP tunnel support.

Information About RFC-2867 RADIUS Tunnel Accounting

To use RADIUS tunnel attributes and commands, you should understand the following concepts:

- [Benefits of RFC-2867 RADIUS Tunnel Accounting, page 2](#)
- [RADIUS Attributes Support for RADIUS Tunnel Accounting, page 2](#)

Benefits of RFC-2867 RADIUS Tunnel Accounting

Without RADIUS tunnel accounting support, VPDN with network accounting, which allows users to determine tunnel-link status changes, did not report all possible attributes to the accounting record file. Now that all possible attributes can be displayed, users can better verify accounting records with their Internet Service Providers (ISPs).

RADIUS Attributes Support for RADIUS Tunnel Accounting

[Table 1](#) outlines the new RADIUS accounting types that are designed to support the provision of compulsory tunneling in dialup networks; that is, these attribute types allow you to better track tunnel status changes.



Note

The accounting types are divided into two separate tunnel types so users can decide if they want tunnel type, tunnel-link type, or both types of accounting.

Table 1 RADIUS Accounting Types for the Acct-Status-Type Attribute

Type-Name	Number	Description	Additional Attributes ¹
Tunnel-Start	9	Marks the beginning of a tunnel setup with another node.	<ul style="list-style-type: none"> • User-Name (1)—from client • NAS-IP-Address (4)—from AAA • Acct-Delay-Time (41)—from AAA • Event-Timestamp (55)—from AAA • Tunnel-Type (64)—from client • Tunnel-Medium-Type (65)—from client • Tunnel-Client-Endpoint (66)—from client • Tunnel-Server-Endpoint (67)—from client • Acct-Tunnel-Connection (68)—from client
Tunnel-Stop	10	Marks the end of a tunnel connection to or from another node.	<ul style="list-style-type: none"> • User-Name (1)—from client • NAS-IP-Address (4)—from AAA • Acct-Delay-Time (41)—from AAA • Acct-Input-Octets (42)—from AAA • Acct-Output-Octets (43)—from AAA • Acct-Session-Id (44)—from AAA • Acct-Session-Time (46)—from AAA • Acct-Input-Packets (47)—from AAA • Acct-Output-Packets (48)—from AAA • Acct-Terminate-Cause (49)—from AAA • Acct-Multi-Session-Id (51)—from AAA • Event-Timestamp (55)—from AAA • Tunnel-Type (64)—from client • Tunnel-Medium-Type (65)—from client • Tunnel-Client-Endpoint (66)—from client • Tunnel-Server-Endpoint (67)—from client • Acct-Tunnel-Connection (68)—from client • Acct-Tunnel-Packets-Lost (86)—from client

Table 1 RADIUS Accounting Types for the Acct-Status-Type Attribute (continued)

Type-Name	Number	Description	Additional Attributes ¹
Tunnel-Reject	11	Marks the rejection of a tunnel setup with another node.	<ul style="list-style-type: none"> • User-Name (1)—from client • NAS-IP-Address (4)—from AAA • Acct-Delay-Time (41)—from AAA • Acct-Terminate-Cause (49)—from client • Event-Timestamp (55)—from AAA • Tunnel-Type (64)—from client • Tunnel-Medium-Type (65)—from client • Tunnel-Client-Endpoint (66)—from client • Tunnel-Server-Endpoint (67)—from client • Acct-Tunnel-Connection (68)—from client
Tunnel-Link-Start	12	Marks the creation of a tunnel link. Only some tunnel types (Layer 2 Transport Protocol [L2TP]) support the multiple links per tunnel; this value should be included only in accounting packets for tunnel types that support multiple links per tunnel.	<ul style="list-style-type: none"> • User-Name (1)—from client • NAS-IP-Address (4)—from AAA • NAS-Port (5)—from AAA • Acct-Delay-Time (41)—from AAA • Event-Timestamp (55)—from AAA • Tunnel-Type (64)—from client • Tunnel-Medium-Type (65)—from client • Tunnel-Client-Endpoint (66)—from client • Tunnel-Server-Endpoint (67)—from client • Acct-Tunnel-Connection (68)—from client

Table 1 RADIUS Accounting Types for the Acct-Status-Type Attribute (continued)

