Configuring RADIUS

The RADIUS security system is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco devices and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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.

Prerequisites for RADIUS

To configure RADIUS on your Cisco device or access server, you must perform these tasks:

- Use the **aaa new-model** global configuration command to enable Authentication, Authorization, and Accounting (AAA). AAA must be configured if you plan to use RADIUS.
- Use the **aaa authentication** global configuration command to define method lists for RADIUS authentication.

- Use **line** and **interface** commands to enable the defined method lists to be used.

Information About RADIUS

RADIUS Network Environments

Cisco supports RADIUS under its authentication, authorization, and accounting (AAA) security paradigm. RADIUS can be used with other AAA security protocols such as TACACS+, Kerberos, and local username lookup. RADIUS is supported on all Cisco platforms, but some RADIUS-supported features run only on specified platforms.

RADIUS has been implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

Use RADIUS in the following network environments that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server that has been customized to work with the Kerberos security system.
- Turnkey network security environments in which applications support the RADIUS protocol, such as in an access environment that uses a smart card access control system. In one case, RADIUS has been used with Enigma's security cards to validate users and grant access to network resources.
- Networks already using RADIUS. You can add a Cisco device with RADIUS to the network. This might be the first step when you make a transition to a TACACS+ server.
- Networks in which a user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to a single protocol such as PPP. For example, when a user logs in, RADIUS identifies this user as having authorization to run PPP using the IP address 10.2.3.4 and the defined access list is started.
- Networks that require resource accounting. You can use RADIUS accounting independent of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, and bytes) used during the session. An ISP might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.
- Networks that support preauthentication. Using the RADIUS server in your network, you can configure AAA preauthentication and set up the preauthentication profiles. Preauthentication enables service providers to better manage ports using their existing RADIUS solutions, and to efficiently manage the use of shared resources to offer differing service-level agreements.

RADIUS is not suitable in these network security situations:

- Multiprotocol access environments. RADIUS does not support the following protocols:
  - AppleTalk Remote Access (ARA)
  - NetBIOS Frame Control Protocol (NBFCP)
  - NetWare Asynchronous Services Interface (NASI)

- X.25 Packet Assemblers/Disassemblers (PAD) connections

- Device-to-device situations. RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one device to a non-Cisco device if the non-Cisco device requires RADIUS authentication.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

RADIUS Operation

When a user attempts to log in and authenticate to an access server using RADIUS, the following steps occur:

1. The user is prompted to enter the username and password.
2. The username and encrypted password are sent over the network to the RADIUS server.
3. The user receives one of the following responses from the RADIUS server:
    1. ACCEPT—The user is authenticated.
    2. CHALLENGE—A challenge is issued by the RADIUS server. The challenge collects additional data from the user.
    3. CHANGE PASSWORD—A request is issued by the RADIUS server, asking the user to select a new password.
    4. REJECT—The user is not authenticated and is prompted to reenter the username and password, or access is denied.

The ACCEPT or REJECT response is bundled with additional data that is used for EXEC or network authorization. You must first complete RADIUS authentication before using RADIUS authorization. The additional data included with the ACCEPT or REJECT packets consists of the following:

- Services that the user can access, including connections such as Telnet, rlogin, or local-area transport (LAT), and services such as PPP, Serial Line Protocol (SLIP), or EXEC services.
- Connection parameters, including the host or client IP address, access list, and user timeouts.

RADIUS Attributes

The network access server monitors the RADIUS authorization and accounting functions defined by RADIUS attributes in each user profile:

Vendor-Proprietary RADIUS Attributes

An Internet Engineering Task Force (IETF) standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server and the RADIUS server. Some vendors, nevertheless, have extended the RADIUS attribute set in a unique way. Cisco software supports a subset of vendor-proprietary RADIUS attributes.

RADIUS Tunnel Attributes

RADIUS is a security server AAA protocol originally developed by Livingston, Inc. RADIUS uses attribute value (AV) pairs to communicate information between the security server and the network access server.

RFC 2138 and RFC 2139 describe the basic functionality of RADIUS and the original set of IETF-standard AV pairs used to send AAA information. Two IETF standards, "RADIUS Attributes for Tunnel Protocol Support" and "RADIUS Accounting Modifications for Tunnel Protocol Support," extend the IETF-defined set of AV pairs to include attributes specific to VPNs. These attributes are used to carry the tunneling information between the RADIUS server and the tunnel initiator.

RFC 2865 and RFC 2868 extend the IETF-defined set of AV pairs to include attributes specific to compulsory tunneling in VPNs by allowing the user to specify authentication names for the network access server and the RADIUS server.

