Configuring RADIUS

Last Updated: July 04, 2011

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 routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information. RADIUS is a fully open protocol, distributed in source code format, that can be modified to work with any security system currently available.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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.

Information About RADIUS

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 router 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 Point-to-Point Protocol (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, bytes, and so on) 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 the following 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
- Router-to-router situations. RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one router to a non-Cisco router if the non-Cisco router requires RADIUS authentication.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

The following sections provide more information about RADIUS:

- RADIUS Operation, page 3
- RADIUS Attributes, page 3
- Preauthentication on a RADIUS Server, page 4
- RADIUS Authentication, page 9
- RADIUS Authorization, page 9
- RADIUS Accounting, page 9
- RADIUS Login-IP-Host, page 9
- RADIUS Prompt, page 10

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:

   a. ACCEPT--The user is authenticated.
   b. CHALLENGE--A challenge is issued by the RADIUS server. The challenge collects additional data from the user.
   c. CHANGE PASSWORD--A request is issued by the RADIUS server, asking the user to select a new password.
   d. 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 LAT, and services such as PPP, 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. For more information about RADIUS attributes, see the " RADIUS Attributes Overview and RADIUS IETF Attributes " module.

This section includes the following sections:

Vendor-Proprietary RADIUS Attributes

An IETF draft 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 IOS 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 draft 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 routers and access servers support new RADIUS IETF-standard virtual private dialup network (VPDN) tunnel attributes. For more information, see the *Cisco IOS Dial Technologies Configuration Guide* and *Cisco IOS VPDN Configuration Guide* .

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 router, you must set up the preauthentication profiles on the RADIUS server.

- RADIUS Profile for DNIS or CLID Preauthentication, page 4
- RADIUS Profile for Call Type Preauthentication, page 4
- RADIUS Profile for Preauthentication Enhancements for Callback, page 5
- RADIUS Profile for a Remote Hostname Used for Large-Scale Dial-Out, page 5
- RADIUS Profile for Modem Management, page 6
- RADIUS Profile for Subsequent Authentication, page 6
- RADIUS Profile for Subsequent Authentication Type, page 7
- RADIUS Profile to Include the Username, page 7
- RADIUS Profile for Two-Way Authentication, page 8
- RADIUS Profile to Support Authorization, page 8

