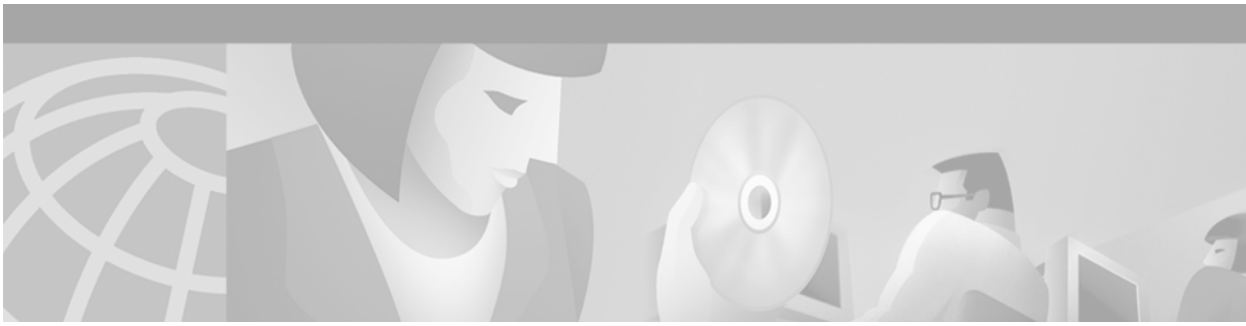

Per VRF AAA

Feature History

Release	Modification
12.2(1)DX	This feature was introduced.
12.2(2)DD	This feature was integrated into Cisco IOS Release 12.2(2)DD. The **ip vrf forwarding** and **radius-server domain-stripping** commands were added.
12.2(4)B	This feature was integrated into Cisco IOS Release 12.2(4)B.

This feature module describes the Per VRF AAA feature. It includes the following sections:

Feature Overview

Using the Per VRF AAA feature, Internet Service Providers (ISPs) can partition authentication, authorization, and accounting (AAA) services based on Virtual Route Forwarding (VRF). This permits the Virtual Home Gateway (VHG) to communicate directly with the customer RADIUS server associated with the customer VPN, without having to go through a RADIUS proxy. Thus, ISPs can scale their VPN offerings more efficiently because they no longer need to proxy AAA to provide their customers the flexibility demanded.

To support Per VRF AAA, AAA must be VRF aware. ISPs must define multiple instances of the same operational parameters—such as AAA server groups, method lists, system accounting, and protocol-specific parameters—and secure the parameters to the VRF partitions.

If an AAA configuration, such as a method list, is uniquely defined many times across the network access server (NAS), the specification of an AAA server that is based on IP addresses and port numbers may create an overlapping of private addresses between VRFs. Securing AAA method lists 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 or Dialed Number Identification Service (DNIS). The server then provides the VPN-specific configuration for the virtual access interface, which 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.

Note Global AAA accounting configurations and some AAA protocol-specific parameters cannot be logically grouped under the Virtual Template configuration.

AAA Server Configurations

To prevent possible overlapping of private addresses between VRFs, AAA servers must be defined in a single global pool that is to be used in the server groups. Servers can no longer be uniquely identified by IP addresses and port numbers.

"Private" servers (servers with private addresses within the default server group that contains all the servers) can be defined within the server group and remain hidden from other groups. The list of servers in server groups includes references to the hosts in the global configuration as well as the definitions of private servers.

Note If private server parameters are not specified, global configurations are used. If global configurations are not specified, default values are used.

All server operational parameters can be configured 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.

Benefits

The Per VRF AAA feature offers the following benefits:

Per VRF AAA Configuration Support

Using the Per VRF AAA feature, ISPs can partition AAA services based on VRF. AAA services are provided on a per-VRF basis. ISPs can allow their customers to control their own AAA services as well as their own networks.

Server Group List Extension

The list of servers in server groups is extended to include the definitions of private servers in addition to references to the hosts in the global configuration.

Restrictions

The Per VRF AAA feature does not support the following features:

- Per VRF AAA is supported only for the RADIUS server.
- All funtionalities must be consistent between the NAS and the AAA servers. The operational parameters should be defined once per VRF rather than set per server group.

