RFC-2867 RADIUS Tunnel Accounting

The RFC-2867 RADIUS Tunnel Accounting feature 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).

Configuration Information

Configuration information is included in the "Configuring AAA for VPDNs" module in the *Cisco IOS VPDN Configuration Guide*, Release 12.4T, at the following URL:

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcg/tvpdn_c/vpc2auht.htm

Command Reference

This section documents modified commands.

- **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. **Note** When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes.
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.
list-name	Character string used to name the list of at least one of the accounting methods described in Table 1.
vrf *vrf-name*	(Optional) Specifies a virtual route forwarding (VRF) configuration. VRF is used *only* 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 2.

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 *vrf-name* 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 *vrf-name* 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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

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 1 contains descriptions of keywords for aaa accounting methods.

Table 1 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 *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name*.

In Table 1, 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 2.

Table 2 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.

Cisco Service Selection Gateway Broadcast Accounting

To configure Cisco Service Selection Gateway (SSG) broadcast accounting, the *list-name* argument must be ssg_broadcast_accounting. For more information about configuring SSG, see the chapter Configuring Accounting for SSG" in the "*Cisco IOS Service Selection Gateway Configuration Guide*", Release 12.4.

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

list-name	Character string used to name the list of at least one accounting method. The *list-name* vlaue must match the *list-name* 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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

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.

vpdn tunnel accounting network

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

vpdn tunnel accounting network *list-name*

no vpdn tunnel accounting network *list-name*

Syntax Description

list-name	Character string used to name the list of at least one accounting method. The *list-name* value must match the *list-name* 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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Before you enable the **vpdn 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 **vpdn 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.