CHAPTER 11

Configuring Local AAA Server, User Database—Domain to VRF

The Local AAA Server, User Database—Domain to VRF feature extends the Cisco IOS AAA Authorization to local AAA profiles on the router without using an AAA Server. The local user database acts as a local AAA server, and is fully compatible with any external AAA Server. If you want to maintain your user database locally or provide a failover local mechanism, you no longer have to sacrifice policy options when defining local users.

This flexibility allows you to provide complete user authentication and authorization locally within Cisco IOS without using an AAA Server, provided the local username list is relatively small. While authentication can be done on the router for a limited number of user names, it might make more sense and be much more scalable to use an AAA Server. Note that accounting is still be done on an AAA server and is not be supported on the router.

The key function that this feature provides is a mapping of user domain names to local AAA profiles. This allows AAA attributes to be applied to the PPP session as part of the PPP session establishment. These local AAA attributes are RADIUS attributes that would normally be defined on a Radius Server but now are defined locally on the router.

Subscriber profiles are used to match user domain names, and on a match to use a defined AAA attribute list. The AAA attribute list contains a list of valid Cisco IOS format AAA attributes.

Note Domain to subscriber profile matching is a global match. Limiting which domains are permitted or denied per PPPoE bba-group or PVC is not supported.

This chapter describes the Local AAA Server, User Database—Domain to VRF feature in the following topics:

- Feature History for Local AAA Server, User Database—Domain to VRF, page 11-2
- Prerequisites for Local AAA Server, User Database—Domain to VRF, page 11-2
- Establishing a PPP Connection, page 11-2
- AAA Attribute Lists, page 11-4
- Subscriber Profiles, page 11-5
- AAA Method Lists, page 11-6
- Configuration Tasks for Local AAA Server, User Database—Domain to VRF Using Local Attributes, page 11-6
- Verifying Local AAA Server, User Database—Domain to VRF Using Local Attributes, page 11-9

- Configuration Example for Local AAA Server, User Database—Domain to VRF, page 11-9
- Monitoring and Maintaining Local AAA Server, User Database—Domain to VRF, page 11-12

Feature History for Local AAA Server, User Database—Domain to VRF

Cisco IOS Release	Description	Required PRE
12.3(7)XI1	This feature was introduced on the Cisco 10000 series router.	PRE2
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.	PRE2

Prerequisites for Local AAA Server, User Database—Domain to VRF

The Local AAA Server, User Database—Domain to VRF feature has the following requirements:

- Configure an external AAA as described in *Cisco IOS Security Configuration Guide, Cisco IOS Release 12.2*.

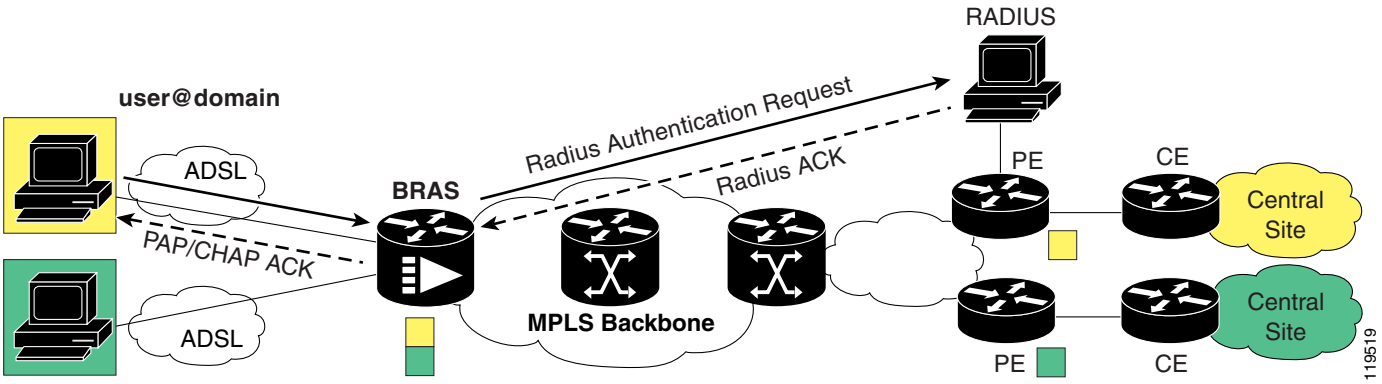
Establishing a PPP Connection

The following example describes the sequence of events involved in setting up AAA authentication, authorization, and accounting when a PPP connection is established and a local AAA server is used.