Related Documents

- *Cisco IOS Security Command Reference*, Release 12.2
- *Cisco IOS Security Configuration Guide*, Release 12.2

Supported Platforms

- Cisco 7200 series
- Cisco 7401 ASR router

Determining Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at http://www.cisco.com/register.

Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

Before configuring the Per VRF AAA feature, you must enable AAA.

Configuration Tasks

See the following sections for configuration tasks for the Per VRF AAA feature. Each task in the list is identified as either optional or required.

- Configuring Private Server Parameters (required)
- Configuring AAA Accounting for VRF (required)
- Configuring RADIUS-Specific Commands for VRF (required)
- Verifying Per VRF AAA (optional)
- Troubleshooting Per VRF AAA (optional)

Configuring Private Server Parameters

To configure private server operational parameters, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa group server radius group-name`	Groups different RADIUS server hosts into distinct lists and distinct methods. • *group-name*—Character string used to name the group of servers.
Step 2	`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. • *ip-address*—Specifies the IP address of the private RADIUS server host. • *seconds*—(Optional) Specifies the timeout value. Enter a value in the range 1 to 1000. If no timeout value is specified, the global value is used. • *retries*—(Optional) Specifies the retransmit value. Enter a value in the range 0 to 100. If no retransmit value is specified, the global value is used. • *string*—(Optional) Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server. **Note** If private server parameters are not specified, global configurations are used. If global configurations are not specified, default values are used.
Step 3	`Router(config-sg-radius)# ip vrf forwarding vrf-name`	(Optional) Configures the VRF reference of the AAA RADIUS server group. • *vrf-name*—Name assigned to a VRF.

Configuring AAA Accounting for VRF

To configure AAA accounting for VRF, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa authentication ppp list-name method1 [method2...]`	Specifies one or more AAA authentication methods for use on serial interfaces running PPP. • *list-name*—Character string used to name the list of authentication methods tried when a user logs in. • *method1* [*method2...*]—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.
Step 2	`Router(config)# aaa authorization network list-name method1 [method2...]`	Sets parameters that restrict user access to a network. • *list-name*—Character string used to name the list of authentication methods tried when a user logs in. • *method1* [*method2...*]—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 successfully authenticated. – **local**—Uses the local username database for authentication. – **none**—Uses no authentication.

	Command	Purpose
Step 3	`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. • **system default**—Performs accounting for all system-level events not associated with users, such as reloads. • **vrf** *vrf-name*—Specifies a Virtual Route Forwarding (VRF) configuration. • **network**—Runs accounting for all network-related service requests, including SLIP[1], PPP[2], PPP NCPs[3], and ARAP[4]. • **default**—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. • **group** *group-name*—At least one of the keywords described in Table 1 on page 12.
Step 4	`Router(config)# aaa accounting delay-start vrf vrf-name`	Delays generation of the start accounting records until the user IP address is established. • **vrf** *vrf-name*—Enables the specification on a per-VRF basis.
Step 5	`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. • **vrf** *vrf-name*—Enables the specification on a per-VRF basis.

1. SLIP = Serial Line Internet Protocol
2. PPP = Point-to-Point Protocol
3. PPP NCPs = Point-to-Point Protocol Network Control Protocols
4. ARAP = AppleTalk Remote Access Protocol

Configuring RADIUS-Specific Commands for VRF

To configure AAA global RADIUS-specific commands for VRF definition, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface type number`	Configures an interface type and enters interface configuration mode.
Step 2	`Router(config-if)# ip vrf forwarding vrf-name`	Associates a VRF with an interface. • *vrf-name*—Name assigned to a VRF.

	Command	Purpose
Step 3	`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. • *protocol1*[*protocol2...*]—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. • *list-name*—(Optional) Specifies the name of a list of methods of authentication to use. If no list name is specified, the system uses the default. The list is created with the **aaa authentication ppp** command.
Step 4	`Router(config-if)# ppp authorization list-name`	Enables AAA authorization on the selected interface. • *list-name*—(Optional) Specifies the name of a list of authorization methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa authorization** command.
Step 5	`Router(config-if)# ppp accounting default`	Enables AAA accounting services on the selected interface.
Step 6	`Router(config-if)# exit`	Exits interface configuration mode.
Step 7	`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. • *subinterface-name*—Specifies the name of the interface that RADIUS uses for all of its outgoing packets. • **vrf** *vrf-name*—Specifies the per-VRF configuration.
Step 8	`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. • **vrf** *vrf-name*—Specifies the per-VRF configuration.
Step 9	`Router(config)# radius-server domain-stripping vrf vrf-name`	(Optional) Enables VRF-aware domain-stripping. • *vrf-name*—Name assigned to a VRF.