Cisco devices and access servers support new RADIUS IETF-standard virtual private dialup network (VPDN) tunnel attributes.

Preauthentication on a RADIUS Server

RADIUS attributes are configured in the RADIUS preauthentication profiles to specify preauthentication behavior. In addition to configuring preauthentication on your Cisco device, you must set up the preauthentication profiles on the RADIUS server.

RADIUS Profile for DNIS or CLID Preauthentication

To configure the RADIUS preauthentication profile, use the Dialed Number Identification Service (DNIS) or Calling Line Identification (CLID) number as the username, and use the password defined in the **dnis** or **clid** command as the password.

Note The preauthentication profile must have "outbound" as the service type because the password is predefined on the network access server (NAS). Setting up the preauthentication profile in this manner prevents users from trying to log in to the NAS with the username of the DNIS number, CLID number, or call type and an obvious password. The "outbound" service type is also included in the Access-Request packet sent to the RADIUS server.

RADIUS Profile for Call Type Preauthentication

To set up the RADIUS preauthentication profile, use the call type string as the username, and use the password defined in the **ctype** command as the password. The table below lists the call type strings that can be used in the preauthentication profile.

Table 1: Call Type Strings Used in Preauthentication

Call Type String	ISDN Bearer Capabilities
digital	Unrestricted digital, restricted digital.

Call Type String	ISDN Bearer Capabilities
speech	Speech, 3.1 kHz audio, 7 kHz audio. **Note** This is the only call type available for channel-associated signaling (CAS) .
v.110	Anything with the V.110 user information layer.
v.120	Anything with the V.120 user information layer.

Note The preauthentication profile must have “outbound” as the service type because the password is predefined on the NAS. Setting up the preauthentication profile in this manner prevents users from trying to log in to the NAS with the username of the DNIS number, CLID number, or call type and an obvious password. The “outbound” service type is also included in the Access-Request packet sent to the RADIUS server and should be a checkin item if the RADIUS server supports checkin items.

RADIUS Profile for Preauthentication Enhancements for Callback

Callback allows remote network users such as telecommuters to dial in to the NAS without being charged. When callback is required, the NAS hangs up the current call and dials the caller back. When the NAS performs the callback, only information for the outgoing connection is applied. The rest of the attributes from the preauthentication access-accept message are discarded.

Note The destination IP address is not required to be returned from the RADIUS server.

The following example shows a RADIUS profile configuration with a callback number of 555-0101 and the service type set to outbound. The cisco-avpair = “preauth:send-name=<string>” uses the string “user1” and the cisco-avpair = “preauth:send-secret=<string>” uses the password “cisco.”

```
5550101 password = “cisco”, Service-Type = Outbound
Service-Type = Callback-Framed
Framed-Protocol = PPP,
Dialback-No = “5550119”
Class = “ISP12”
cisco-avpair = “preauth:send-name=user1”
cisco-avpair = “preauth:send-secret=cisco”
```

RADIUS Profile for a Remote Hostname Used for Large-Scale Dial-Out

The following example protects against accidentally calling a valid telephone number but accessing the wrong device by providing the name of the remote device, for use in large-scale dial-out:

```
5550101 password = "PASSWORD1", Service-Type = Outbound
       Service-Type = Callback-Framed
       Framed-Protocol = PPP,
       Dialback-No = "5550190"
       Class = "ISP12"
```

```
cisco-avpair = "preauth:send-name=user1"
cisco-avpair = "preauth:send-secret=PASSWORD1"
cisco-avpair = "preauth:remote-name=Device2"
```

RADIUS Profile for Modem Management

When DNIS, CLID, or call type preauthentication is used, the affirmative response from the RADIUS server might include a modem string for modem management in the NAS through vendor-specific attribute (VSA) 26. The modem management VSA has this syntax:

```
cisco-avpair = “preauth:modem-service=modem min-speed <
x
> max-speed <
y
>
modulation <
z
> error-correction <
a
> compression <
b
>"
```

The table below lists the modem management string elements within the VSA.

Table 2: Modem Management String

Command	Argument
min-speed	300 to 56000, any
max-speed	300 to 56000, any
modulation	K56Flex, v22bis, v32bis, v34, v90, any
error-correction	lapm, mnp4
compression	mnp5, v42bis

When the modem management string is received from the RADIUS server in the form of a VSA, the information is passed to the Cisco software and applied on a per-call basis. Modem ISDN channel aggregation (MICA) modems provide a control channel through which messages can be sent during the call setup time. Hence, this modem management feature is supported only with MICA modems. This feature is not supported with Microcom modems.

