

Per VRF AAA

The Per VRF AAA feature allows ISPs to partition authentication, authorization, and accounting (AAA) services on the basis of Virtual Private Network (VPN) routing and forwarding (VRF) instances, allowing their customers to control some of their own AAA services.

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, allowing access to both customer servers and global service provider servers simultaneously.

In Cisco IOS XE Release 2.4 and later releases, a customer template can be used, which may be stored either locally or remotely, and AAA services can be performed on the information that is stored in the customer template. This feature is referred to as the Dynamic Per VRF AAA feature.

- Prerequisites for Per VRF AAA, on page 1
- Restrictions for Per VRF AAA, on page 1
- Information About Per VRF AAA, on page 2
- How to Configure Per VRF AAA, on page 6
- Configuration Examples for Per VRF AAA, on page 18
- Additional References, on page 26
- Feature Information for Per VRF AAA, on page 27
- Glossary, on page 28

Prerequisites for Per VRF AAA

Before configuring the Per VRF AAA feature, AAA must be enabled. See “How to Configure Per VRF AAA” section on page 6 for more information.

Restrictions for Per VRF AAA

- This feature is supported only for RADIUS servers.
- Operational parameters should be defined once per VRF rather than set per server group, because all functionality must be consistent between the network access server (NAS) and the AAA servers.
- The ability to configure a customer template either locally or remotely is available only for Cisco IOS XE Release 2.4 and later releases.

Information About Per VRF AAA

When you use the Per VRF AAA feature, AAA services can be based on VRF instances. This feature permits the Provider Edge (PE) or Virtual Home Gateway (VHG) to communicate directly with the customer's RADIUS server, which is associated with the customer's Virtual Private Network (VPN), without having to go through a RADIUS proxy. Thus, ISPs can scale their VPN offerings more efficiently because they no longer have to use RADIUS proxies and ISPs can also provide their customers with additional flexibility.

How Per VRF AAA Works

To support AAA on a per customer basis, some AAA features must be made VRF aware. That is, ISPs must be able to define operational parameters--such as AAA server groups, method lists, system accounting, and protocol-specific parameters--and bind those parameters to a particular VRF instance. Defining and binding the operational parameters can be accomplished using one or more of the following methods:

- Virtual private dialup network (VPDN) virtual template or dialer interfaces that are configured for a specific customer
- Locally defined customer templates--Per VPN with customer definitions. The customer template is stored locally on the VHG. This method can be used to associate a remote user with a specific VPN based on the domain name or dialed number identification service (DNIS) and provide the VPN-specific configuration for virtual access interface and all operational parameters for the customer AAA server.
- Remotely defined customer templates--Per VPN with customer definitions that are stored on the service provider AAA server in a RADIUS profile. This method is used to associate a remote user with a specific VPN based on the domain name or DNIS and provide the VPN-specific configuration for the virtual access interface and all operational parameters for the AAA server of the customer.



Note The ability to configure locally or remotely defined customer templates is available only with Cisco IOS XE Release 2.4 and later releases.

AAA Accounting Records

The Cisco implementation of AAA accounting provides "start" and "stop" record support for calls that have passed user authentication. Start and stop records are necessary for users employing accounting records to manage and monitor their networks.

New Vendor-Specific Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (VSA) attribute 26. Attribute 26 encapsulates VSAs, thereby, allowing vendors to support their own extended attributes otherwise not suitable for general use.

The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair." The value is a string of the following format:

```
protocol : attribute sep value *
```

"Protocol" is a value of the Cisco "protocol" attribute for a particular type of authorization. "Attribute" and "value" are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and "sep" is "=" for mandatory attributes and "*" for optional attributes. This format allows the full set of features available for TACACS+ authorization to be used also for RADIUS.

The table below summarizes the VSAs that are now supported with Per VRF AAA.

Table 1: VSAs Supported with Per VRF AAA

VSA Name	Value Type	Description
Note Each VSA must have the prefix "template:" before the VSA name, unless a different prefix is explicitly stated.		
account-delay	string	This VSA must be "on." The functionality of this VSA is equal to the **aaa accounting delay-start**command for the customer template.
account-send-stop	string	This VSA must be "on." The functionality of this VSA is equal to the **aaa accounting send stop-record authentication**command with the **failure** keyword.
account-send-success-remote	string	This VSA must be "on." The functionality of this VSA is equal to the **aaa accounting send stop-record authentication**command with the **success** keyword.
attr-44	string	This VSA must be "access-req." The functionality of this VSA is equal to the **radius-server attribute 44 include-in-access-req** command.
ip-addr	string	This VSA specifies the IP address, followed by the mask that the router uses to indicate its own IP address and mask in negotiation with the client; for example, ip-addr=192.168.202.169 255.255.255.255
ip-unnumbered	string	This VSA specifies the name of an interface on the router. The functionality of this VSA is equal to the **ip unnumbered** command, which specifies an interface name such as "Loopback 0."
ip-vrf	string	This VSA specifies which VRF will be used for the packets of the end user. This VRF name should match the name that is used on the router via the **ip vrf forwarding** command.