Verifying Per VRF AAA

To verify the Per VRF AAA feature, use the following command in EXEC mode:

Command	Purpose
`Router# show ip route vrf vrf-name`	Displays the IP routing table associated with a VRF. • *vrf-name*—Name assigned to a VRF.

Troubleshooting Per VRF AAA

To troubleshoot the Per VRF AAA feature, use at least one of the following EXEC commands:

Command	Purpose
`Router# debug aaa accounting`	Displays information on accountable events as they occur.
`Router# debug aaa authentication`	Displays information on AAA authentication.
`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.

Configuration Examples

This section provides the following configuration examples:

- Private Server Parameters Configuration Example, page 9
- AAA Accounting for VRF Configuration Example, page 10
- RADIUS-Specific Command Defined Per VRF Example, page 10

Private Server Parameters Configuration Example

The following example shows how to define the sg_water RADIUS group server and associate private servers with it:

```
Router(config)# aaa new-model
Router(config)# aaa group server radius sg_water
Router(config-sg-radius)# server-private 1.1.1.1 timeout 5 retransmit 3 key water
Router(config-sg-radius)# server-private 2.2.2.2 timeout 5 retransmit 3 key water
Router(config-sg-radius)# ip vrf forwarding sg_fire
```

AAA Accounting for VRF Configuration Example

The following example shows how to configure AAA accounting for VRF support:

```
Router(config)# aaa authentication ppp method_list_water group sg_water
Router(config)# aaa authorization network method_list_water group sg_water
Router(config)# aaa accounting network method_list_water start-stop group sg_water
Router(config)# aaa accounting system default vrf water start-stop group sg_water
Router(config)# aaa accounting delay-start vrf water
Router(config)# aaa accounting send stop-record authentication failure vrf water
```

RADIUS-Specific Command Defined Per VRF Example

The following example shows how to configure AAA global RADIUS-specific commands for a VRF definition. In this example, VRF is associated with the “water” interface and selected on method_list_water.

```
Router(config)# interface Virtual-Template1
Router(config-if)# ip vrf forwarding water
Router(config-if)# ppp authentication chap method_list_water
Router(config-if)# ppp authorization method_list_water
Router(config-if)# ppp accounting method_list_water
Router(config-if)# exit
Router(config)# ip radius source-interface Ethernet 0/1 vrf water
Router(config)# radius-server domain-stripping
Router(config)# radius-server attribute 44 include-in-access-req vrf water
```

Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- **aaa accounting**
- **aaa accounting delay-start**
- **aaa accounting send stop-record authentication failure**
- **ip radius source-interface**
- **ip vrf forwarding**
- **radius-server attribute 44 include-in-access-req**
- **radius-server domain-stripping**
- **server-private**

aaa accounting

To enable authentication, authorization, and accounting (AAA) of requested services for billing or security purposes when you use RADIUS, use the **aaa accounting** command in global configuration mode. To disable AAA, 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** | **wait-start** | **none**} [**broadcast**] **group** *group-name*

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

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 SLIP, PPP, PPP NCPs, and 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, LAT[1], TN3270, PAD[2], 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 2.
vrf *vrf-name*	Specifies a Virtual Route Forwarding (VRF) configuration. VRF is used 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.
wait-start	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 does not begin until the “start” accounting notice is received by the server.
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 1.

1. LAT = local-area transport
2. PAD = packet assembler/disassembler

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 added 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 added.
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.

Usage Guidelines

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

Table 1 contains descriptions of accounting method keywords.

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 *group-name*	Uses a subset of RADIUS servers for accounting as defined by the server group *group-name*.

In Table 1, the **group radius** method refers to a set of previously defined RADIUS servers. Use the **radius-server host** command to configure the host server. Use the **aaa group server radius** command to create a named group of servers.