RADIUS Profile for Subsequent Authentication

If preauthentication passes, you can use vendor-proprietary RADIUS attribute 201 (Require-Auth) in the preauthentication profile to determine whether subsequent authentication is performed. If attribute 201, returned in the access-accept message, has a value of 0, subsequent authentication is not performed. If attribute 201 has a value of 1, subsequent authentication is performed as usual.

Attribute 201 has this syntax:

```
cisco-avpair = “preauth:auth-required=<
```

```
n
>"
```

where <*n*> has the same value range as attribute 201 (that is, 0 or 1).

If attribute 201 is missing in the preauthentication profile, a value of 1 is assumed, and subsequent authentication is performed.

Note Before you can perform subsequent authentication, you must set up a regular user profile in addition to a preauthentication profile.

RADIUS Profile for Subsequent Authentication Types

If you specified subsequent authentication in the preauthentication profile, you must also specify the authentication types to be used for subsequent authentication. To specify the authentication types allowed in subsequent authentication, use this VSA:

```
cisco-avpair = "preauth:auth-type=<
string
>"
```

The table below lists the allowed values for the <*string*> element.

Table 3: <string> Element Values

String	Description
chap	Requires the username and password for the Challenge-Handshake Authentication Protocol (CHAP) for PPP authentication.
ms-chap	Requires the username and password for the MS-CHAP for PPP authentication.
pap	Requires the username and password for the Password Authentication Protocol (PAP) for PPP authentication.

To specify that multiple authentication types are allowed, you can configure more than one instance of this VSA in the preauthentication profile. The sequence of the authentication type VSAs in the preauthentication profile is significant because it specifies the order of authentication types to be used in the PPP negotiation.

This VSA is a per-user attribute and replaces the authentication type list in the **ppp authentication** interface configuration command.

Note You should use this VSA only if subsequent authentication is required because it specifies the authentication type for subsequent authentication.

RADIUS Profile to Include the Username

If only preauthentication is used to authenticate a call, the NAS could be missing a username when it brings up the call. RADIUS can provide a username for the NAS to use through RADIUS attribute 1 (User-Name) or through a VSA returned in the Access-Accept packet. The VSA for specifying the username has this syntax:

```
cisco-avpair = “preauth:username=<
string
>”
```

If no username is specified, the DNIS number, CLID number, or call type is used, depending on the last preauthentication command configured (for example, if **clid** was the last preauthentication command configured, the CLID number is used as the username).

If subsequent authentication is used to authenticate a call, there might be two usernames: one provided by RADIUS and one provided by the user. In this case, the username provided by the user overrides the one contained in the RADIUS preauthentication profile. The username provided by the user is used for both authentication and accounting.

RADIUS Profile for Two-Way Authentication

In the case of two-way authentication, the calling networking device must authenticate the NAS. The PAP username and password or CHAP username and password need not be configured locally on the NAS. Instead, the username and password can be included in the Access-Accept messages for preauthentication.

Note Do not configure the **ppp authentication** command with the **radius** command.

To set up PAP, do not configure the **ppp pap sent-name password** command on the interface. The VSAs “preauth:send-name” and “preauth:send-secret” are used as the PAP username and PAP password for outbound authentication.

For CHAP, “preauth:send-name” is used not only for outbound authentication but also for inbound authentication. For a CHAP inbound case, the NAS uses the name defined in “preauth:send-name” in the challenge packet to the caller networking device. For a CHAP outbound case, both “preauth:send-name” and “preauth:send-secret” are used in the response packet.

The following example shows a configuration that specifies two-way authentication:

```
5550101 password = "PASSWORD2", Service-Type = Outbound
Service-Type = Framed-User
cisco-avpair = "preauth:auth-required=1"
cisco-avpair = "preauth:auth-type=pap"
cisco-avpair = "preauth:send-name=user1"
cisco-avpair = "preauth:send-secret=PASSWORD2"
class = "<some class>"
```

Note Two-way authentication does not work when resource pooling is enabled.

RADIUS Profile to Support Authorization

If only preauthentication is configured, subsequent authentication is bypassed. Note that because the username and password are not available, authorization is also bypassed. However, you can include authorization attributes in the preauthentication profile to apply per-user attributes and avoid having to return subsequently to RADIUS for authorization. To initiate the authorization process, you must also configure the **aaa authorization network** command on the NAS.

You can configure authorization attributes in the preauthentication profile with one exception: the service-type attribute (attribute 6). The service-type attribute must be converted to a VSA in the preauthentication profile. This VSA has this syntax:

```
cisco-avpair = "preauth:service-type=<
n
>"
```

where <*n*> is one of the standard RFC 2865 values for attribute 6.