VSA Name	Value Type	Description
peer-ip-pool	string	This VSA specifies the name of an IP address pool from which an address will be allocated for the peer. This pool should be configured using the **ip local pool**command or should be automatically downloadable via RADIUS.
ppp-acct-list	string	This VSA defines the accounting method list that is to be used for PPP sessions. The VSA syntax is as follows: "ppp-acct-list=[start-stop | stop-only | none] group X [group Y] [broadcast]." It is equal to the **aaa accounting network mylist** command functionality. The user must specify at least one of the following options: start-stop, stop-only, or none. If either start-stop or stop-only is specified, the user must specify at least one, but not more than four, group arguments. Each group name must consist of integers. The servers in the group should have already been identified in the access-accept via the VSA "rad-serv." After each group has been specified, the user can specify the broadcast option
ppp-authen-list	string	This VSA defines which authentication method list is to be used for PPP sessions and, if more than one method is specified, in what order the methods should be used. The VSA syntax is as follows: "ppp-authen-list=[groupX | local | local-case | none | if-needed]," which is equal to the **aaa authentication ppp mylist** command functionality. The user must specify at least one, but no more than four, authentication methods. If a server group is specified, the group name must be an integer. The servers in the group should have already been identified in the access-accept via the VSA "rad-serv."
ppp-authen-type	string	This VSA allows the end user to specify at least one of the following authentication types: pap, chap, eap, ms-chap, ms-chap-v2, any, or a combination of the available types that is separated by spaces. The end user will be permitted to log in using only the methods that are specified in this VSA. PPP will attempt these authentication methods in the order presented in the attribute.

VSA Name	Value Type	Description
ppp-author-list	string	This VSA defines the authorization method list that is to be used for PPP sessions. It indicates which methods will be used and in what order. The VSA syntax is as follows: "ppp-author-list=[groupX] [local] [if-authenticated] [none]," which is equal to the **aaa authorization network mylist**command functionality. The user must specify at least one, but no more than four, authorization methods. If a server group is specified, the group name must be an integer. The servers in the group should have already been identified in the access-accept via the VSA "rad-serv."
Note The RADIUS VSAs--rad-serv, rad-serv-filter, rad-serv-source-if, and rad-serv-vrf--must have the prefix "aaa:" before the VSA name.		
rad-serv	string	This VSA indicates the IP address, key, timeout, and retransmit number of a server, as well as the group of the server. The VSA syntax is as follows: "rad-serv=a.b.c.d [key SomeKey] [auth-port X] [acct-port Y] [retransmit V] [timeout W]." Other than the IP address, all parameters are optional and can be issued in any order. If the optional parameters are not specified, their default values will be used. The key cannot contain any spaces; for "retransmit V," "V" can range from 1-100; for "timeout W," the "W" can range from 1-1000.
rad-serv-filter	string	The VSA syntax is as follows: "rad-serv-filter=authorization | accounting-request | reply-accept | reject-filtername." The filtername must be defined via the **radius-server attribute list filtername** command. **Note** This VSA is supported in Cisco IOS XE Release 2.3 and later releases.
rad-serv-source-if	string	This VSA specifies the name of the interface that is used for transmitting RADIUS packets. The specified interface must match the interface configured on the router.
rad-serv-vrf	string	This VSA specifies the name of the VRF that is used for transmitting RADIUS packets. The VRF name should match the name that was specified via the **ip vrf forwarding** command.

VRF Aware Framed-Routes

In Cisco IOS XE Release 2.3 and later, the Cisco ASR 1000 Series Aggregation Services Routers support VRF aware framed-routes. No configuration is required to enable support for this feature. Framed-routes are automatically detected and if the framed-route is part of a VRF associated with an interface, the rout is applied accordingly.

How to Configure Per VRF AAA

Configuring Per VRF AAA

Configuring AAA

To enable AAA you need to complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA globally.

Configuring Server Groups

To configure server groups you need to complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius** *groupname*
5. **server-private** *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
6. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA globally.
Step 4	**aaa group server radius** *groupname* **Example:** `Router(config)# aaa group server radius v2.44.com`	Groups different RADIUS server hosts into distinct lists and distinct methods. Enters server-group configuration mode.
Step 5	**server-private** *ip-address* [**auth-port** *port-number*	**acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] **Example:** `Router(config-sg-radius)# server-private 10.10.130.2 auth-port 1600 key ww`	Configures the IP address of the private RADIUS server for the group server. **Note** If private server parameters are not specified, global configurations will be used. If global configurations are not specified, default values will be used.
Step 6	**exit** **Example:** `Router(config-sg-radius)# exit`	Exits from server-group configuration mode; returns to global configuration mode.

Configuring Authentication Authorization and Accounting for Per VRF AAA

To configure authentication, authorization, and accounting for Per VRF AAA, you need to complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
5. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} *method1* [*method2...*]
6. **aaa accounting system default** [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname*
7. **aaa accounting delay-start** [**vrf** *vrf-name*]
8. **aaa accounting send stop-record authentication** {**failure** | **success remote-server**} [**vrf** *vrf-name*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA globally.
Step 4	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication ppp method_list_v2.44.com group v2.44.com`	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.
Step 5	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} *method1* [*method2...*]	Sets parameters that restrict user access to a network.