Per VRF AAA supports RADIUS accounting; 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.

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) 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 Methods Lists

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.

Note System accounting does not use named accounting lists; you can only define the default list 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 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 server. Like the **start-stop** keyword, the **wait-start** keyword sends "start" and "stop" accounting notices; however, the requested user process does not begin until the "start" accounting notice is received by the accounting 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 is activated, the network access server monitors RADIUS accounting attributes pertinent to the connection. 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*.

Examples

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

```
aaa accounting commands 15 default stop-only group radius
```

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

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

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 vrf water default start-stop group sg_water
```

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 new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

aaa accounting delay-start

To delay generation of accounting "start" records until the user IP address is established, use the **aaa accounting delay-start** command in global configuration mode. To disable this functionality, use the **no** form of this command.

aaa accounting delay-start [**vrf** *vrf-name*]

no aaa accounting delay-start [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	Specifies the VRF configuration.

Defaults

Accounting records are not delayed.

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.
12.2(1)DX	The **vrf** keyword and *vrf-name* argument were added.
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.

Usage Guidelines

Use the **aaa accounting delay-start** command to delay generation of accounting "start" records until the IP address of the user has been established. Use **vrf** *vrf-name* to delay accounting "start" records per Virtual Route Forwarding (VRF) configuration, which overrides global configurations.

Examples

The following example shows how to delay accounting "start" records until the IP address of the user is established:

```
aaa new-model
aaa authentication ppp default radius
aaa accounting network default start-stop radius
aaa accounting delay-start
radius-server host 172.16.0.0 non-standard
radius-server key rad123
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

aaa accounting send stop-record authentication failure

To generate accounting "stop" records for users who fail to authenticate at login or during session negotiation, use the **aaa accounting send stop-record authentication failure** command in global configuration mode. To stop generating records for users who fail to authenticate at login or during session negotiation, use the **no** form of this command.

aaa accounting send stop-record authentication failure [**vrf** *vrf-name*]

no aaa accounting send stop-record authentication failure [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	Specifies the VRF configuration.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(1)DX	The **vrf** keyword and *vrf-name* argument were added.
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.

Usage Guidelines

Use this command to generate accounting "stop" records for users who fail to authenticate at login or during session negotiation. When the **aaa accounting** command is activated, the Cisco IOS software by default does not generate accounting records for system users who fail login authentication or who succeed in login authentication but fail PPP negotiation for some reason.

Use **vrf** *vrf-name* to generate accounting "stop" records per Virtual Route Forwarding (VRF) configuration, which overrides global configuration.

Examples

The following example shows how to generate "stop" records for users who fail to authenticate at login or during session negotiation on VRF "abc":

```
aaa accounting send stop-record authentication failure vrf abc
```

ip radius source-interface

To force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets, use the **ip radius source-interface** command in global configuration mode. To prevent RADIUS from using the IP address of a specified interface for all outgoing RADIUS packets, use the **no** form of this command.

ip radius source-interface *subinterface-name* [**vrf** *vrf-name*]

no ip radius source-interface

Syntax Description

subinterface-name	Name of the interface that RADIUS uses for all of its outgoing packets.
vrf *vrf-name*	Specifies the per-VRF configuration.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(1)DX	The **vrf** keyword and *vrf-name* argument were added.
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.

Usage Guidelines

Use this command to set the IP address of a subinterface to be used as the source address for all outgoing RADIUS packets. This address is used as long as the interface is in the *up* state. In this way, the RADIUS server can use one IP address entry for every network access client instead of maintaining a list of IP addresses.

This command is especially useful in cases where the router has many interfaces and you want to ensure that all RADIUS packets from a particular router have the same IP address.

The specified interface must have an IP address associated with it. If the specified subinterface does not have an IP address or is in the *down* state, then RADIUS reverts to the default. To avoid this, add an IP address to the subinterface or bring the interface to the *up* state.

Use **vrf** *vrf-name* to configure this command per Virtual Route Forwarding (VRF). Although this command can be configured under the server group, all functionalities must be consistent between the NAS and all AAA servers; thus, this feature is better defined once per VRF rather than per server group.

Note Per-host configurations have precedence over any per-server groups configurations, which have precedence over any global configuration.