Note If subsequent authentication is required, the authorization attributes in the preauthentication profile are not applied.

RADIUS Authentication

After you have identified the RADIUS server and defined the RADIUS authentication key, you must define method lists for RADIUS authentication. Because RADIUS authentication is facilitated through AAA, you must enter the **aaa authentication** command, specifying RADIUS as the authentication method.

RADIUS Authorization

AAA authorization lets you set parameters that restrict a user's access to the network. Authorization using RADIUS provides one method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, AppleTalk Remote Access (ARA), and Telnet. Because RADIUS authorization is facilitated through AAA, you must enter the **aaa authorization** command, specifying RADIUS as the authorization method.

RADIUS Accounting

The AAA accounting feature enables you to track the services users are accessing and the amount of network resources they are consuming. Because RADIUS accounting is facilitated through AAA, you must enter the **aaa accounting** command, specifying RADIUS as the accounting method.

RADIUS Login-IP-Host

To enable the network access server (NAS) to attempt more than one login host when trying to connect a dial-in user, you can enter as many as three Login-IP-Host entries in the user's profile on the RADIUS server.

The following example shows that three Login-IP-Host instances are configured for the user *user1*, and that TCP-Clear is used for the connection:

```
user1 Password = xyz
        Service-Type = Login,
        Login-Service = TCP-Clear,
        Login-IP-Host = 10.0.0.0,
        Login-IP-Host = 10.2.2.2,
        Login-IP-Host = 10.255.255.255,
        Login-TCP-Port = 23
```

The order in which the hosts are entered is the order in which they are attempted. Use the **ip tcp synwait-time** command to set the number of seconds that the NAS waits before trying to connect to the next host on the list; the default is 30 seconds.

Your RADIUS server might permit more than three Login-IP-Host entries; however, the NAS supports only three hosts in Access-Accept packets.

RADIUS Prompt

To control whether user responses to Access-Challenge packets are echoed to the screen, you can configure the Prompt attribute in the user profile on the RADIUS server. This attribute is included only in Access-Challenge packets. The following example shows the Prompt attribute set to No-Echo, which prevents the user's responses from echoing:

```
user1 Password = xyz
Service-Type = Login,
Login-Service = Telnet,
Prompt = No-Echo,
Login-IP-Host = 172.31.255.255
```

To allow user responses to echo, set the attribute to Echo. If the Prompt attribute is not included in the user profile, responses are echoed by default.

This attribute overrides the behavior of the **radius-server challenge-noecho** command configured on the access server. For example, if the access server is configured to suppress echoing, but the individual user profile allows echoing, the user responses are echoed.

Note If you want to use the Prompt attribute, your RADIUS server must be configured to support Access-Challenge packets.

Vendor-Specific RADIUS Attributes

The IETF standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes 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 with this format:

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

"Protocol" is a value of the Cisco "protocol" attribute for a particular type of authorization; protocols that can be used include IP, Internetwork Packet Exchange (IPX), VPDN, VoIP, Secure Shell (SSH), Resource

Reservation Protocol (RSVP), Serial Interface Processor (SIP), AirNet, and Outbound. “Attribute” and “value” are an appropriate AV pair defined in the Cisco TACACS+ specification, and “sep” is “=” for mandatory attributes and “*” for optional attributes, allowing the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair causes Cisco’s “multiple named ip address pools” feature to be activated during IP authorization (during PPP’s Internet Protocol Control Protocol (IPCP) address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

If you insert an “*”, the AV pair “ip:addr-pool=first” becomes optional. Note that any AV pair can be made optional:

```
cisco-avpair= "ip:addr-pool*first"
```

The following example shows how to cause a user logging in from a network access server to have immediate access to EXEC commands:

```
cisco-avpair= "shell:priv-lvl=15"
```

Other vendors have their own unique vendor IDs, options, and associated VSAs.

Static Routes and IP Addresses on the RADIUS Server

Some vendor-proprietary implementations of RADIUS let the user define static routes and IP pool definitions on the RADIUS server instead of on each individual network access server in the network. Each network access server then queries the RADIUS server for static route and IP pool information.

To have the Cisco device or access server query the RADIUS server for static routes and IP pool definitions when the device starts up, use the **radius-server configure-nas** command.

Because the **radius-server configure-nas** command is performed when the Cisco devcie starts up, it does not take effect until you enter a **copy system:running-config nvram:startup-config** command.