	Command or Action	Purpose
	Example: `Router(config)# aaa authorization network method_list_v2.44.com group v2.44.com`	
Step 6	**aaa accounting system default** [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname* **Example:** `Router(config)# aaa accounting system default vrf v2.44.com start-stop group v2.44.com`	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS.
Step 7	**aaa accounting delay-start** [**vrf** *vrf-name*] **Example:** `Router(config)# aaa acounting delay-start vrf v2.44.com`	Displays generation of the start accounting records until the user IP address is established.
Step 8	**aaa accounting send stop-record authentication** {**failure** | **success remote-server**} [**vrf** *vrf-name*] **Example:** `Router(config)# aaa accounting send stop-record authentication failure vrf v2.44.com`	Generates accounting stop records. When using the **failure** keyword a "stop" record will be sent for calls that are rejected during authentication. When using the **success** keyword a "stop" record will be sent for calls that meet one of the following criteria: • Calls that are authenticated by a remote AAA server when the call is terminated. • Calls that are not authenticated by a remote AAA server and the start record has been sent. • Calls that are successfully established and then terminated with the "stop-only" **aaa accounting** configuration. **Note** The **success** and **remote-server** keywords are available in Cisco IOS XE Release 2.4 and later releases.

Configuring RADIUS-Specific Commands for Per VRF AAA

To configure RADIUS-specific commands for Per VRF AAA you need to complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip radius source-interface** *subinterface-name* [**vrf** *vrf-name*]
4. **radius-server attribute 44 include-in-access-req** [**vrf** *vrf-name*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip radius source-interface** *subinterface-name* [**vrf** *vrf-name*] **Example:** `Router(config)# ip radius source-interface loopback55`	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.
Step 4	**radius-server attribute 44 include-in-access-req** [**vrf** *vrf-name*] **Example:** `Router(config)# radius-server attribute 44 include-in-access-req vrf v2.44.com`	Sends RADIUS attribute 44 in access request packets before user authentication and enables the specification on a per-VRF basis.

Configuring Interface-Specific Commands for Per VRF AAA

To configure interface-specific commands for Per VRF AAA, you need to complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip vrf forwarding** *vrf-name*
5. **ppp authentication** {*protocol1* [*protocol2...*]} *listname*
6. **ppp authorization** *list-name*
7. **ppp accounting default**
8. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [*name-tag*] **Example:** `Router(config)# interface loopback11`	Configures an interface type and enters interface configuration mode.
Step 4	**ip vrf forwarding** *vrf-name* **Example:** `Router(config-if)# ip vrf forwarding v2.44.com`	Associates a VRF with an interface.
Step 5	**ppp authentication** {*protocol1* [*protocol2*...]} *listname* **Example:** `Router(config-if)# ppp authentication chap callin V2_44_com`	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.
Step 6	**ppp authorization** *list-name* **Example:** `Router(config-if)# ppp authorization V2_44_com`	Enables AAA authorization on the selected interface.
Step 7	**ppp accounting default** **Example:** `Router(config-if)# ppp accounting default`	Enables AAA accounting services on the selected interface.
Step 8	**exit** **Example:** `Router(config)# exit`	Exits interface configuration mode.

Configuring Per VRF AAA Using Local Customer Templates

Configuring AAA

Perform the tasks as outlined in the Configuring Per VRF AAA.

Configuring Server Groups

Perform the tasks as outlined in the Configuring Server Groups.

Configuring Authentication Authorization and Accounting for Per VRF AAA

Perform the tasks as outlined in the Configuring Authentication Authorization and Accounting for Per VRF AAA.

Configuring Authorization for Per VRF AAA with Local Customer Templates

To configure authorization for Per VRF AAA with local templates, you need to complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization template**
4. **aaa authorization network default local**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa authorization template** **Example:** `Router(config)# aaa authorization template`	Enables the use of local or remote templates.
Step 4	**aaa authorization network default local** **Example:**	Specifies local as the default method for authorization.

	Command or Action	Purpose
	`Router(config)# aaa authorization network default local`	

Configuring Local Customer Templates

To configure local customer templates, you need to complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn search-order domain**
4. **template** *name* [**default** | **exit** | **multilink** | **no** | **peer** | **ppp**]
5. **peer default ip address pool** *pool-name*
6. **ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**]
7. **ppp authorization** [**default** | *list-name*]
8. **aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname*
9. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn search-order domain** **Example:** `Router (config)# vpdn search-order domain`	Looks up the profiles based on domain.
Step 4	**template** *name* [**default**	**exit**	**multilink**	**no**	**peer**	**ppp**] **Example:** `Router (config)# template v2.44.com`	Creates a customer profile template and assigns a unique name that relates to the customer that will be receiving it. Enters template configuration mode. **Note**

	Command or Action	Purpose
		Steps 5, 6, and 7 are optional. Enter **multilink**, **peer**, and **ppp** keywords appropriate to customer application requirements.
Step 5	**peer default ip address pool** *pool-name* **Example:** `Router(config-template)# peer default ip address pool v2_44_com_pool`	(Optional) Specifies that the customer profile to which this template is attached will use a local IP address pool with the specified name.
Step 6	**ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] **Example:** `Router(config-template)# ppp authentication chap`	(Optional) Sets the PPP link authentication method.
Step 7	**ppp authorization** [**default** | *list-name*] **Example:** `Router(config-template)# ppp authorization v2_44_com`	(Optional) Sets the PPP link authorization method.
Step 8	**aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname* **Example:** `Router(config-template)# aaa accounting v2_44_com`	(Optional) Enables AAA operational parameters for the specified customer profile.
Step 9	**exit** **Example:** `Router(config-template)# exit`	Exits from template configuration mode; returns to global configuration mode.