AAA Authentication

Figure 11-1 shows the AAA authentication set up when establishing a PPP connection.

Figure 11-1 AAA Authentication

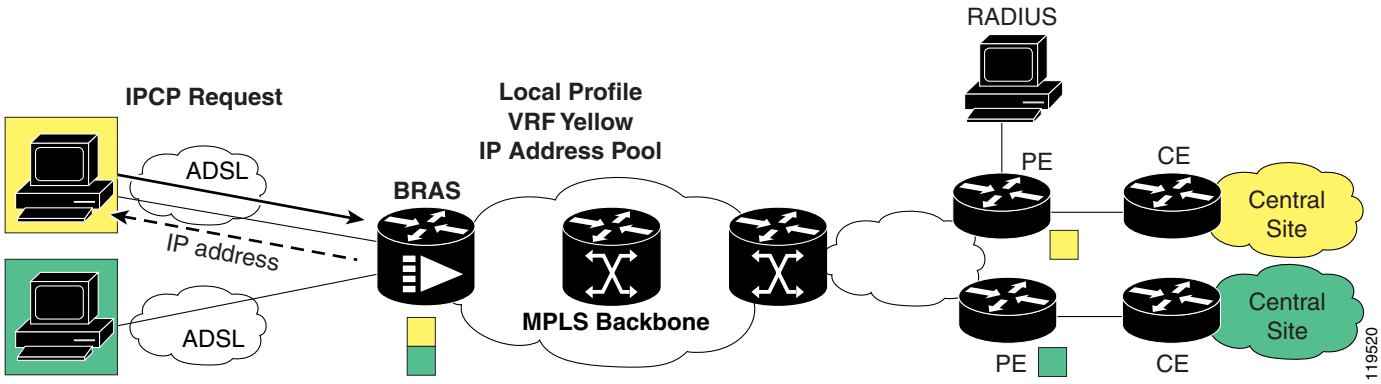


In the figure, the PPP client attempts to establish a PPP session with user@domain. This PAP or CHAP user name request is forwarded to the broadband remote access server (BRAS) for authentication. Authentication could be done locally on the BRAS, but in most cases the authentication is forwarded to a RADIUS server. The RADIUS server looks up the user@domain or user (if the BRAS strips off the domain), and if found sends a RADIUS ACK back to the BRAS. The BRAS sends a PAP or CHAP ACK back to the PPP client.

AAA Authorization

Figure 11-2 shows the AAA authorization set up when establishing a PPP connection.