Type-Name	Number	Description	Additional Attributes ¹
Tunnel-Link-Stop	13	Marks the end of a tunnel link. Only some tunnel types (L2TP) support the multiple links per tunnel; this value should be included only in accounting packets for tunnel types that support multiple links per tunnel.	<ul style="list-style-type: none"> • User-Name (1)—from client • NAS-IP-Address (4)—from AAA • NAS-Port (5)—from AAA • Acct-Delay-Time (41)—from AAA • Acct-Input-Octets (42)—from AAA • Acct-Output-Octets (43)—from AAA • Acct-Session-Id (44)—from AAA • Acct-Session-Time (46)—from AAA • Acct-Input-Packets (47)—from AAA • Acct-Output-Packets (48)—from AAA • Acct-Terminate-Cause (49)—from AAA • Acct-Multi-Session-Id (51)—from AAA • Event-Timestamp (55)—from AAA • NAS-Port-Type (61)—from AAA • Tunnel-Type (64)—from client • Tunnel-Medium-Type (65)—from client • Tunnel-Client-Endpoint (66)—from client • Tunnel-Server-Endpoint (67)—from client • Acct-Tunnel-Connection (68)—from client • Acct-Tunnel-Packets-Lost (86)—from client
Tunnel-Link-Reject	14	Marks the rejection of a tunnel setup for a new link in an existing tunnel. Only some tunnel types (L2TP) support the multiple links per tunnel; this value should be included only in accounting packets for tunnel types that support multiple links per tunnel.	<ul style="list-style-type: none"> • User-Name (1)—from client • NAS-IP-Address (4)—from AAA • Acct-Delay-Time (41)—from AAA • Acct-Terminate-Cause (49)—from AAA • Event-Timestamp (55)—from AAA • Tunnel-Type (64)—from client • Tunnel-Medium-Type (65)—from client • Tunnel-Client-Endpoint (66)—from client • Tunnel-Server-Endpoint (67)—from client • Acct-Tunnel-Connection (68)—from client

1. If the specified tunnel type is used, these attributes should also be included in the accounting request packet.

How to Configure RADIUS Tunnel Accounting

This section contains the following procedures

- [Enabling Tunnel Type Accounting Records, page 6](#)
- [Verifying RADIUS Tunnel Accounting, page 8](#)

Enabling Tunnel Type Accounting Records

Use this task to configure your LAC to send tunnel and tunnel-link accounting records to be sent to the RADIUS server.

VPDN Tunnel Events

Two new command line interfaces (CLIs)—vpdn session accounting network (tunnel-link-type records) and vpdn tunnel accounting network (tunnel-type records)—are supported to help identify the following events:

- A VPDN tunnel is brought up or destroyed
- A request to create a VPDN tunnel is rejected
- A user session within a VPDN tunnel is brought up or brought down
- A user session create request is rejected



Note

The first two events are tunnel-type accounting records: authentication, authorization, and accounting (AAA) sends Tunnel-Start, Tunnel-Stop, or Tunnel-Reject accounting records to the RADIUS server. The next two events are tunnel-link-type accounting records: AAA sends Tunnel-Link-Start, Tunnel-Link-Stop, or Tunnel-Link-Reject accounting records to the RADIUS server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa accounting network** { **default** | *list-name* } { **start-stop** | **stop-only** | **wait-start** | none }
group *groupname*
4. **vpdn enable**
5. **vpdn tunnel accounting network** *list-name*
6. **vpdn session accounting network** *list-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# <code>aaa accounting network</code> { <code>default</code> <code>list-name</code> } { <code>start-stop</code> <code>stop-only</code> <code>wait-start</code> <code>none</code> } <code>group</code> <i>groupname</i>	Enables network accounting. <ul style="list-style-type: none"> default—If the default network accounting method-list is configured and no additional accounting configurations are enabled on the interface, network accounting is enabled by default. If either the vpdn session accounting network command or the vpdn tunnel accounting network command is linked to the default method-list, all tunnel and tunnel-link accounting records are enabled for those sessions. <i>list-name</i>—The <i>list-name</i> defined in the aaa accounting command must be the same as the <i>list-name</i> defined in the VPDN command; otherwise, accounting will not occur.
Step 4	Router(config)# <code>vpdn enable</code>	Enables virtual private dialup networking on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (if applicable).
Step 5	Router(config)# <code>vpdn tunnel accounting network</code> <i>list-name</i>	Enables Tunnel-Start, Tunnel-Stop, and Tunnel-Reject accounting records. <ul style="list-style-type: none"> <i>list-name</i>—The <i>list-name</i> must match the <i>list-name</i> defined in the aaa accounting command; otherwise, network accounting will not occur.
Step 6	Router(config)# <code>vpdn session accounting network</code> <i>list-name</i>	Enables Tunnel-Link-Start, Tunnel-Link-Stop, and Tunnel-Link-Reject accounting records. <ul style="list-style-type: none"> <i>list-name</i>—The <i>list-name</i> must match the <i>list-name</i> defined in the aaa accounting command; otherwise, network accounting will not occur.