How to Configure RADIUS

Configuring a Device for Vendor-Proprietary RADIUS Server Communication

Although an IETF standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. Cisco software supports a subset of vendor-proprietary RADIUS attributes.

To configure RADIUS (whether vendor-proprietary or IETF compliant), you must use the **radius-server** commands to specify the host running the RADIUS server daemon and the secret text string it shares with the Cisco device. To identify that the RADIUS server is using a vendor-proprietary implementation of RADIUS, use the **radius-server host non-standard** command. Vendor-proprietary attributes are not supported unless you use the **radius-server host non-standard** command.

Note To configure an IPv4 or IPv6 RADIUS server, use the commands as mentioned below:

- If you have configured an IPv4 RADIUS server, you can use either the **radius-server host** command or the **radius server** *name* command.
- If you have configured an IPv6 RADIUS server, use the **radius server** *name* command.

For more information about the **radius server** command, see *Cisco IOS Security Command Reference: Commands M to R*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server vsa send** [**accounting** | **authentication**]
4. **radius-server host** {*hostname* | *ip-address*} **non-standard**
5. **radius-server key** {**0** *string* | **7** *string* | *string*}
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius-server vsa send** [**accounting** | **authentication**] **Example:** `Device(config)# radius-server vsa send`	Enables the network access server to recognize and use VSAs as defined by RADIUS IETF attribute 26.
Step 4	**radius-server host** {*hostname* | *ip-address*} **non-standard** **Example:** `Device(config)# radius-server host host1 non-standard`	Specifies the IP address or hostname of the remote RADIUS server host and identifies that it is using a vendor-proprietary implementation of RADIUS.

	Command or Action	Purpose
		Note To configure an IPv4 or IPv6 RADIUS server, use the commands as mentioned below: • If you have configured an IPv4 RADIUS server, you can use either the **radius-server host** command or the **radius server** *name* command. • If you have configured an IPv6 RADIUS server, use the **radius server** *name* command. For more information about the **radius server** command, see *Cisco IOS Security Command Reference: Commands M to R*.
Step 5	**radius-server key** {**0** *string* | **7** *string* | *string*} **Example:** `Device(config)# radius-server key myRaDIUSpassword`	Specifies the shared secret text string used between the device and the vendor-proprietary RADIUS server. • The device and the RADIUS server use this text string to encrypt passwords and exchange responses.
Step 6	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Configuring a Device to Expand Network Access Server Port Information

Sometimes PPP or login authentication occurs on an interface that is different from the interface on which the call itself comes in. For example, in a V.120 ISDN call, login or PPP authentication occurs on a virtual asynchronous interface “ttt”, but the call itself occurs on one of the channels of the ISDN interface.

The **radius-server attribute nas-port extended** command configures RADIUS to expand the size of the NAS-Port attribute (RADIUS IETF attribute 5) field to 32 bits. The upper 16 bits of the NAS-Port attribute display the type and number of the controlling interface; the lower 16 bits indicate the interface undergoing authentication.

Note The **radius-server attribute nas-port format** command replaces the **radius-server extended-portnames** command and the **radius-server attribute nas-port extended** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server configure-nas**
4. **radius-server attribute nas-port format**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius-server configure-nas** **Example:** `Device(config)# radius-server configure-nas`	(Optional) Tells the Cisco device or access server to query the RADIUS server for the static routes and IP pool definitions used throughout its domain. **Note** Because the **radius-server configure-nas** command is used when the Cisco device starts up, it does not take effect until you issue a **copy system:running-config nvram:startup-config** command.
Step 4	**radius-server attribute nas-port format** **Example:** `Device(config)# radius-server attribute nas-port format`	Expands the size of the NAS-Port attribute from 16 to 32 bits to display extended interface information.
Step 5	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Replacing the NAS-Port Attribute with the RADIUS Attribute

On platforms with multiple interfaces (ports) per slot, the Cisco RADIUS implementation does not provide a unique NAS-Port attribute that permits distinguishing between the interfaces. For example, if a dual PRI is in slot 1, calls on both Serial1/0:1 and Serial1/1:1 appear as NAS-Port = 20101 because of the 16-bit field size limitation associated with the RADIUS IETF NAS-Port attribute. In this case, you can replace the NAS-Port attribute with a VSA (RADIUS IETF attribute 26). Cisco's vendor ID is 9, and the Cisco-NAS-Port attribute is subtype 2. VSAs can be turned on by entering the **radius-server vsa send** command. The port information in this attribute is provided and configured using the **aaa nas port extended** command.