RADIUS Profile for DNIS or CLID Preauthentication

To configure the RADIUS preauthentication profile, use the DNIS or 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 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 may 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 CAS.
v.110	Anything with V.110 user information layer.
v.120	Anything with 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 check-in item if the RADIUS server supports check-in 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 router by providing the name of the remote router, 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=Router2"
```

RADIUS Profile for Modem Management

When DNIS, CLID, or call type preauthentication is used, the affirmative response from the RADIUS server may include a modem string for modem management in the NAS through VSA 26. The modem management VSA has the following 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 IOS 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 and newer technologies. This feature is not supported with Microcom modems.

RADIUS Profile for Subsequent Authentication

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

Attribute 201 has the following 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, then a value of 1 is assumed, and subsequent authentication is performed.

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

RADIUS Profile for Subsequent Authentication Type

If you have 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 the following 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 username and password of Challenge-Handshake Authentication Protocol (CHAP) for PPP authentication.
ms-chap	Requires username and password of MS-CHAP for PPP authentication.
pap	Requires username and password of 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 may 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 the following 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 that has been configured (for example, if **clid** was the last preauthentication command configured, the CLID number will be 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 will need to 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 The **ppp authentication** command must be configured with the **radius** command.

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

For CHAP, “preauth:send-name” will be used not only for outbound authentication, but also for inbound authentication. For a CHAP inbound case, the NAS will use 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” will be 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, then subsequent authentication will be bypassed. Note that because the username and password are not available, authorization will also be bypassed. However, you may 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 may 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 the following 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 will not be 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 issue 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 issue the **aaa accounting** command, specifying RADIUS as the accounting method.

RADIUS Login-IP-Host

To enable the network access server 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 have been configured for the user user1>, and that TCP-Clear will be 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 network access server 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, then 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 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 (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 of the following 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. This allows 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 router or access server query the RADIUS server for static routes and IP pool definitions when the device starts up, use the **radius-server configuration-nas**command.

How to Configure RADIUS

To configure RADIUS on your Cisco router or access server, you must perform the following tasks:

- Use the **aaa new-model** global configuration command to enable 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. For more information about using the **aaa authentication** command, see the “ Configuring Authentication ” module.
- Use **line** and **interface** commands to enable the defined method lists to be used. For more information, see the “ Configuring Authentication ” module.

The following configuration tasks are optional:

- You may use the **aaa group server**command to group selected RADIUS hosts for specific services. For more information about using the **aaa group server** command, see the Configuring AAA Server Groups.
- You may use the **aaa dnis map**command to select RADIUS server groups based on Dialed Number Identification Service (DNIS) number. Before you use this command, you must define RADIUS server groups using the **aaa group server** command. For more information about using the **aaa dnis map**command, see the Configuring AAA Server Group Selection Based on DNIS.
- You may use the **aaa authorization** global configuration command to authorize specific user functions. For more information about using the **aaa authorization** command, see the “ Configuring Authorization ” module.
- You may use the **aaa accounting** command to enable accounting for RADIUS connections. For more information about using the **aaa accounting** command, see the “ Configuring Accounting ” module.
- You may use the **dialer aaa**interface configuration command to create remote site profiles that contain outgoing call attributes on the AAA server. For more information about using the **dialer aaa** command, see the Configuring the Suffix and Password in RADIUS Access Requests.

For RADIUS configuration examples using the commands in this module, refer to the section Configuration Examples for RADIUS.

- Configuring Router to RADIUS Server Communication, page 12
- Configuring a Router for Vendor-Proprietary RADIUS Server Communication, page 15
- Configuring a Router to Expand Network Access Server Port Information, page 16
- Replacing NAS-Port Attribute with RADIUS Attribute, page 18

Configuring Router to RADIUS Server Communication