What To Do Next

After you have enabled RADIUS tunnel accounting, you can verify your configuration via the following optional task “[Verifying RADIUS Tunnel Accounting](#).”

Verifying RADIUS Tunnel Accounting

Use either one or both of the following optional steps to verify your RADIUS tunnel accounting configuration.

SUMMARY STEPS

1. **enable**
2. **show accounting**
3. **show vpdn [session | tunnel]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	Router# show accounting	Displays the active accountable events on the network and helps collect information in the event of a data loss on the accounting server.
Step 3	Router# show vpdn [session] [tunnel]	Displays information about active L2TP tunnel and message identifiers in a VPDN. <ul style="list-style-type: none"> • session—Displays a summary of the status of all active tunnels. • tunnel—Displays information about all active L2TP tunnels in summary-style format.

Configuration Examples for RADIUS Tunnel Accounting

This section provides the following configuration examples:

- [Configuring RADIUS Tunnel Accounting on LAC: Example, page 8](#)
- [Configuring RADIUS Tunnel Accounting on LNS: Example, page 10](#)

Configuring RADIUS Tunnel Accounting on LAC: Example

The following example shows how to configure your L2TP access concentrator (LAC) to send tunnel and tunnel-link accounting records to the RADIUS server:

```
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
```

```
aaa session-id common
enable secret 5 $1$IDjH$iL7puCja1RMlyOM.JAeuf/
enable password lab
!
username ISP_LAC password 0 tunnelpass
!
!
resource-pool disable
!
!
ip subnet-zero
ip cef
no ip domain-lookup
ip host dirt 171.69.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
vpdn search-order domain dnis
!
vpdn-group 1
  request-dialin
  protocol l2tp
  domain cisco.com
  initiate-to ip 10.1.26.71
  local name ISP_LAC
!
isdn switch-type primary-5ess
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
controller T1 7/4
  framing esf
  linecode b8zs
  pri-group timeslots 1-24
!
!
!
interface FastEthernet0/0
  ip address 10.1.27.74 255.255.255.0
  no ip mroute-cache
  duplex half
  speed auto
  no cdp enable
!
interface FastEthernet0/1
  no ip address
  no ip mroute-cache
  shutdown
  duplex auto
  speed auto
  no cdp enable
!
interface Serial7/4:23
  ip address 60.0.0.2 255.255.255.0
  encapsulation ppp
  dialer string 2000
  dialer-group 1
  isdn switch-type primary-5ess
  ppp authentication chap
!
```

```

interface Group-Async0
 no ip address
 shutdown
 group-range 1/00 3/107
 !
 ip default-gateway 10.1.27.254
 ip classless
 ip route 0.0.0.0 0.0.0.0 10.1.27.254
 no ip http server
 ip pim bidir-enable
 !
 !
 dialer-list 1 protocol ip permit
 no cdp run
 !
 !
 radius-server host 172.19.192.26 auth-port 1645 acct-port 1646 key rad123
 radius-server retransmit 3
 call rsvp-sync
 !