The standard NAS-Port attribute (RADIUS IETF attribute 5) is sent. If you do not want this information to be sent, you can suppress it by using the **no radius-server attribute nas-port** command. After this command is configured, the standard NAS-Port attribute is no longer sent.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server vsa send** [**accounting** | **authentication**]
4. **aaa nas port extended**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius-server vsa send** [**accounting** | **authentication**] **Example:** `Device(config)# radius-server vsa send`	Enables the network access server to recognize and use vendor-specific attributes as defined by RADIUS IETF attribute 26.
Step 4	**aaa nas port extended** **Example:** `Device(config)# aaa nas port extended`	Expands the size of the VSA NAS-Port field from 16 to 32 bits to display extended interface information.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Configuring the Suffix and Password in RADIUS Access Requests

Large-scale dial-out eliminates the need to configure dialer maps on every NAS for every destination. Instead, you can create remote site profiles that contain outgoing call attributes on the AAA server. The profile is downloaded by the NAS when packet traffic requires a call to be placed to a remote site.

You can configure the username in the Access-Request message to RADIUS. The default suffix of the username, "-out," is appended to the username. The format for composing the username attribute is the IP address plus the configured suffix.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa route download** *time*
5. **aaa authorization configuration default**
6. **interface dialer** *number*
7. **dialer aaa**
8. **dialer aaa suffix** *suffix* **password** *password*
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables the AAA access control model.
Step 4	**aaa route download** *time* **Example:** `Device(config)# aaa route download 450`	Enables the download static route feature and sets the amount of time in minutes between downloads.
Step 5	**aaa authorization configuration default** **Example:** `Device(config)# aaa authorization configuration default`	Downloads static route configuration information from the AAA server using TACACS+ or RADIUS.
Step 6	**interface dialer** *number* **Example:** `Device(config)# interface dialer 1`	Defines a dialer rotary group and enters interface configuration mode.
Step 7	**dialer aaa** **Example:** `Device(config-if)# dialer aaa`	Allows a dialer to access the AAA server for dialing information.
Step 8	**dialer aaa suffix** *suffix* **password** *password* **Example:** `Device(config-if)# dialer aaa suffix @samp password password12`	Allows a dialer to access the AAA server for dialing information and specifies a suffix and nondefault password for authentication.
Step 9	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to privileged EXEC mode.

Monitoring and Maintaining RADIUS

SUMMARY STEPS

1. **enable**
2. **debug radius**
3. **show radius statistics**
4. **show aaa servers**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug radius** **Example:** `Device# debug radius`	Displays information associated with RADIUS.
Step 3	**show radius statistics** **Example:** `Device# show radius statistics`	Displays the RADIUS statistics for accounting and authentication packets.
Step 4	**show aaa servers** **Example:** `Device# show aaa servers`	Displays the status and number of packets that are sent to and received from all public and private AAA RADIUS servers as interpreted by the AAA Server MIB.
Step 5	**exit** **Example:** `Device# exit`	Exits the device session.

Configuration Examples for RADIUS

Example: RADIUS Authentication and Authorization

The following example shows how to configure the device to authenticate and authorize using RADIUS:

```
aaa authentication login use-radius group radius local
aaa authentication ppp user-radius if-needed group radius
aaa authorization exec default group radius
aaa authorization network default group radius
```

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:

- The **aaa authentication login use-radius group radius local** command configures the device to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database. In this example, **use-radius** is the name of the method list, which specifies RADIUS and then local authentication.
- The **aaa authentication ppp user-radius if-needed group radius** command configures the Cisco software to use RADIUS authentication for lines using PPP with CHAP or PAP if the user has not already been authorized. If the EXEC facility has authenticated the user, RADIUS authentication is not performed. In this example, **user-radius** is the name of the method list defining RADIUS as the if-needed authentication method.
- The **aaa authorization exec default group radius** command sets the RADIUS information that is used for EXEC authorization, autocommands, and access lists.
- The **aaa authorization network default group radius** command sets RADIUS for network authorization, address assignment, and access lists.

Example: RADIUS Authentication, Authorization, and Accounting

The following example shows a general configuration using RADIUS with the AAA command set:

```
radius-server host 10.45.1.2
radius-server key myRaDiUSpassWoRd
username root password ALongPassword
aaa authentication ppp dialins group radius local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa authentication login admins local
aaa authorization exec default local
line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem ri-is-cd
interface group-async 1
 encaps ppp
 ppp authentication pap dialins
```

The lines in this example RADIUS authentication, authorization, and accounting configuration are defined as follows:

- The **radius-server host** command defines the IP address of the RADIUS server host.

- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **aaa authentication ppp dialins group radius local** command defines the authentication method list “dialins,” which specifies that RADIUS authentication and then (if the RADIUS server does not respond) local authentication is used on serial lines using PPP.
- The **aaa authorization network default group radius local** command is used to assign an address and other network parameters to the RADIUS user.
- The **aaa accounting network default start-stop group radius** command tracks PPP usage.
- The **aaa authentication login admins local** command defines another method list, “admins,” for login authentication.
- The **login authentication admins** command applies the “admins” method list for login authentication.
- The **ppp authentication pap dialins** command applies the “dialins” method list to the lines specified.

Example: Vendor-Proprietary RADIUS Configuration

The following example shows a general configuration using vendor-proprietary RADIUS with the AAA command set:

Note To configure an IPv4 or IPv6 RADIUS server, use the commands as mentioned below:

- If you have configured an IPv4 RADIUS server, you can use either the **radius-server host** command or the **radius server** *name* command.
- If you have configured an IPv6 RADIUS server, use the **radius server** *name* command.

For more information about the **radius server** command, see *Cisco IOS Security Command Reference: Commands M to R*.

```
radius server myserver
radius server address ipv4 192.0.2.2
radius server non-standard
radius server key 7 anykey
radius-server configure-nas
username root password ALongPassword
aaa authentication ppp dialins group radius local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa authentication login admins local
aaa authorization exec default local
```

The lines in this RADIUS authentication, authorization, and accounting configuration example are defined as follows:

- The **radius server** *name* **non-standard** command defines the name of the RADIUS server host and identifies that this RADIUS host uses a vendor-proprietary version of RADIUS.
- The **radius server** *name* **key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **radius-server configure-nas** command defines that the Cisco device or access server queries the RADIUS server for static routes and IP pool definitions when the device first starts up.

- The **aaa authentication ppp dialins group radius local** command defines the authentication method list "dialins," which specifies that RADIUS authentication and then (if the RADIUS server does not respond) local authentication is used on serial lines using PPP.
- The **aaa authorization network default group radius local** command assigns an address and other network parameters to the RADIUS user.
- The **aaa accounting network default start-stop group radius** command tracks PPP usage.
- The **aaa authentication login admins local** command defines another method list, "admins," for login authentication.

Example: Multiple RADIUS Server Entries for the Same Server IP Address

The following example shows how to configure the network access server to recognize several RADIUS host entries with the same IP address. Two different host entries on the same RADIUS server are configured for the same services—authentication and accounting. The second host entry configured acts as failover backup to the first one. (The RADIUS host entries are tried in the order they are configured.)

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group radius
! The next set of commands configures multiple host entries for the same IP address.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 2000 acct-port 2000
```

Example: RADIUS User Profile with RADIUS Tunneling Attributes

The following example shows a RADIUS user profile (Merit Daemon format) that includes RADIUS tunneling attributes:

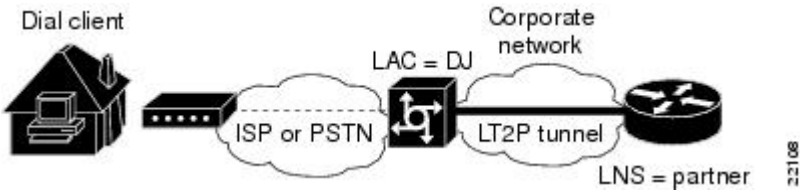
```
cisco-avpair = vpdn:l2tp-cm-local-window-size=1024
cisco-avpair = vpdn:l2tp-nosession-timeout=30
cisco-avpair = vpdn:l2tp-cm-retransmit-retries=10
cisco-avpair = vpdn:l2tp-cm-min-timeout=2
cisco-avpair = vpdn:l2tp-hello-interval=60
Service-Type = outbound
Tunnel-Assignment-Id_tag1 = ISP1
Tunnel-Client-Auth-Id_tag1 = LAC1
Tunnel-Client-Endpoint_tag1 = 10.0.0.2
Tunnel-Medium-Type_tag1 = IPv4
Tunnel-Password_tag1 = tunnel1
Tunnel-Server-Auth-Id_tag1 = LNS1
Tunnel-Server-Endpoint_tag1 = 10.0.0.1
Tunnel-Type_tag1 = l2tp
```

Examples: L2TP Access Concentrator Configuration

The following example shows a basic L2TP configuration for the L2TP access concentrator (LAC) for the topology shown in the figure below. The local name is not defined, so the hostname used is the local name.

Because the L2TP tunnel password is not defined, the username password is used. In this example, VPDN is configured locally on the LAC and does not take advantage of the new RADIUS tunnel attributes.

Figure 1: Topology for Configuration Examples