Examples

The following example makes RADIUS use the IP address of subinterface "s2" for all outgoing RADIUS packets:

```
ip radius source-interface s2
```

Related Commands

Command	Description
ip telnet source-interface	Allows a user to select an address of an interface as the source address for Telnet connections.
ip tftp source-interface	Allows a user to select the interface whose address will be used as the source address for TFTP connections.

ip vrf forwarding

To configure the VRF reference of an AAA RADIUS server group, use the **ip vrf forwarding** command in server-group configuration mode. To unconfigure ip vrf forwarding so that server groups use the global default routing table, use the **no** form of this command.

ip vrf forwarding *vrf-name*

no ipvrf forwarding *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Defaults

Server groups use the global default routing table.

Command Modes

Server-group configuration

Command History

Release	Modification
12.2(2)DD	This command was introduced in server-group configuration mode.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.

Usage Guidelines

Use this command in server-group configuration mode to configure a VRF reference for any AAA RADIUS server group. This enables dial users to utilize AAA servers in different routing domains.

Examples

The following example configures the VRF user to reference the RADIUS server in a different VRF server group:

```
aaa group server radius sg_global
 server-private 172.16.0.0 timeout 5 retransmit 3

aaa group server radius sg_water
```

```
server-private 10.10.0.0 timeout 5 retransmit 3 key water
ip vrf forwarding water
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
interface Virtual-Template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
server-private	Configures the IP address of the private RADIUS server for the group server.

radius-server attribute 44 include-in-access-req

To send RADIUS attribute 44 (Accounting Session ID) in access request packets before user authentication (including requests for preauthentication), use the **radius-server attribute 44 include-in-access-req** command in global configuration mode. To remove this command from your configuration, use the **no** form of this command.

radius-server attribute 44 include-in-access-req [**vrf** *vrf-name*]

no radius-server attribute 44 include-in-access-req [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	Specifies the per-VRF configuration.

Defaults

RADIUS attribute 44 is not sent in access request packets.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(1)DX	The **vrf** keyword and *vrf-name* argument were added.
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.

Usage Guidelines

There is no guarantee that the Accounting Session IDs will increment uniformly and consistently. In other words, between two calls, the Accounting Session ID can increase by more than one.

The syntax **vrf** *vrf-name* specifies Accounting Session IDs per Virtual Route Forwarding (VRF). Although Accounting Session IDs can be configured under the server group, all functionalities must be consistent between the NAS and all AAA servers; thus, Accounting Session IDs are better defined once per VRF rather than per server group.

Note Per-host Accounting Session ID configurations have precedence over any per-server groups configurations, which have precedence over any global configuration.

Examples The following example shows a configuration that sends RADIUS attribute 44 in access request packets:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 include-in-access-req
```

radius-server domain-stripping

To enable VRF-aware domain-stripping, use the **radius-server domain-stripping** command in global configuration mode. To remove this command from your configuration, use the **no** form of this command.

radius-server domain-stripping [**vrf** *vrf-name*]

no radius-server domain-stripping [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	Specifies the per-VRF configuration.

Defaults RADIUS server domain-stripping is not configured.

Command Modes Global configuration

Command History

Release	Modification
12.2(2)DD	This command was introduced.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.

Usage Guidelines Use the **radius-server domain-stripping** command to strip or truncate the domain from a username. For example, if the username is user1@cisco.com and **radius-server domain-stripping** is configured, only "user1" is sent out as the username.

When the keyword **vrf** *vrf-name* is configured, domain-stripping applies only to the specified VRF.

Examples The following example shows a configuration that strips the domain name from the VRF "abc":

```
radius-server domain-stripping vrf abc
```

Related Commands

Command	Purpose
radius-server directed-request	Allow users logging in to a Cisco server to select the RADIUS server for authentication.

server-private

To configure the IP address of the private RADIUS server for the group server, use the **server-private** command in server-group configuration mode. To remove the associated private server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

server-private *ip-address* [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

no server-private *ip-address* [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

Syntax Description

ip-address	IP address of the private RADIUS server host.
timeout	(Optional) The time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the **radius-server timeout** command. If no timeout value is specified, the global value is used. Enter a value in the range 1 to 1000.
seconds	(Optional) Specifies the timeout value. Enter a value in the range 1 to 1000. If no timeout value is specified, the global value is used.
retransmit	(Optional) The number of times a RADIUS request is resent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the **radius-server retransmit** command.
retries	(Optional) Specifies the retransmit value. Enter a value in the range 0 to 100. If no retransmit value is specified, the global value is used.
key	(Optional) Specifies the authentication and encryption key used between the router and the RADIUS daemon running on this RADIUS server. This key overrides the global setting of the **radius-server key** command. If no key string is specified, the global value is used.
string	(Optional) Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Defaults

If server-private parameters are not specified, global configurations will be used; if global configurations are not specified, default values will be used.