```

Configuring RADIUS Tunnel Accounting on LNS: Example

The following example shows how to configure your L2TP network server (LNS) to send tunnel and tunnel-link accounting records to the RADIUS server:

```

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 64.24.80.28 3.47.0.0
 ip host dirt 171.69.1.129
 !
 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 70.0.0.101 255.255.255.0
!
interface Loopback1
 ip address 80.0.0.101 255.255.255.0
!
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 70.0.0.1 70.0.0.100
ip local pool vpdn-pool2 80.0.0.1 80.0.0.100
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 90.1.1.2 255.255.255.255 10.1.26.254
no ip http server
ip pim bidir-enable
!
!
dialer-list 1 protocol ip permit
no cdp run
!
!
radius-server host 172.19.192.80 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
call rsvp-sync
```

Additional References

The following sections provide references related to RFC-2867 RADIUS Tunnel Accounting.

Related Documents

Related Topic	Document Title
RADIUS attributes	The appendix “RADIUS Attributes” in the <i>Cisco IOS Security Configuration Guide</i>
Vpdn	The chapter “Configuring Virtual Private Networks” in the <i>Cisco IOS Dial Technologies Configuration Guide</i>
Network accounting	The chapter “Configuring Accounting” in the <i>Cisco IOS Security Configuration Guide</i>

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2867	<i>RADIUS Accounting Modifications for Tunnel Protocol Support</i>

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents modified commands only.

- [aaa accounting](#)
- [vpdn session accounting network](#)
- [vpdn tunnel accounting network](#)

aaa accounting

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the **aaa accounting** command in global configuration mode. To disable AAA accounting, use the **no** form of this command.

```
aaa accounting {auth-proxy | system | network | exec | connection | commands level} {default |
list-name} [vrf vrf-name] {start-stop | stop-only | none} [broadcast] group groupname
```

```
no aaa accounting {auth-proxy | system | network | exec | connection | commands level} {default
| list-name} [vrf vrf-name] [broadcast] group groupname
```

Syntax Description

auth-proxy	Provides information about all authenticated-proxy user events.
system	Performs accounting for all system-level events not associated with users, such as reloads.
network	Runs accounting for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Protocols (NCPs), and AppleTalk Remote Access Protocol (ARAP).
exec	Runs accounting for EXEC shell session. This keyword might return user profile information such as what is generated by the autocommand command.
connection	Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler and disassembler (PAD), and rlogin.
commands level	Runs accounting for all commands at the specified privilege level. Valid privilege level entries are integers from 0 through 15.
default	Uses the listed accounting methods that follow this argument as the default list of methods for accounting services.
<i>list-name</i>	Character string used to name the list of at least one of the accounting methods described in Table 2 .
vrf vrf-name	(Optional) Specifies a virtual route forwarding (VRF) configuration. Note VRF is used <i>only</i> with system accounting.
start-stop	Sends a “start” accounting notice at the beginning of a process and a “stop” accounting notice at the end of a process. The “start” accounting record is sent in the background. The requested user process begins regardless of whether the “start” accounting notice was received by the accounting server.
stop-only	Sends a “stop” accounting notice at the end of the requested user process.
none	Disables accounting services on this line or interface.
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
group group-name	At least one of the keywords described in Table 3 .

Defaults

AAA accounting is disabled.

Command Modes Global configuration

Command History	Release	Modification
	10.3	This command was introduced.
	12.0(5)T	Group server support was added.
	12.1(1)T	The broadcast keyword was introduced on the Cisco AS5300 and Cisco AS5800 universal access servers.
	12.1(5)T	The auth-proxy keyword was added.
	12.2(1)DX	The vrf keyword and <i>vrf-name</i> argument were introduced on the Cisco 7200 series and Cisco 7401ASR.
	12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(13)T	The vrf keyword and <i>vrf-name</i> argument were integrated into Cisco IOS Release 12.2(13)T.
	12.2(15)B	The tunnel and tunnel-link accounting methods were introduced.
	12.3(4)T	The tunnel and tunnel-link accounting methods were integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines Use the **aaa accounting** command to enable accounting and to create named method lists that define specific accounting methods on a per-line or per-interface basis.

[Table 2](#) contains descriptions of keywords for aaa accounting methods.

Table 2 *aaa accounting Methods*

Keyword	Description
group radius	Uses the list of all RADIUS servers for authentication as defined by the aaa group server radius command.
group tacacs+	Uses the list of all TACACS+ servers for authentication as defined by the aaa group server tacacs+ command.
group <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group <i>group-name</i> .