```
! Enable AAA globally.
aaa new-model
! Enable AAA authentication for PPP and list the default method to use for PPP
! authentication.
aaa authentication ppp default local
! Define the username as “DJ.”
username DJ password 7 030C5E070A00781B
! Enable VPDN.
vpdn enable
! Define VPDN group number 1.
vpdn-group 1
! Allow the LAC to respond to dialin requests using L2TP from IP address 172.21.9.13
! domain “cisco.com.”
 request dialin
  protocol l2tp
  domain cisco.com
 initiate-ip to 172.21.9.13
 local name nas-1
```

The following example shows the configuration for the LAC if RADIUS tunnel attributes are supported. In this example, there is no local VPDN configuration on the LAC; the LAC, instead, is configured to query the remote RADIUS security server.

```
! Enable global AAA securities services.
aaa new-model
! Enable AAA authentication for PPP and list RADIUS as the default method to use
! for PPP authentication.
aaa authentication ppp default group radius local
! Enable AAA (network) authorization and list RADIUS as the default method to use for
! authorization.
aaa authorization network default group radius
! Define the username as “DJ.”
username DJ password 7 030C5E070A00781B
! Enable VPDN.
vpdn enable
! Configure the LAC to interface with the remote RADIUS security server.
radius host 171.19.1.1 auth-port 1645 acct-port 1646
radius-server key cisco
```

Examples: L2TP Network Server Configuration

The following example shows a basic L2TP configuration with corresponding comments on the L2TP network server (LNS):

```
! Enable AAA globally.
aaa new-model
! Enable AAA authentication for PPP and list the default method to use for PPP
! authentication.
aaa authentication ppp default local
```

```
! Define the username as “partner.”
username partner password 7 030C5E070A00781B
! Create virtual-template 1 and assign all values for virtual access interfaces.
interface Virtual-Template1
! Borrow the IP address from loopback interface.
 ip unnumbered loopback0
! Disable multicast fast switching.
 no ip mroute-cache
! Use CHAP to authenticate PPP.
 ppp authentication chap
! Enable VPDN.
vpdn enable
! Create vpdn-group number 1.
vpdn-group 1
! Accept all dialin l2tp tunnels from virtual-template 1 from remote peer DJ.
 accept dialin l2tp virtual-template 1 remote DJ
  protocol any
  virtual-template 1
 terminate-from hostname nas1
local name hgw1
```

The following example shows how to configure the LNS with a basic L2TP configuration using RADIUS tunneling attributes:

```
aaa new-model
aaa authentication login default none
aaa authentication login console none
aaa authentication ppp default local group radius
aaa authorization network default group radius if-authenticated
!
username l2tp-svr-auth-id password 0 l2tp-tnl-pass
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
accept-dialin
protocol l2tp
virtual-template 1
terminate-from hostname l2tp-cli-auth-id
local name l2tp-svr-auth-id
!
interface GigabitEthernet1/0/0
ip address 10.0.0.3 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface Virtual-Template1
ip unnumbered loopback0
ppp authentication pap
!
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server key <deleted>
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
AAA and RADIUS commands	*Cisco IOS Security Command Reference*

Related Topic	Document Title
RADIUS attributes	*RADIUS Attributes Configuration Guide* (part of the Securing User Services Configuration Library)
AAA	*Authentication, Authorization, and Accounting Configuration Guide* (part of the Securing User Services Configuration Library)
L2TP, VPN, or VPDN	*Dial Technologies Configuration Guide* and *VPDN Configuration Guide*
Modem configuration and management	*Dial Technologies Configuration Guide*
RADIUS port identification for PPP	*Wide-Area Networking Configuration Guide*

RFCs

RFC	Title
RFC 2138	*Remote Authentication Dial-In User Service (RADIUS)*
RFC 2139	*RADIUS Accounting*
RFC 2865	*RADIUS*
RFC 2867	*RADIUS Accounting Modifications for Tunnel Protocol Support*
RFC 2868	*RADIUS Attributes for Tunnel Protocol Support*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring RADIUS

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 4: Feature Information for Configuring RADIUS

Feature Name	Releases	Feature Information
Configuring RADIUS	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.5S	The RADIUS security system is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco devices and send authentication requests to a central RADIUS server that contains all user authentication and network service access information. In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.
RADIUS Statistics via SNMP	Cisco IOS XE Release 3.2S	This feature provides statistics related to RADIUS traffic and private RADIUS servers. The following commands were introduced or modified: **show aaa servers**, **show radius statistics**.