Configuring Per VRF AAA Using Remote Customer Templates

Configuring AAA

Perform the tasks as outlined in the Configuring Per VRF AAA.

Configuring Server Groups

Perform the tasks as outlined in the Configuring Server Groups.

Configuring Authentication for Per VRF AAA with Remote Customer Profiles

To configure authentication for Per VRF AAA with remote customer profiles, you need to perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
4. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# ppp authentication ppp default group radius`	Specifies one or more authentication, authorization, and accounting (AAA) authentication methods for use on serial interfaces that are running PPP.
Step 4	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*] **Example:** `Router(config)# aaa authorization network default group sp`	Sets parameters that restrict user access to a network.

Configuring Authorization for Per VRF AAA with Remote Customer Profiles

To configuring authorization for Per VRF AAA with remote customer profiles, you need to perform the following step.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization template**
4. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa authorization template** **Example:** `Router(config)# aaa authorization template`	Enables use of local or remote templates.
Step 4	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*] **Example:** `Router(config)# aaa authorization network default sp`	Specifies the server group that is named as the default method for authorization.

Configuring the RADIUS Profile on the SP RADIUS Server

Configure the RADIUS profile on the Service Provider (SP) RADIUS server. See the Per VRF AAA Using a Remote RADIUS Customer Template Example for an example of how to update the RADIUS profile.

Verifying VRF Routing Configurations

To verify VRF routing configurations, you need to complete the following steps:

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. show ip route vrf *vrf-name*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	show ip route vrf *vrf-name* **Example:** `Router(config)# show ip route vrf northvrf`	Displays the IP routing table associated with a VRF.

Troubleshooting Per VRF AAA Configurations

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

Command	Purpose
`Router# debug aaa accounting`	Displays information on accountable events as they occur.
`Router# debug aaa authentication`	Displays information on AAA authentication.
`Router# 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 Layer 2 Transport Protocol (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 for Per VRF AAA

Per VRF Configuration Examples

Per VRF AAA Example

The following example shows how to configure the Per VRF AAA feature using a AAA server group with associated private servers:

```
aaa new-model
aaa authentication ppp method_list_v1.55.com group v1.55.com
aaa authorization network method_list_v1.55.com group v1.55.com
aaa accounting network method_list_v1.55.com start-stop group v1.55.com
aaa accounting system default vrf v1.55.com start-stop group v1.55.com
aaa accounting delay-start vrf v1.55.com
aaa accounting send stop-record authentication failure vrf v1.55.com
aaa group server radius v1.55.com
    server-private 10.10.132.4 auth-port 1645 acct-port 1646 key ww
    ip vrf forwarding v1.55.com
ip radius source-interface loopback55
radius-server attribute 44 include-in-access-req vrf v1.55.com
```

Per VRF AAA Using a Locally Defined Customer Template Example

The following example shows how to configure the Per VRF AAA feature using a locally defined customer template with a AAA server group that has associated private servers:

```
aaa new-model
aaa authentication ppp method_list_v1.55.com group v1.55.com
aaa authorization network method_list_v1.55.com group v1.55.com
aaa authorization network default local
aaa authorization template
aaa accounting network method_list_v1.55.com start-stop group v1.55.com
aaa accounting system default vrf v1.55.com start-stop group v1.55.com
aaa group server radius V1_55_com
  server-private 10.10.132.4 auth-port 1645 acct-port 1646 key ww
  ip vrf forwarding V1.55.com
template V1.55.com
  peer default ip address pool V1_55_com_pool
  ppp authentication chap callin V1_55_com
  ppp authorization V1_55_com
  ppp accounting V1_55_com
  aaa accounting delay-start
  aaa accounting send stop-record authentication failure
  radius-server attribute 44 include-in-access-req
  ip vrf forwarding v1.55.com
  ip radius source-interface Loopback55
```

Per VRF AAA Using a Remote RADIUS Customer Template Example

The following examples shows how to configure the Per VRF AAA feature using a remotely defined customer template on the SP RADIUS server with a AAA server group that has associated private servers:

```
aaa new-model
```

```
aaa authentication ppp default group radius
aaa authorization template
aaa authorization network default group sp
aaa group server radius sp
   server 10.3.3.3
radius-server host 10.3.3.3 auth-port 1645 acct-port 1646 key sp_key
```

The following RADIUS server profile is configured on the SP RADIUS server:

```
cisco-avpair = "aaa:rad-serv#1=10.10.132.4 key ww"
cisco-avpair = "aaa:rad-serv-vrf#1=V1.55.com"
cisco-avpair = "aaa:rad-serv-source-if#1=Loopback 55"
cisco-avpair = "template:ppp-authen-list=group 1"
cisco-avpair = "template:ppp-author-list=group 1"
cisco-avpair = "template:ppp-acct-list= start-stop group 1"
cisco-avpair = "template:account-delay=on"
cisco-avpair = "template:account-send-stop=on"
cisco-avpair = "template:rad-attr44=access-req"
cisco-avpair = "template:peer-ip-pool=V1.55-pool"
cisco-avpair = "template:ip-vrf=V1.55.com"
cisco-avpair = "template:ip-unnumbered=Loopback 55"
framed-protocol = ppp
service-type = framed
```