Command Modes

Server-group configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced.
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.

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between VRFs, AAA servers must be defined in a single global pool that is to be used in the server groups; that is, the servers can no longer be uniquely identified by IP addresses and port numbers.

Private servers (servers with private addresses within the default server group that contains all the servers) avoid failover; that is, private servers are not exposed in the global list. Thus, private servers can be defined within the server group and remain hidden from other groups. The list of servers in server groups includes references to the hosts in the global configuration as well as the definitions of private servers.

Note Private servers are not known from any other server group other than the one it is defined within.

Note All server operational parameters can be configured per host, per server group, or globally. Per-host configuration have precedence over any per-server groups configurations, which have precedence over any global configuration.

Examples

The following example shows how to define the sg_water RADIUS group server and associate private servers with it:

```
aaa group server radius sg_water
 server-private 1.1.1.1 timeout 5 retransmit 3 key coke
 server-private 2.2.2.2 timeout 5 retransmit 3 key coke
```

Related Commands

Command	Description
aaa group server	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.

Glossary

AAA—Authentication, authorization, and accounting. Suite of network security services that provide the primary framework through which access control can be set up on your Cisco router or access server.

authentication, authorization, and accounting—See AAA.

L2F—Layer 2 Forwarding. A Layer 2 tunneling protocol that enables an ISP or other access service to create a virtual tunnel to link customer remote sites or remote users with corporate home networks. In particular, a network access server (NAS) at the ISP point of presence (POP) exchanges PPP messages with the remote users and communicates by L2F or L2TP requests and responses with the customer tunnel server to set up tunnels.

L2TP—Layer 2 Tunnel Protocol. A Layer 2 tunneling protocol that enables an ISP or other access service to create a virtual tunnel to link customer remote sites or remote users with corporate home networks. In particular, a network access server (NAS) at the ISP point of presence (POP) exchanges PPP messages with the remote users and communicates by L2F or L2TP requests and responses with the customer tunnel server to set up tunnels.

L2TP access concentrator—See LAC.

L2TP network server—See LNS.

LAC—L2TP access concentrator. A network access server (NAS) to which the client directly connects and through which PPP frames are tunneled to the L2TP network server (LNS). The LAC need only implement the media over which L2TP is to operate to pass traffic to one or more LNSs. The LAC may tunnel any protocol carried within PPP. The LAC initiates incoming calls and receives outgoing calls. A LAC is analogous to an L2F network access server.

LNS—L2TP network server. A termination point for L2TP tunnels, and an access point where PPP frames are processed and passed to higher-layer protocols. An LNS can operate on any platform that terminates PPP. The LNS handles the server side of the L2TP protocol. L2TP relies only on the single medium over which L2TP tunnels arrive. The LNS initiates outgoing calls and receives incoming calls. An LNS is analogous to a home gateway in L2F technology.

NAS—Network access server. Cisco platform (or collection of platforms such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the Public Switched Telephone Network).

network access server—See NAS.

RADIUS—Remote Authentication Dial-In User Service. RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

Remote Authentication Dial-In User Service—See RADIUS.

virtual private networks—See VPN.

Virtual Route Forwarding—See VRF.

VPN—A system that permits dial-in networks to exist remotely to home networks, while giving the appearance of being directly connected. VPNs use L2TP and L2F to terminate the Layer 2 and higher parts of the network connection at the LNS instead of the LAC.

VRF—Virtual Route Forwarding. Initially, a router has only one global default routing/forwarding table. VRFs can be viewed as multiple disjoined routing/forwarding tables, where the routes of a user have no correlation with the routes of another user.