Figure 11-2 AAA Authorization

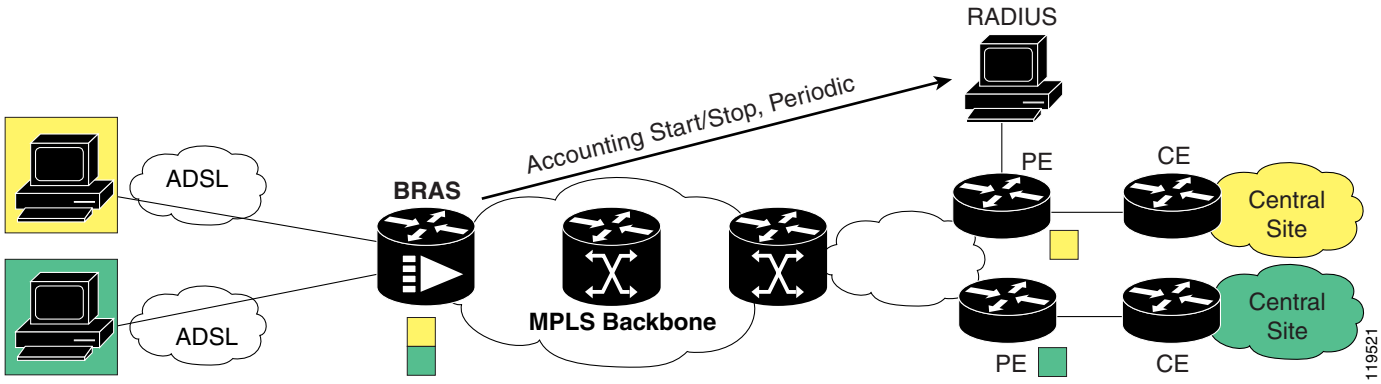


In the figure, the PPP client requests an IP address using PPP IPCP to the BRAS. The BRAS does a match of the domain to a local profile. This local profile contains the VRF to assign to this PPP session. The BRAS replies back to the PPP client with an IP address from the defined IP address pool in the local profile.

AAA Accounting

Figure 11-3 shows the AAA accounting set up when establishing a PPP connection.

Figure 11-3 AAA Accounting



In the figure, the BRAS can be configured to provide AAA accounting start/stop and periodic records for each PPP session. The BRAS can also be configured to provide NAS-Port information in the accounting records that will detail the slot/card/interface and VPI/VCI or VLAN.

AAA Attribute Lists

AAA Attribute Lists are used by the subscriber profiles when there is a match of the user name domain. These lists define RADIUS user profiles local to the router. The attributes are available for configuration using the **aaa attribute list** *name* global configuration command. Every attribute known to AAA is made available for configuration.

The AAA attributes that are defined in the AAA attribute list are standard RADIUS attributes, however they are in the Cisco IOS AAA format of the attribute. You must convert the attributes from RADIUS format to Cisco IOS AAA format.

Converting from RADIUS Format to Cisco IOS AAA Format

Use the **show aaa attribute protocol radius** command to get the Cisco IOS AAA format of the IETF RADIUS Attribute. This provides a complete list of all the aaa attributes supported. The following is an example where you need to convert the RADIUS attribute Filter-Id to Cisco IOS AAA format. This example represents part of the output of the **show aaa attribute protocol radius** command.

IIETF defined attributes:

```
Type=4     Name=acl                            Format=Ulong
Protocol:RADIUS
Unknown       Type=11    Name=Filter-Id             Format=Binary
```

Cisco IOS converts the IETF RADIUS attribute 11 (Filter-Id) of type Binary into an internal attribute named acl of type Ulong. Now you can configure this attribute locally using the attribute type acl.

Note You cannot add new AAA attributes during the conversion process. The conversion is only making the attributes configurable and usable locally on the router. The defined local AAA attributes must be supported RADIUS attributes.

Defining AAA Attribute Lists

Typically, you define an AAA attribute list for each user name domain. Cisco IOS Release 12.3(7)XI1 introduces the following two new commands to define local AAA attribute lists and attribute types:

Command	Purpose
Router(config)# **aaa attribute list** *aaa attribute list name*	Defines an AAA attribute list locally on the router. This attribute list is applied to the PPP session. *aaa attribute name* is the name of the local AAA attribute list.
Router(config)# **aaa attribute type** *name value* [**service ppp**] [**protocol** {**ip** | **atm** | **vpdn**}] [*tag*]	Defines an AAA attribute locally on the router. These attributes are RADIUS attributes in Cisco IOS AAA format. *name* defines the Cisco IOS AAA internal name of the IETF RADIUS attribute. *value* defines a string, binary, or IPv4 address value. This is the RADIUS attribute that is being defined but in IOS AAA format. **service** defines the access method, which is typically PPP. **protocol** can be ip, atm, or vpdn. *tag* provides a means of grouping attributes that refer to the same VPDN tunnel.

The following is an example of the commands you use to configure method lists:

```
aaa attribute list <name>
attribute type <name> <value> <service> <protocol> <tag>
```

Subscriber Profiles

Subscriber profiles are used to match user domain names, and on a match to use a defined AAA attribute list. Cisco IOS Release 12.3(7)XI1 introduces the following new command to define subscriber profiles:

Command	Purpose
Router(config)# **subscriber profile** *domain-name*	Defines an AAA attribute list locally on the router. This attribute list is applied to the PPP session. *domain-name* is the PPP user name domain.