Customer Template Examples

Locally Configured Customer Template with RADIUS Attribute Screening and Broadcast Accounting Example

The following example shows how to create a locally configured template for a single customer, configuring additional features including RADIUS attribute screening and broadcast accounting:

```
aaa authentication ppp default local group radius
aaa authentication ppp V1_55_com group V1_55_com
aaa authorization template
aaa authorization network default local group radius
aaa authorization network V1_55_com group V1_55_com
aaa accounting network V1_55_com start-stop broadcast group V1_55_com group SP_AAA_server
aaa group server radius SP_AAA_server
 server 10.10.100.7 auth-port 1645 acct-port 1646
aaa group server radius V1_55_com
 server-private 10.10.132.4 auth-port 1645 acct-port 1646
 authorization accept min-author
 accounting accept usage-only
 ip vrf forwarding V1.55.com
ip vrf V1.55.com
 rd 1:55
 route-target export 1:55
 route-target import 1:55
template V1.55.com
 peer default ip address pool V1.55-pool
 ppp authentication chap callin V1_55_com
 ppp authorization V1_55_com
 ppp accounting V1_55_com
 aaa accounting delay-start
 aaa accounting send stop-record authentication failure
 radius-server attribute 44 include-in-access-req
vpdn-group V1.55
 accept-dialin
  protocol l2tp
```

```
  virtual-template 13
 terminate-from hostname lac-lb-V1.55
 source-ip 10.10.104.12
 lcp renegotiation always
 l2tp tunnel password 7 060506324F41
interface Virtual-Template13
 ip vrf forwarding V1.55.com
 ip unnumbered Loopback55
 ppp authentication chap callin
 ppp multilink
ip local pool V1.55-pool 10.1.55.10 10.1.55.19 group V1.55-group
ip radius source-interface Loopback0
ip radius source-interface Loopback55 vrf V1.55.com
radius-server attribute list min-author
 attribute 6-7,22,27-28,242
radius-server attribute list usage-only
 attribute 1,40,42-43,46
radius-server host 10.10.100.7 auth-port 1645 acct-port 1646 key ww
radius-server host 10.10.132.4 auth-port 1645 acct-port 1646 key ww
```

Remotely Configured Customer Template with RADIUS Attribute Screening and Broadcast Accounting Example

The following example shows how to create a remotely configured template for a single customer, configuring additional features including RADIUS attribute screening and broadcast accounting:

```
aaa authentication ppp default local group radius
aaa authorization template
aaa authorization network default local group radius
ip vrf V1.55.com
 rd 1:55
 route-target export 1:55
 route-target import 1:55
vpdn-group V1.55
 accept-dialin
  protocol l2tp
  virtual-template 13
 terminate-from hostname lac-lb-V1.55
 source-ip 10.10.104.12
 lcp renegotiation always
 l2tp tunnel password 7 060506324F41
interface Virtual-Template13
 no ip address
 ppp authentication chap callin
 ppp multilink
ip local pool V1.55-pool 10.1.55.10 10.1.55.19 group V1.55-group
radius-server attribute list min-author
 attribute 6-7,22,27-28,242
radius-server attribute list usage-only
 attribute 1,40,42-43,46
```

The customer template is stored as a RADIUS server profile for v1.55.com.

```
cisco-avpair = "aaa:rad-serv#1=10.10.132.4 key ww"
cisco-avpair = "aaa:rad-serv-vrf#1=V1.55.com"
cisco-avpair = "aaa:rad-serv-source-if#1=Loopback 55"
cisco-avpair = "aaa:rad-serv#2=10.10.100.7 key ww"
cisco-avpair = "aaa:rad-serv-source-if#2=Loopback 0"
cisco-avpair = "template:ppp-authen-list=group 1"
cisco-avpair = "template:ppp-author-list=group 1"
cisco-avpair = "template:ppp-acct-list= start-stop group 1 group 2 broadcast"
```

```
cisco-avpair = "template:account-delay=on"
cisco-avpair = "template:account-send-stop=on"
cisco-avpair = "template:rad-attr44=access-req"
cisco-avpair = "aaa:rad-serv-filter#1=authorization accept min-author"
cisco-avpair = "aaa:rad-serv-filter#1=accounting accept usage-only"
cisco-avpair = "template:peer-ip-pool=V1.55-pool"
cisco-avpair = "template:ip-vrf=V1.55.com"
cisco-avpair = "template:ip-unnumbered=Loopback 55"
framed-protocol = ppp
service-type = framed
```

AAA Accounting Stop Record Examples

The following AAA accounting stop record examples show how to configure the **aaa accounting send stop-record authentication** command to control the generation of "stop" records when the **aaa accounting** command is issued with the **start-stop** or **stop-only** keyword.



Note The **success** and **remote-server** keywords are available in Cisco IOS XE Release 2.4 and later releases.

