



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 dialup network (VPDN) commands that help users better troubleshoot VPDN session events.

- [Restrictions for RFC-2867 RADIUS Tunnel Accounting, on page 1](#)
- [Information About RFC-2867 RADIUS Tunnel Accounting, on page 1](#)
- [How to Configure RADIUS Tunnel Accounting, on page 6](#)
- [Configuration Examples for RADIUS Tunnel Accounting, on page 9](#)
- [Additional References, on page 12](#)
- [Feature Information for RFC-2867 RADIUS Tunnel Accounting, on page 13](#)

Restrictions for RFC-2867 RADIUS Tunnel Accounting

RADIUS tunnel accounting works only with L2TP tunnel support.

Information About RFC-2867 RADIUS Tunnel Accounting

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

The table below 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 |

| Type-Name | Number | Description | Additional Attributes ¹ |
|-------------|--------|---|---|
| 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 |

| 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 |

| 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 |

| Type-Name | Number | Description | Additional Attributes ¹ |
|--------------------|--------|--|--|
| 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

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.

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.

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

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: <pre>Router> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Router# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | Router(config)# aaa accounting network default <i>list-name</i> { start-stop stop-only wait-start none group <i>groupname</i> Example: Example: Example: Example: Example: Example: Example: Example: | 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. <p>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.</p> <ul style="list-style-type: none"> • <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. |

| | Command or Action | Purpose |
|---------------|---|---|
| | Example: Example: <pre>Router(config)# aaa accounting network m1 start-stop group radius</pre> | |
| Step 4 | Router(config)# vpdn enable Example: <pre>Router(config)# vpdn enable</pre> | 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)# vpdn tunnel accounting network <i>list-name</i> Example: <pre>Router(config)# vpdn tunnel accounting network m1</pre> | 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)# vpdn session accounting network <i>list-name</i> Example: <pre>Router(config)# vpdn session accounting network m1</pre> | 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. Router# **show accounting**
3. Router# **show vpdn [session] [tunnel]**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--------------------------------------|--|
| Step 1 | enable Example: | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |

| | Command or Action | Purpose |
|---------------|---|--|
| | Router> enable | |
| Step 2 | Router# show accounting Example: 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] Example: Example: Example: Router# show vpdn session | 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

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 172.16.1.129
!
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
!
mta receive maximum-recipients 0
!
interface GigabitEthernet0/0/0
 ip address 10.1.27.74 255.255.255.0
 no ip mroute-cache
 duplex half
 speed auto
 no cdp enable
!
interface FastEthernet0/0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
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
!
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 172.24.80.28 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  
!  
mta receive maximum-recipients 0  
!  
interface Loopback0  
    ip address 192.168.70.101 255.255.255.0  
!  
interface Loopback1  
    ip address 192.168.80.101 255.255.255.0  
!  
interface FastEthernet0/0/0  
    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 FastEthernet0/0/1  
    no ip address  
    no ip mroute-cache  
    shutdown  
    duplex auto  
    speed auto  
    no cdp enable  
!  
ip local pool vpdn-pool1 192.168.70.1 192.168.70.100  
ip local pool vpdn-pool2 192.168.80.1 192.168.80.100  
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 10.90.1.2 255.255.255.255 10.1.26.254  
no ip http server  
ip pim bidir-enable  
!  
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 | “RADIUS Attributes Overview and RADIUS IETF Attributes” in the <i>Cisco IOS XE Security Configuration Guide: Securing User Services</i> , Release 2 |
| VPDN | <i>Cisco IOS XE VPDN Configuration Guide</i> , Release 2 |
| Network accounting | “Configuring Accounting” in the <i>Cisco IOS XE Security Configuration Guide: Securing User Services</i> , Release 2 |
| Commands | <ul style="list-style-type: none"> • <i>Cisco IOS Security Command Reference</i> • <i>Cisco IOS VPDN Command Reference</i> |

Standards

| Standards | Title |
|---|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

MIBs

| MIBs | MIBs Link |
|--|--|
| No new or modified MIBs are supported by this feature, and support for existing standards has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS XE software 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 |
|---|---|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | http://www.cisco.com/techsupport |

Feature Information for RFC-2867 RADIUS Tunnel Accounting

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for RFC-2867 RADIUS Tunnel Accounting

| Feature Name | Releases | Feature Information |
|-----------------------------------|--------------------------|--|
| RFC-2867 RADIUS Tunnel Accounting | Cisco IOS XE Release 2.1 | <p>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).</p> <p>This feature also introduces two new virtual private virtual private dialup network (VPDN) commands that help users better troubleshoot VPDN session events.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified: aaa accounting, vpdn session accounting network, vpdn tunnel accounting network.</p> |