The RADIUS host is normally a multiuser system running RADIUS server software from Cisco (CiscoSecure ACS), Livingston, Merit, Microsoft, or another software provider. Configuring router to RADIUS server communication can have several components:

- Hostname or IP address
- Authentication destination port
- Accounting destination port
- Timeout period
- Retransmission value
- Key string

RADIUS security servers are identified on the basis of their hostname or IP address, hostname and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service--for example, accounting--the second host entry configured acts as failover backup to the first one. If the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order they are configured.)

A RADIUS server and a Cisco router use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the router.

The timeout, retransmission, and encryption key values are configurable globally for all RADIUS servers, on a per-server basis or in some combination of global and per-server settings. To apply these settings globally to all RADIUS servers communicating with the router, use the three unique global commands: **radius-server timeout**, **radius-server retransmit**, and **radius-server key**. To apply these values on a specific RADIUS server, use the **radius-server host**command.

Note You can configure both global and per-server timeout, retransmission, and key value commands simultaneously on the same Cisco network access server. If both global and per-server functions are configured on a router, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands.

To configure router to server RADIUS server communication, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string]* [**alias** {*hostname* | *ip-address*}]
4. **radius-server key** {**0** *string* | **7** *string* | *string*}
5. **radius-server retransmit** *retries*
6. **radius-server timeout** *seconds*
7. **radius-server deadtime** *minutes*
8. **exit**

DETAILED STEPS

	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.

	Command or Action	Purpose
Step 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string]* [**alias** {*hostname* | *ip-address*}] **Example:** `Router(config)# radius-server host 10.45.1.2`	Specifies the IP address or hostname of the remote RADIUS server host and assigns authentication and accounting destination port numbers. **Note** In this step, the timeout, retransmission, and encryption key values are configure on a per-server basis. • Use the **auth-port** *port-number* keyword-argument pair to configure a specific UDP port on this RADIUS server to be used solely for authentication. • Use the **acct-port** *port-number* keyword-argument pair to configure a specific UDP port on this RADIUS server to be used solely for accounting. • Use the **alias** keyword to configure up to eight multiple IP addresses for use when referring to RADIUS servers. • To configure the network access server to recognize more than one host entry associated with a single IP address, repeat this command as many times as necessary, making sure that each UDP port number is different. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host. • If no timeout is set, the global value is used; otherwise, enter a value in the range from 1 to 1000. If no retransmit value is set, the global value is used; otherwise, enter a value in the range from 1 to 1000. If no key string is specified, the global value is used. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host**command syntax because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Step 4	**radius-server key** {**0** *string* | **7** *string* | *string*}
	Example:
	`Router(config)# radius-server key myRaDIUSpassword`
		Specifies the shared secret text string used between the router and a RADIUS server.
		Note In this step, the encryption key value is configured globally for all RADIUS servers.
		• Use the **0** *string* option to configure an unencrypted shared secret. Use the **7** *string* option to configure an encrypted shared secret.

Step 5	**radius-server retransmit** *retries* **Example:** `Router(config)# radius-server retransmit 25`	Specifies how many times the router transmits each RADIUS request to the server before giving up (the default is 3). **Note** In this step, the retransmission value is configured globally for all RADIUS servers.

	Command or Action	Purpose
Step 6	**radius-server timeout** *seconds* **Example:** `Router(config)# radius-server timeout 6`	Specifies for how many seconds a router waits for a reply to a RADIUS request before retransmitting the request. **Note** In this step, the timeout value is configured globally for all RADIUS servers.
Step 7	**radius-server deadtime** *minutes* **Example:** `Router(config)# radius-server deadtime 5`	Specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication.
Step 8	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.

Configuring a Router for Vendor-Proprietary RADIUS Server Communication

Although an IETF draft 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 IOS software supports a subset of vendor-proprietary RADIUS attributes.

To configure RADIUS (whether vendor-proprietary or IETF draft-compliant), you must specify the host running the RADIUS server daemon and the secret text string it shares with the Cisco device. You must specify the RADIUS host and secret text string by using the **radius-server** commands. 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 will not be supported unless you use the **radius-server host non-standard**command.

To configure a router for vendor-proprietary RADIUS server communication, perform the following task.

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:** `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	**radius-server vsa send** [**accounting** | **authentication**] **Example:** `Router(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:** `Router(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.

Step 5	**radius-server key** {**0** *string* | **7** *string* | *string*}
	Example:
	`Router(config)# radius-server key myRaDIUSpassword`
		Specifies the shared secret text string used between the router and the vendor-proprietary RADIUS server.