AAA Accounting Stop Record and Rejected Call Example

The following example shows the "stop" record being sent for a rejected call during authentication when the **aaa accounting send stop-record authentication**command is issued with the **success** keyword.

```
Router# show running-config | include aaa
.
.
.
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication success remote-server
aaa accounting network default start-stop group radius
Router#
*Jul  7 03:39:40.199: AAA/BIND(00000026): Bind i/f Virtual-Template2
*Jul  7 03:39:40.199: ppp21 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul  7 03:39:42.199: RADIUS:  AAA Unsupported     [156] 7
*Jul  7 03:39:42.199: RADIUS:   30 2F 30 2F
30                                  [0/0/0]
*Jul  7 03:39:42.199: RADIUS(00000026): Config NAS IP: 10.0.0.0
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026): acct_session_id: 55
*Jul  7 03:39:42.199: RADIUS(00000026): sending
*Jul  7 03:39:42.199: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul  7 03:39:42.199: RADIUS(00000026): Send Access-Request to
172.19.192.238:2195 id 1645/14, len 94
*Jul  7 03:39:42.199: RADIUS:  authenticator A6 D1 6B A4 76 9D 52 CF - 33 5D
16 BE AC 7E 5F A6
*Jul  7 03:39:42.199: RADIUS:  Framed-Protocol     [7]   6
PPP                         [1]
*Jul  7 03:39:42.199: RADIUS:  User-Name           [1]   16  "user@example.com"
*Jul  7 03:39:42.199: RADIUS:  CHAP-Password       [3]   19  *
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Type       [61]  6
Virtual                     [5]
*Jul  7 03:39:42.199: RADIUS:  NAS-Port            [5]   6
```

```
0
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:39:42.199: RADIUS:  Service-Type        [6]   6
Framed                     [2]
*Jul  7 03:39:42.199: RADIUS:  NAS-IP-Address      [4]   6
10.0.1.123
*Jul  7 03:39:42.271: RADIUS: Received from id 1645/14 172.19.192.238:2195,
Access-Accept, len 194
*Jul  7 03:39:42.271: RADIUS:  authenticator 30 AD FF 8E 59 0C E4 6C - BA 11
23 63 81 DE 6F D7
*Jul  7 03:39:42.271: RADIUS:  Framed-Protocol     [7]   6
PPP                        [1]
*Jul  7 03:39:42.275: RADIUS:  Service-Type        [6]   6
Framed                     [2]
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  26
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   20  "vpdn:tunnel-
id=lac"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  29
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   23  "vpdn:tunnel-
type=l2tp"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  30
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   24  "vpdn:gw-
password=cisco"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  31
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   25  "vpdn:nas-
password=cisco"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  34
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   28  "vpdn:ip-
addresses=10.0.0.2"
*Jul  7 03:39:42.275: RADIUS:  Service-Type        [6]   6
Framed                     [2]
*Jul  7 03:39:42.275: RADIUS:  Framed-Protocol     [7]   6
PPP                        [1]
*Jul  7 03:39:42.275: RADIUS(00000026): Received from id 1645/14
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-id
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: gw-password
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: nas-password
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: ip-addresses
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul  7 03:39:42.279: AAA/BIND(00000027): Bind i/f
*Jul  7 03:39:42.279:  Tnl 21407 L2TP: O SCCRQ
*Jul  7 03:39:42.279:  Tnl 21407 L2TP: O SCCRQ, flg TLS, ver 2, len 134, tnl
0, ns 0, nr 0
         C8 02 00 86 00 00 00 00 00 00 00 80 08 00 00
         00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 30 80 09 00 00 00 07 6C 61 63 00 19 00
         00 00 08 43 69 73 63 6F 20 53 79 73 74 65 6D 73
         2C 20 49 6E 63 2E 80 ...
*Jul  7 03:39:49.279:  Tnl 21407 L2TP: O StopCCN
*Jul  7 03:39:49.279:  Tnl 21407 L2TP: O StopCCN, flg TLS, ver 2, len 66, tnl
0, ns 1, nr 0
         C8 02 00 42 00 00 00 00 00 01 00 00 80 08 00 00
         00 00 00 04 80 1E 00 00 00 01 00 02 00 06 54 6F
         6F 20 6D 61 6E 79 20 72 65 74 72 61 6E 73 6D 69
         74 73 00 08 00 09 00 69 00 01 80 08 00 00 00 09
         53 9F
*Jul  7 03:39:49.279: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul  7 03:39:49.279: RADIUS(00000026): Config NAS IP: 10.0.0.0
*Jul  7 03:39:49.279: RADIUS(00000026): sending
*Jul  7 03:39:49.279: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
```

```
Radius-Server 172.19.192.238
*Jul  7 03:39:49.279: RADIUS(00000026): Send Accounting-Request to
172.19.192.238:2196 id 1646/32, len 179
*Jul  7 03:39:49.279: RADIUS:  authenticator 0A 85 2F F0 65 6F 25 E1 - 97 54
CC BF EA F7 62 89
*Jul  7 03:39:49.279: RADIUS:  Acct-Session-Id     [44]  10  "00000037"
*Jul  7 03:39:49.279: RADIUS:  Framed-Protocol     [7]   6
PPP                        [1]
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Medium-Type  [65]  6
00:IPv4                    [1]
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Client-Endpoi[66]  10  "10.0.0.1"
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Server-Endpoi[67]  10  "10.0.0.2"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Type         [64]  6
00:L2TP                    [3]
*Jul  7 03:39:49.283: RADIUS:  Acct-Tunnel-Connecti[68]  3   "0"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Client-Auth-I[90]  5   "lac"
*Jul  7 03:39:49.283: RADIUS:  User-Name           [1]   16  "user@example.com"
*Jul  7 03:39:49.283: RADIUS:  Acct-Authentic      [45]  6
RADIUS                     [1]
*Jul  7 03:39:49.283: RADIUS:  Acct-Session-Time   [46]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Octets   [42]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Octets  [43]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Packets  [47]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Packets [48]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Terminate-Cause[49]  6   nas-
error                  [9]
*Jul  7 03:39:49.283: RADIUS:  Acct-Status-Type    [40]  6
Stop                       [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Type       [61]  6
Virtual                    [5]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:39:49.283: RADIUS:  Service-Type        [6]   6
Framed                     [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-IP-Address      [4]   6
10.0.1.123
*Jul  7 03:39:49.283: RADIUS:  Acct-Delay-Time     [41]  6
0
*Jul  7 03:39:49.335: RADIUS: Received from id 1646/32 172.19.192.238:2196,
Accounting-response, len 20
*Jul  7 03:39:49.335: RADIUS:  authenticator C8 C4 61 AF 4D 9F 78 07 - 94 2B
44 44 17 56 EC 03
```