In [Table 2](#), the **group radius** and **group tacacs+** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Cisco IOS software supports the following two methods of accounting:

- **RADIUS**—The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.
- **TACACS+**—The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

Method lists for accounting define the way accounting will be performed. Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for particular types of accounting services. Create a list by entering the *list-name* and the *method*, where *list-name* is any character string used to name this list (excluding the names of methods, such as RADIUS or TACACS+) and *method* identifies the methods to be tried in sequence as given.

If the **aaa accounting** command for a particular accounting type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this accounting type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no accounting takes place.

Named accounting method lists are specific to the indicated type of accounting. Method list keywords are described in [Table 3](#).

Table 3 *aaa accounting Method List Keywords*

Keyword	Description
auth-proxy	Creates a method list to provide accounting information about all authenticated hosts that use the authentication proxy service.
commands	Creates a method list to provide accounting information about specific, individual EXEC commands associated with a specific privilege level.
connection	Creates a method list to provide accounting information about all outbound connections made from the network access server.
exec	Creates a method list to provide accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times.
network	Creates a method list to provide accounting information for SLIP, PPP, NCPs, and ARAP sessions.
resource	Creates a method list to provide accounting records for calls that have passed user authentication or calls that failed to be authenticated.
tunnel	Creates a method list to provide accounting records (Tunnel-Start, Tunnel-Stop, and Tunnel-Reject) for virtual private dialup network (VPDN) tunnel status changes.
tunnel-link	Creates a method list to provide accounting records (Tunnel-Link-Start, Tunnel-Link-Stop, and Tunnel-Link-Reject) for VPDN tunnel-link status changes.



Note

System accounting does not use named accounting lists; you can define the default list only for system accounting.

For minimal accounting, include the **stop-only** keyword to send a “stop” record accounting notice at the end of the requested user process. For more accounting, you can include the **start-stop** keyword, so that RADIUS or TACACS+ sends a “start” accounting notice at the beginning of the requested process and a “stop” accounting notice at the end of the process. Accounting is stored only on the RADIUS or TACACS+ server. The **none** keyword disables accounting services for the specified line or interface.

To specify an accounting configuration for a particular VRF, specify a default system accounting method list, and use the **vrf** keyword and *vrf-name* argument. System accounting does not have knowledge of VRF unless specified.

When AAA accounting is activated, the network access server monitors either RADIUS accounting attributes or TACACS+ AV pairs pertinent to the connection, depending on the security method you have implemented. The network access server reports these attributes as accounting records, which are then stored in an accounting log on the security server. For a list of supported RADIUS accounting attributes, refer to the appendix “RADIUS Attributes” in the *Cisco IOS Security Configuration Guide*. For a list of supported TACACS+ accounting AV pairs, refer to the appendix “TACACS+ Attribute-Value Pairs” in the *Cisco IOS Security Configuration Guide*.

**Note**

This command cannot be used with TACACS or extended TACACS.

Examples

The following example defines a default commands accounting method list, where accounting services are provided by a TACACS+ security server, set for privilege level 15 commands with a stop-only restriction.

```
aaa accounting commands 15 default stop-only group tacacs+
```

The following example defines a default auth-proxy accounting method list, where accounting services are provided by a TACACS+ security server with a start-stop restriction. The **aaa accounting** command activates authentication proxy accounting.

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization auth-proxy default group tacacs+
aaa accounting auth-proxy default start-stop group tacacs+
```

The following example defines a default system accounting method list, where accounting services are provided by RADIUS security server “sg_water” with a start-stop restriction. The **aaa accounting** command specifies accounting for vrf “water.”

```
aaa accounting system default vrf water start-stop group sg_water
```

The following example shows how to enable network accounting and send tunnel and tunnel-link accounting records to the RADIUS server. (Tunnel-Reject and Tunnel-Link-Reject accounting records are automatically sent if either start or stop records are configured.)