		• The router and the RADIUS server use this text string to encrypt passwords and exchange responses.

Step 6	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.

Configuring a Router to Expand Network Access Server Port Information

There are some situations when 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.

To configure a router to expand the NAS-Port information, perform the following task.

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:** `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	**radius-server configure-nas** **Example:** `Router(config)# radius-server configure-nas`	(Optional) Tells the Cisco router 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 router starts up, it will not take effect until you issue a **copy system:running config nvram:startup-config**command.
Step 4	**radius-server attribute nas-port format** **Example:** `Router(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.

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

Replacing NAS-Port Attribute with RADIUS Attribute

On platforms with multiple interfaces (ports) per slot, the Cisco RADIUS implementation will 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 will appear as NAS-Port = 20101. This is because of the 16-bit field size limitation associated with RADIUS IETF NAS-Port attribute. In this case, 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) will be 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 will no longer be sent.

To replace the NAS-Port attribute with RADIUS IETF attribute 26 and to display extended field information, perform the following task.

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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**radius-server vsa send** [**accounting** | **authentication**] **Example:** `Router(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:** `Router(config)# aaa nas port extended`	Expands the size of the VSA NAS-Port field from 16 to 32 bits to display extended interface information.
Step 5	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.

Configuring AAA Server Groups

Configuring the router to use AAA server groups provides a way to group existing server hosts. This allows you to select a subset of the configured server hosts and use them for a particular service. A server group is used in conjunction with a global server-host list. The server group lists the IP addresses of the selected server hosts.

Server groups can also include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service--for example, accounting--the second host entry that is configured acts as failover backup to the first one. If the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order in which they are configured.)

To define a server host with a server group name, enter the following commands in global configuration mode. The listed server must exist in global configuration mode.

Each server in the group must be defined previously using the **radius-server host** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}]
4. **aaa group server** {**radius** | **tacacs+**} *group-name*
5. **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
6. **end**

DETAILED STEPS

	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	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] **Example:** `Router(config)# radius-server host 10.45.1.2`	Specifies and defines the IP address of the server host before configuring the AAA server group.
Step 4	**aaa group server** {**radius** | **tacacs+**} *group-name* **Example:** `Router(config)# aaa group server radius group1`	Defines the AAA server group with a group name. • All members of a group must be the same type, that is, RADIUS or TACACS+. This command puts the router in server group configuration mode.
Step 5	**server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] **Example:** `Router(config-sg-radius)# server 172.16.1.1 acct-port 1616`	Associates a particular RADIUS server with the defined server group. • Each security server is identified by its IP address and UDP port number. • Repeat this step for each RADIUS server in the AAA server group.

	Command or Action	Purpose

Step 6	**end**
	Example:
	`Router(config-sg-radius)# end`
		Exits server group configuration mode and returns to privileged EXEC mode.

Configuring AAA Server Groups with Deadtime

After you have configured a server host with a server name, you can use the **deadtime** command to configure each server per server group. Configuring deadtime within a server group allows you to direct AAA traffic to separate groups of servers that have different operational characteristics.

Configuring deadtime is not limited to a global configuration. A separate timer is attached to each server host in every server group. Therefore, when a server is found to be unresponsive after numerous retransmissions and timeouts, the server is assumed to be dead. The timers attached to each server host in all server groups are triggered. In essence, the timers are checked and subsequent requests to a server (once it is assumed to be dead) are directed to alternate timers, if configured. When the network access server receives a reply from the server, it checks and stops all configured timers (if running) for that server in all server groups.

If the timer has expired, the server to which the timer is attached is assumed to be alive. This becomes the only server that can be tried for later AAA requests using the server groups to which the timer belongs.

Note Because one server has different timers and may have different deadtime values configured in the server groups, the same server may, in the future, have different states (dead and alive) at the same time.

Note To change the state of a server, you must start and stop all configured timers in all server groups.

The size of the server group will be slightly increased because of the addition of new timers and the deadtime attribute. The overall impact of the structure depends on the number and size of the server groups and how the servers are shared among server groups in a specific configuration.

To configure deadtime within a AAA server group, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *group*
4. **deadtime** *minutes*
5. **end**

DETAILED STEPS