The following is an example of the commands you use to configure a subscriber profile:

```
subscriber authorization enable
subscriber profile domain-name
service local
aaa attribute list aaa attribute list name
```

AAA Method Lists

The AAA method lists are defined to use RADIUS for authentication and accounting. Authorization is done locally using the AAA attribute lists. Defining the AAA attribute lists for PPP under the virtual template no longer requires defining the AAA lists. Instead, a default authentication and authorization list can be defined on the virtual template and the AAA method lists can be defined in the AAA attribute lists. 2000 method lists are supported.

Using method lists does require that you define **aaa authentication ppp default** and **aaa authorization network default** lists. The following is an example of the commands you use to configure method lists:

```
interface virtual-template
ppp authentication pap chap

aaa new-model
aaa authentication ppp default local
aaa authorization network default local
aaa authentication ppp method list name group radius
aaa authorization network method list name local if-authenticated
aaa accounting network method list name start-stop group radius

aaa attribute list <domain name>
attribute type ppp-authen-list "method list name"
attribute type ppp-author-list "method list name"
attribute type ppp-acct-list "method list name"
```

Configuration Tasks for Local AAA Server, User Database—Domain to VRF Using Local Attributes

To configure a user name domain to a VRF using local AAA attributes, perform the following configuration tasks:

- Defining AAA, page 11-6
- Defining RADIUS and Enabling NAS-PORT, page 11-7
- Defining a VRF, page 11-7
- Applying AAA to a Virtual Template, page 11-7
- Defining a Loopback Interface, page 11-8
- Creating an IP Address Pool, page 11-8
- Defining a Subscriber Profile, page 11-8
- Defining an AAA Attribute List, page 11-8

Defining AAA

To define AAA (authentication, authorization, and accounting), enter the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa new-model`	Enables the AAA access control model.
Step 2	`Router(config)# aaa authentication ppp list-name group radius`	Specifies RADIUS to authenticate the PPP user name.

	Command	Purpose
Step 3	`Router(config)# aaa authorization network` *list-name* **local if-authenticated**	Specifies to use the local profile if authenticated.
Step 4	`Router(config)# aaa accounting network` *list-name* **start-stop group radius**	Specifies RADIUS accounting as optional.
Step 5	`Router(config)# aaa authentication ppp default local`	Required to allow the definition of the AAA authentication list in the AAA attribute list.
Step 6	`Router(config)# aaa authorization network default local`	Required to allow the definition of the AAA authorization list in the AAA attribute list.

Defining RADIUS and Enabling NAS-PORT

To define RADIUS and enable NAS-PORT, enter the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# radius-server host` *ip-address* **auth-port 1645 acct-port 1646 key** *password*	Defines the Radius server that AAA authentication, authorization and accounting requests are sent to.
Step 2	`Router(config)# radius-server attribute nas-port format d`	Defines NAS-Port information to be sent to the AAA accounting server. (optional)

Defining a VRF

To define a VRF, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ip vrf` *vrf-name*	Enters VRF configuration mode and defines the VRF instance by assigning a VRF name.
Step 2	`Router(config-vrf)# rd` *route-distinguisher*	Creates routing and forwarding tables.
Step 3	`Router(config-vrf)# route-target` {**import** | **export** | **both**} *route-target-ext-community*	Creates a list of import an export route target communities for the specified VRF.

Applying AAA to a Virtual Template

To apply AAA to a virtual template, enter the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface virtual-template` *number*	Defines the virtual template to use for PPP.
Step 2	`Router(config)# ppp mtu adaptive`	For PPPoE, defines auto negotiation of MTU size.
Step 3	`Router(config)# ppp authentication pap chap`	Enables PAP, then CHAP, for PPP authentication.

Defining a Loopback Interface

To define a loopback interface, enter the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface loopback number`	Defines a loopback for the PPP session.
Step 2	`Router(config)# ip vrf forwarding vrf name`	Enables VRF forwarding.
Step 3	`Router(config)# ip address address mask`	Sets the IP address.

Creating an IP Address Pool

To an IP address pool, enter the following command in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ip local pool start address end address`	Defines an IP pool from which the PPP sessions are IP addresses.