```
aaa accounting network tunnel start-stop group radius
aaa accounting network session start-stop group radius
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa group server tacacs	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
tacacs-server host	Specifies a TACACS+ server host.

vpdn session accounting network

To enable tunnel-link type accounting records to be sent to the RADIUS server, use the **vpdn session accounting network** command in global configuration mode. To disable tunnel-link type accounting records, use the **no** form of this command.

vpdn session accounting network *list-name*

no vpdn session accounting network *list-name*

Syntax Description

<i>list-name</i>	Character string used to name the list of at least one accounting method. The <i>list-name</i> value must match the <i>list-name</i> value defined in the aaa accounting command; otherwise, network accounting will not occur.
------------------	--

Defaults

Tunnel-link type accounting records are not sent.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Before you enable the **vpdn session accounting network** command, you must enable network accounting by using the **aaa accounting** command.



Note

If the default network accounting method list is configured and no additional accounting configurations are enabled on the interface, network accounting is enabled by default.

If the **vpdn session accounting network** command is linked to the default method list, all tunnel-link accounting records are enabled for those sessions.

This command displays the following tunnel-link accounting type records, which are used with the RADIUS accounting attribute Acct-Status-Type (attribute 40):

- Tunnel-Link-Start (12)—Marks the creation of a tunnel link.
- Tunnel-Link-Stop (13)—Marks the end of a tunnel link.



Note

Only some tunnel types (such as Layer 2 Transport Protocol [L2TP]) support the multiple links per tunnel; these values should be included only in accounting packets for tunnel types that support multiple links per tunnel.

- Tunnel-Link-Reject (14)—Marks the rejection of a tunnel setup for a new link in an existing tunnel. Only some tunnel types (L2TP) support the multiple links per tunnel; this value should be included only in accounting packets for tunnel types that support multiple links per tunnel.

**Note**

If either Tunnel-Link-Start or Tunnel-Link-Stop are enabled, Tunnel-Link-Reject will be sent, even if it has not been enabled.

Examples

The following example shows how to configure an L2TP access concentrator (LAC) to send tunnel-link type accounting records to the RADIUS server:

```
aaa accounting network m1 start-stop group radius
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
vpdn search-order domain dnis
!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain cisco.com
 initiate-to ip 10.1.1.1
 local name ISP_LAC
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
vpdn tunnel accounting network	Enables tunnel type accounting records to be sent to the RADIUS server.

vpng tunnel accounting network

To enable tunnel type accounting records to be sent to the RADIUS server, use the **vpng tunnel accounting network** command in global configuration mode. To disable tunnel type accounting records, use the **no** form of this command.

vpng tunnel accounting network *list-name*

no vpng tunnel accounting network *list-name*

Syntax Description

<i>list-name</i>	Character string used to name the list of at least one accounting method. The <i>list-name</i> value must match the <i>list-name</i> value defined in the aaa accounting command; otherwise, network accounting will not occur.
------------------	--

Defaults

Tunnel type accounting records are not sent.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Before you enable the **vpng tunnel accounting network** command, you must enable network accounting by using the **aaa accounting** command.



Note

If the default network accounting method list is configured and no additional accounting configurations are enabled on the interface, network accounting is enabled by default.

If the **vpng tunnel accounting network command** is linked to the default method list, all tunnel accounting records are enabled for those sessions.

This command displays the following tunnel accounting type records, which are used with the RADIUS accounting attribute Acct-Status-Type (attribute 40):

Tunnel-Start (9)—Marks the beginning of a tunnel setup with another node.

Tunnel-Stop (10)—Marks the end of a tunnel connection to or from another node.

Tunnel-Reject (11)—Marks the rejection of a tunnel setup with another node.



Note

If either Tunnel-Start or Tunnel-Stop are enabled, Tunnel-Reject will be sent, even if it has not been enabled.

Examples

The following example shows how to configure an L2TP access concentrator (LAC) to send tunnel type accounting records to the RADIUS server:

```
! The method list defined in the VPDN command must be the same as the method list defined
! in aaa accounting command; otherwise, accounting will not occur.
aaa accounting network m1 start-stop group radius
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
vpdn search-order domain dnis
!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain cisco.com
 initiate-to ip 10.1.1.1
 local name ISP_LAC
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
vpdn session accounting network	Enables tunnel-link type accounting records to be sent to the RADIUS server.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

© 2002, 2003, 2005 Cisco Systems, Inc. All rights reserved.