	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 group server radius** *group* **Example:** `Router(config)# aaa group server radius group1`	Defines a RADIUS type server group and enters server group configuration mode.
Step 4	**deadtime** *minutes* **Example:** `Router(config-sg-radius)# deadtime 1`	Configures and defines deadtime value in minutes. **Note** Local server group deadtime will override the global configuration. If omitted from the local server group configuration, the deadtime value will be inherited from the master list.

Step 5	**end**
	Example:
	`Router(config-sg-radius)# end`
		Exits server group configuration mode and returns to privileged EXEC mode.

Configuring AAA DNIS Preauthentication

DNIS preauthentication enables preauthentication at call setup based on the number dialed. The DNIS number is sent directly to the security server when a call is received. If authenticated by AAA, the call is accepted.

To configure DNIS preauthentication, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa preauthorization**
4. **group** {**radius** | **tacacs+** | *server-group*}
5. **dnis** [**password** *string*]
6. **end**

DETAILED STEPS

	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 preauthorization** **Example:** `Router(config)# aaa preauthorization`	Enters AAA preauthentication configuration mode.

Step 4	**group** {**radius** | **tacacs+** | *server-group*}
	Example:
	`Router(config-preauth)# group radius`
		(Optional) Selects the security server to use for AAA preauthentication requests.
		• The default is RADIUS.

Step 5	**dnis** [**password** *string*]
	Example:
	`Router`
	`(config-preauth)# dnis password dnispass`
		Enables preauthentication using DNIS and optionally specifies a password to use in Access-Request packets.

	Command or Action	Purpose

Step 6	**end**
	Example:
	`Router(config-preauth)# end`
		Exits AAA preauthentication configuration mode and returns to privileged EXEC mode.

Configuring AAA Server Group Selection Based on DNIS

Cisco IOS software allows you to assign a DNIS number to a particular AAA server group so that the server group can process authentication, authorization, and accounting requests for users dialing in to the network using that particular DNIS. Any phone line (a regular home phone or a commercial T1/PRI line) can be associated with several phone numbers. The DNIS number identifies the number that was called to reach you.

For example, suppose you want to share the same phone number with several customers, but you want to know which customer is calling before you pick up the phone. You can customize how you answer the phone because DNIS allows you to know which customer is calling when you answer.

Cisco routers with either ISDN or internal modems can receive the DNIS number. This functionality allows users to assign different RADIUS server groups for different customers (that is, different RADIUS servers for different DNIS numbers). Additionally, using server groups, you can specify the same server group for AAA services or a separate server group for each AAA service.

Cisco IOS software provides the flexibility to implement authentication and accounting services in several ways:

- Globally--AAA services are defined using global configuration access list commands and applied in general to all interfaces on a specific network access server.
- Per interface--AAA services are defined using interface configuration commands and applied specifically to the interface being configured on a specific network access server.
- DNIS mapping--You can use DNIS to specify an AAA server to supply AAA services.

Because each of these AAA configuration methods can be configured simultaneously, Cisco has established an order of precedence to determine which server or groups of servers provide AAA services. The order of precedence is as follows:

- Per DNIS--If you configure the network access server to use DNIS to identify or determine which server group provides AAA services, then this method takes precedence over any additional AAA selection method.
- Per interface--If you configure the network access server per interface to use access lists to determine how a server provides AAA services, this method takes precedence over any global configuration AAA access lists.
- Globally--If you configure the network access server by using global AAA access lists to determine how the security server provides AAA services, this method has the least precedence.

Note Prior to configuring the AAA Server Group Selection Based on DNIS feature, you must configure the list of RADIUS server hosts and AAA server groups. See the sections Configuring Router to RADIUS Server Communication, page 12 and Configuring AAA Server Groups, page 19.

To configure the router to select a particular AAA server group based on the DNIS of the server group, configure DNIS mapping. To map a server group with a group name with DNIS number, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa dnis map enable**
4. **aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name*
5. **aaa dnis map** *dnis-number* **authorization network group** *server-group-name*
6. **aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name*
7. **exit**

DETAILED STEPS

	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 dnis map enable** **Example:** `Router(config)# aaa dnis map enable`	Enables DNIS mapping.

	Command or Action	Purpose
Step 4	**aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name* **Example:** `Router(config)# aaa dnis map 7777 authentication ppp group sg1`	Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for authentication.
Step 5	**aaa dnis map** *dnis-number* **authorization network group** *server-group-name* **Example:** `Router(config)# aaa dnis map 7777 authorization network group sg1`	Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for authorization.
Step 6	**aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name* **Example:** `Router(config)# aaa dnis map 8888 accounting network stop-only group sg2`	Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for accounting.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring AAA Preauthentication