Defining a Subscriber Profile

To define a subscriber profile, enter the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# subscriber authorization enable`	Enables subscriber authorization.
Step 2	`Router(config)# subscriber profile domain-name`	Specifies the user name domain to match.
Step 3	`Router(config)# service local`	Specifies to perform local subscriber authorization.
Step 4	`Router(config)# aaa attribute list aaa attribute-list name`	Defines the AAA attribute list from which to get RADIUS attributes and that is applied to the PPP session.

Defining an AAA Attribute List

To define AAA attribute list, enter the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa attribute list aaa attribute-list name`	Defines an AAA attribute list.
Step 2	`Router(config)# attribute type addr-pool pool_name protocol ip`	Defines an IP address pool to use.
Step 3	`Router(config)# attribute type ip-unnumbered loopback number service ppp protocol ip`	Defines the loopback interface to use.
Step 4	`Router(config)# attribute type vrf-id vrf_name service ppp protocol ip`	Defines the VRF to use.

	Command	Purpose
Step 5	`Router(config)# attribute type ppp-authen-list aaa_list_name`	Defines the AAA authentication list to use.
Step 6	`Router(config)# attribute type ppp-author-list aaa_list_name`	Defines the AAA authorization list to use.
Step 7	`Router(config)# attribute type ppp-acct-list aaa_list_name`	Defines the AAA accounting list to use.

Verifying Local AAA Server, User Database—Domain to VRF Using Local Attributes

To verify domain to VRF using local attributes, use the **show aaa users all** command and the **show running-config** command. See the next section for a configuration example.

Configuration Example for Local AAA Server, User Database—Domain to VRF

The following configuration example has two subscriber profiles that match on domain cisco1.com and cisco2.com.

A subscriber with the domain name cisco1.com uses the parameters defined in the subscriber profile cisco1.com. The name of the subscriber profile must be identical to the domain part of the full username (username@domain). An attribute list cisco1.com defined in the service profile is used to reference AAA attributes for the PPP subscribers.

Subscriber cisco1.com is applied with AAA attributes from AAA attribute list cisco1.com. An attribute is applied to put the PPP session into a VRF called vrf1. An IP address is assigned from a local DHCP pool called dhcp-pool. AAA authentication, authorization, and accounting are also defined and use an AAA list called test1. These all use an AAA group server called group_server_test1.

A subscriber with the domain name cisco2.com uses the parameters defined in the subscriber profile cisco2.com. The name of the subscriber profile must be identical to the domain part of the full username (username@domain). An attribute list cisco2.com defined in the service profile is used to reference aaa attributes for the PPP subscribers.