AAA Accounting Stop Record and Successful Call Example

The following example shows “start” and “stop” records being sent for a successful call when the **aaa accounting send stop-record authentication** command is issued with the **failure** keyword.

```
Router# show running-config | include aaa

.
.
.
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication failure
```

```
aaa accounting network default start-stop group radius
.
.
.
*Jul  7 03:28:31.543: AAA/BIND(00000018): Bind i/f Virtual-Template2
*Jul  7 03:28:31.547: ppp14 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:28:33.555: AAA/AUTHOR (0x18): Pick method list 'default'
*Jul  7 03:28:33.555: AAA/BIND(00000019): Bind i/f
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ, flg TLS, ver 2, len 141, tnl 0,
ns 0, nr 0
         C8 02 00 8D 00 00 00 00 00 00 00 80 08 00 00
         00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 30 80 10 00 00 00 07 4C 41 43 2D 74 75
         6E 6E 65 6C 00 19 00 00 00 08 43 69 73 63 6F 20
         53 79 73 74 65 6D 73 ...
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 0, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse SCCRP
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 2, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Protocol Ver 256
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 3, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Framing Cap 0x0
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 4, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Bearer Cap 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 6, len 8, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Firmware Ver 0x1120
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 7, len 16, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Hostname LNS-tunnel
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 8, len 25, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Vendor Name Cisco Systems, Inc.
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 9, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Assigned Tunnel ID 6897
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 10, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Rx Window Size 20050
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 11, len 22, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng
         81 13 03 F6 A8 E4 1D DD 25 18 25 6E 67 8C 7C 39
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 13, len 22, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng Resp
         4D 52 91 DC 1A 43 B3 31 B4 F5 B8 E1 88 22 4F 41
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: No missing AVPs in SCCRP
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: I SCCRP, flg TLS, ver 2, len 157, tnl
5192, ns 0, nr 1
contiguous pak, size 157
         C8 02 00 9D 14 48 00 00 00 00 00 01 80 08 00 00
         00 00 00 02 80 08 00 00 00 02 01 00 80 0A 00 00
         00 03 00 00 00 00 80 0A 00 00 00 04 00 00 00 00
         00 08 00 00 00 06 11 20 80 10 00 00 00 07 4C 4E
         53 2D 74 75 6E 6E 65 6C ...
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: I SCCRP from LNS-tunnel
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: O SCCCN  to LNS-tunnel tnlid 6897
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: O SCCCN, flg TLS, ver 2, len 42, tnl
6897, ns 1, nr 1
         C8 02 00 2A 1A F1 00 00 00 01 00 01 80 08 00 00
         00 00 00 03 80 16 00 00 00 0D 32 24 17 BC 6A 19
         B1 79 F3 F9 A9 D4 67 7D 9A DB
*Jul  7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ to LNS-tunnel 6897/0
*Jul  7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ, flg TLS, ver 2, len
63, tnl 6897, lsid 11, rsid 0, ns 2, nr 1
         C8 02 00 3F 1A F1 00 00 00 02 00 01 80 08 00 00
         00 00 00 0A 80 0A 00 00 00 0F C8 14 B4 03 80 08
         00 00 00 0E 00 0B 80 0A 00 00 00 12 00 00 00 00
         00 0F 00 09 00 64 0F 10 09 02 02 00 1B 00 00
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse  AVP 0, len 8, flag
```

```
0x8000 (M)
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse ICRP
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse  AVP 14, len 8, flag
0x8000 (M)
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Assigned Call ID 5
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: No missing AVPs in ICRP
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: I ICRP, flg TLS, ver 2, len
28, tnl 5192, lsid 11, rsid 0, ns 1, nr 3
contiguous pak, size 28
         C8 02 00 1C 14 48 00 0B 00 01 00 03 80 08 00 00
         00 00 00 0B 80 08 00 00 00 0E 00 05
*Jul  7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN to LNS-tunnel 6897/5
*Jul  7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN, flg TLS, ver 2, len
167, tnl 6897, lsid 11, rsid 5, ns 3, nr 2
         C8 02 00 A7 1A F1 00 05 00 03 00 02 80 08 00 00
         00 00 00 0C 80 0A 00 00 00 18 06 1A 80 00 00 0A
         00 00 00 26 06 1A 80 00 80 0A 00 00 00 13 00 00
         00 01 00 15 00 00 00 1B 01 04 05 D4 03 05 C2 23
         05 05 06 0A 0B E2 7A ...
*Jul  7 03:28:33.579: RADIUS/ENCODE(00000018):Orig. component type = PPoE
*Jul  7 03:28:33.579: RADIUS(00000018): Config NAS IP: 10.0.0.0
*Jul  7 03:28:33.579: RADIUS(00000018): sending
*Jul  7 03:28:33.579: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul  7 03:28:33.579: RADIUS(00000018): Send Accounting-Request to
172.19.192.238:2196 id 1646/23, len 176
*Jul  7 03:28:33.579: RADIUS:  authenticator 3C 81 D6 C5 2B 6D 21 8E - 19 FF
43 B5 41 86 A8 A5
*Jul  7 03:28:33.579: RADIUS:  Acct-Session-Id     [44]  10  "00000023"
*Jul  7 03:28:33.579: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:28:33.579: RADIUS:  Tunnel-Medium-Type  [65]  6
00:IPv4                   [1]
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Client-Endpoi[66]  10  "10.0.0.1"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Server-Endpoi[67]  10  "10.0.0.2"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Assignment-Id[82]  5   "lac"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Type         [64]  6
00:L2TP                   [3]
*Jul  7 03:28:33.583: RADIUS:  Acct-Tunnel-Connecti[68]  12  "3356800003"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Client-Auth-I[90]  12  "LAC-tunnel"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Server-Auth-I[91]  12  "LNS-tunnel"
*Jul  7 03:28:33.583: RADIUS:  User-Name           [1]   16  "user@example.com"
*Jul  7 03:28:33.583: RADIUS:  Acct-Authentic      [45]  6
Local                     [2]
*Jul  7 03:28:33.583: RADIUS:  Acct-Status-Type    [40]  6
Start                     [1]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Type       [61]  6
Virtual                   [5]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:28:33.583: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:28:33.583: RADIUS:  NAS-IP-Address      [4]   6
10.0.1.123
*Jul  7 03:28:33.583: RADIUS:  Acct-Delay-Time     [41]  6
0
*Jul  7 03:28:33.683: RADIUS: Received from id 1646/23 172.19.192.238:2196,
Accounting-response, len 20
*Jul  7 03:28:33.683: RADIUS:  authenticator 1C E9 53 42 A2 8A 58 9A - C3 CC
1D 79 9F A4 6F 3A
```