Subscriber cisco2.com is applied with AAA attributes from AAA attribute list cisco2.com. An attribute is applied to put the PPP session into a VRF called vrf2. An IP address is assigned from a local pool called pppoe2. AAA authentication, authorization, and accounting are also defined and use an AAA list called test2. These all use an AAA group server called group_server_test2.

```
aaa new-model
!
!
aaa group server radius group_server_test1
 server-private 192.168.2.20 auth-port 1645 acct-port 1646 key cisco
 ip vrf forwarding vrf1
!
aaa group server radius group_server_test2
 server-private 192.168.2.12 auth-port 1645 acct-port 1646 key cisco
 ip vrf forwarding vrf2
!
aaa authentication ppp default local
aaa authentication ppp test1 group test1
aaa authentication ppp test2 group test2
aaa authorization network default local
aaa authorization network test1 local if-authenticated
```

```
aaa authorization network test2 local if-authenticated
aaa accounting delay-start all
aaa accounting network test1 start-stop group group_server_test1
aaa accounting network test2 start-stop group group_server_test2
!
aaa attribute list cisco1.com
 attribute type addr-pool "dhcp-pool" protocol ip
 attribute type ip-unnumbered "loopback1" service ppp protocol ip
 attribute type vrf-id "vrf1" service ppp protocol ip
 attribute type ppp-authen-list "test1"
 attribute type ppp-author-list "test1"
 attribute type ppp-acct-list "test1"
!
aaa attribute list cisco2.com
 attribute type addr-pool "pppoe2" protocol ip
 attribute type ip-unnumbered "loopback2" service ppp protocol ip
 attribute type vrf-id "vrf2" service ppp protocol ip
 attribute type ppp-authen-list "test2"
 attribute type ppp-author-list "test2"
 attribute type ppp-acct-list "test2"
!
ip dhcp pool dhcp-pool
   vrf vrf1
   network 101.1.0.0 255.255.0.0
   default-router 100.1.1.1
   lease 0 2 30
!
ip vrf vrf1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
ip vrf vrf2
 rd 2:2
 route-target export 2:2
 route-target import 2:2
!
subscriber authorization enable
!
subscriber profile cisco1.com
 service local
 aaa attribute list cisco1.com
!
subscriber profile cisco2.com
 aaa attribute list cisco2.com
!
vpdn enable
!
ppp hold-queue 80000
no virtual-template snmp
!
buffers small permanent 15000
buffers middle permanent 12000
buffers large permanent 1000
!
bba-group pppoe cisco1.com
 virtual-template 1
!
bba-group pppoe cisco2.com
 virtual-template 2
!
interface Loopback1
 ip vrf forwarding vrf1
 ip address 100.1.1.1 255.255.255.255
```

```
!
interface Loopback2
 ip vrf forwarding vrf2
 ip address 101.1.1.1 255.255.255.255
!
interface FastEthernet0/0/0
 shutdown
!
interface ATM1/0/0
 no ip address
 no atm pxf queuing
 no atm ilmi-keepalive
!
interface ATM1/0/0.1 multipoint
 pvc 1/32
  encapsulation aal5autoppp Virtual-Template1 group cisco1.com
  no create on-demand
!
!
interface ATM1/0/0.2 multipoint
 pvc 1/33
  encapsulation aal5autoppp Virtual-Template2 group cisco2.com
!
!
interface FastEthernet6/0/0
 ip vrf forwarding vrf1
 ip address 192.168.2.201 255.255.255.0
 duplex auto
!
interface FastEthernet6/0/1
 ip vrf forwarding vrf2
 ip address 192.168.2.202 255.255.255.0
 duplex auto
!
interface Virtual-Template1
 no ip address
 no logging event link-status
 no snmp trap link-status
 ppp mtu adaptive
 ppp authentication chap callin
!
ip local pool pppoe2 12.1.1.1 12.1.250.1
!
ip radius source-interface FastEthernet6/0/0.1 vrf vrf1
ip radius source-interface FastEthernet6/0/0.2 vrf vrf2
!
radius-server attribute nas-port format d
radius-server domain-stripping
```

Example—VRF with DBS

Applying the PCR and SCR to this PPP:

```
aaa attribute list cisco1.com
attribute type addr-pool "pppoe" protocol ip
attribute type ip-unnumbered "loopback1" service ppp protocol ip
attribute type vrf-id "vrf1" service ppp protocol ip
attribute type peak-cell-rate 2048 protocol atm
attribute type sustainable-cell-rate 1024 protocol atm
```

Example—VRF with ACL

Applying a defined output ACL to this PPP:

```
aaa attribute list cisco1.com
attribute type addr-pool "pppoe" protocol ip
attribute type ip-unnumbered "loopback1" service ppp protocol ip
attribute type vrf-id "vrf1" service ppp protocol ip
attribute type outacl "101" service ppp protocol ip

access-list 101 deny   icmp any any
```

Monitoring and Maintaining Local AAA Server, User Database—Domain to VRF

The following debug commands can be helpful in monitoring and maintaining Local AAA Server, User Database—Domain to VRF:

- **debug aaa id**—displays a unique key for a session and provides a way to track sessions
- **debug aaa authentication**—displays the methods of authentication being used and the results of these methods
- **debug aaa authorization**—displays the methods of authorization being used and the results of these methods
- **debug aaa per-user**—displays information about per-user QoS parameters
- **debug ppp negotiation**—shows PPP negotiation debug messages
- **debug ppp authen**—indicates if a client is passing authentication
- **debug ppp error**—displays protocol errors and error statistics associated with PPP connection negotiation and operation
- **debug ppp forward**—displays who is taking control of a session
- **debug sss error**—displays diagnostic information about errors that may occur during Subscriber Service Switch (SSS) call setup
- **debug radius**—displays information about the RADIUS server

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco Systems technical support personnel. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.