Additional References

The following sections provide references related to Per VRF AAA.

Related Documents

Related Topic	Document Title
Configuring server groups	Configuring RADIUS chapter in the *Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2.
RADIUS attribute screening	RADIUS Attribute Value Screening chapter in the *Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2.
Configuring broadcast accounting	Configuring Accounting chapter in the *Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2.
Cisco IOS Security Commands	*Cisco IOS Security Command Reference*
Cisco IOS Switching Services Commands	*Cisco IOS IP Switching Command Reference*
Configuring Multiprotocol Label Switching	*Cisco IOS XE Multiprotocol Label Switching Configuration Guide*, Release 2
Configuring virtual templates	Virtual Templates and Profiles section of the *Cisco IOS XE Dial Technologies Configuration Guide*, Release 2

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 MIBs 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
No new or modified RFCs are supported by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Per VRF AAA

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 Per VRF AAA

Feature Name	Releases	Feature Information
Per VRF AAA	Cisco IOS XE Release 2.1	The Per VRF AAA feature allows authentication, authorization, and accounting (AAA) on the basis of Virtual Private Network (VPN) routing and forwarding (VRF) instances. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: **aaa accounting, aaa accounting delay-start, ip radius source-interface, server-private (RADIUS)**, **ip vrf forwarding (server-group)**, **radius-server domain-stripping**, **aaa authorization template**.
RADIUS Per-VRF Server Group	Cisco IOS XE Release 2.1	Using the Radius Per-VRF Server Group feature, Internet Service Providers (ISPs) can partition RADIUS server groups based on Virtual Route Forwarding (VRF). This means that you can define RADIUS server groups that belong to a VRF. This feature is supported by “aaa: rad-serv-vrf” VSA. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: **ip vrf forwarding**.

Feature Name	Releases	Feature Information
Attribute Filtering Per-Domain and VRF Aware Framed-Routes	Cisco IOS XE Release 2.3	The Attribute Filtering Per-Domain and VRF Aware Framed-Routes feature allows for attribute filtering per-domain and VRF aware Framed-Routes. It introduces support for the “aaa:rad-serv-filter” VSA. In Cisco IOS XE Release 2.3, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
AAA CLI Stop Record Enhancement	Cisco IOS XE Release 2.4	The AAA CLI Stop Record Enhancement feature enables sending an accounting stop record only when an access accept is received from the AAA server. In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: **aaa accounting send stop-record authentication**.
Dynamic Per VRF AAA	Cisco IOS XE Release 2.4	The Dynamic Per VRF AAA feature allows you to use a customer template, which may be stored either locally or remotely, and AAA services can be performed on the information that is stored in the customer template. In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Glossary

AAA--authentication, authorization, and accounting. A framework of security services that provide the method for identifying users (authentication), for remote access control (authorization), and for collecting and sending security server information used for billing, auditing, and reporting (accounting).

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.

PE--Provider Edge. Networking devices that are located on the edge of a service provider network.

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.

VPN --Virtual Private Network. 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.