Configuring AAA preauthentication with ISDN PRI or channel-associated signaling (CAS) allows service providers to better manage ports using their existing RADIUS solutions and efficiently manage the use of shared resources to offer differing service-level agreements. With ISDN PRI or CAS, information about an incoming call is available to the network access server (NAS) before the call is connected. The available call information includes the following:

- The DNIS number, also referred to as the called number
- The Calling Line Identification (CLID) number, also referred to as the calling number
- The call type, also referred to as the bearer capability

The AAA preauthentication feature allows a Cisco NAS to decide--on the basis of the DNIS number, the CLID number, or the call type--whether to connect an incoming call. (With ISDN PRI, it enables user authentication and authorization before a call is answered. With CAS, the call must be answered; however, the call can be dropped if preauthentication fails.)

When an incoming call arrives from the public network switch, but before it is connected, AAA preauthentication enables the NAS to send the DNIS number, CLID number, and call type to a RADIUS server for authorization. If the server authorizes the call, then the NAS accepts the call. If the server does not authorize the call, then the NAS sends a disconnect message to the public network switch to reject the call.

In the event that the RADIUS server application becomes unavailable or is slow to respond, a guard timer can be set in the NAS. When the timer expires, the NAS uses a configurable parameter to accept or reject the incoming call that has no authorization.

The AAA preauthentication feature supports the use of attribute 44 by the RADIUS server application and the use of RADIUS attributes that are configured in the RADIUS preauthentication profiles to specify preauthentication behavior. They may also be used, for instance, to specify whether subsequent authentication should occur and, if so, what authentication method should be used.

The following restrictions apply to AAA preauthentication with ISDN PRI and CAS:

- Attribute 44 is available for CAS calls only when preauthentication or resource pooling is enabled.
- Multichassis Multilink PPP (MMP) is not available with ISDN PRI.
- AAA preauthentication is available only on the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

Note Prior to configuring AAA preauthentication, you must enable the **aaa new-model** command and make sure that the supporting preauthentication application is running on a RADIUS server in your network.

To configure AAA preauthentication, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa preauthorization**
4. **group** *server-group*
5. **clid** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]
6. **ctype** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]
7. **dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]
8. **dnis bypass** *dnis-group-name*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa preauthorization** **Example:** `Router(config)# aaa preauthorization`	Enters AAA preauthentication configuration mode.
Step 4	**group** *server-group* **Example:** `Router(config-preauth)# group sg2`	Specifies the AAA RADIUS server group to use for preauthentication.
Step 5	**clid** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] **Example:** `Router(config-preauth)# clid required`	Preauthenticates calls on the basis of the CLID number.
Step 6	**ctype** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] **Example:** `Router(config-preauth)# ctype required`	Preauthenticates calls on the basis of the call type.
Step 7	**dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] **Example:** `Router(config-preauth)# dnis required`	Preauthenticates calls on the basis of the DNIS number.
Step 8	**dnis bypass** *dnis-group-name* **Example:** `Router(config-preauth)# dnis bypass group1`	Specifies a group of DNIS numbers that will be bypassed for preauthentication.

	Command or Action	Purpose

Step 9	**end**
	Example:
	`Router(config-preauth)# end`
		Exits preauthentication configuration mode and returns to privileged EXEC mode.

Configuring DNIS Preauthentication

To configure DNIS preauthentication, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa preauthorization**
4. **group** {**radius** | **tacacs+** | *server-group*}
5. **dnis** [**password** *string*]
6. **end**

DETAILED STEPS

	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 preauthorization** **Example:** `Router(config)# aaa preauthorization`	Enters AAA preauthentication mode.

	Command or Action	Purpose

Step 4	**group** {**radius** | **tacacs+** | *server-group*}
	Example:
	`Router`
	`(config-preauth)# group radius`
		(Optional) Selects the security server to use for AAA preauthentication requests.
		• The default is RADIUS.

Step 5	**dnis** [**password** *string*] **Example:** `Router(config-preauth)# dnis password dnispass`	Enables preauthentication using DNIS and optionally specifies a password to use in Access-Request packets.

Step 6	**end**
	Example:
	`Router(config-preauth)# end`
		Exits AAA preauthentication configuration mode and returns to privileged EXEC mode.

Configuring a Guard Timer

Because response times for preauthentication and authentication requests can vary, the guard timer allows you to control the handling of calls. The guard timer starts when the DNIS is sent to the RADIUS server. If the NAS does not receive a response from AAA before the guard timer expires, it accepts or rejects the calls on the basis of the configuration of the timer.

To set a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to an authentication or preauthentication request, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **isdn guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}]
5. **call guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}]
6. **end**

DETAILED STEPS

	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* **Example:** `Router(config)# interface serial 1/0/0:23`	Enters interface configuration mode.
Step 4	**isdn guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}] **Example:** `Router(config-if)# isdn guard-timer 8000 on-expiry reject`	Sets an ISDN guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request.
Step 5	**call guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}] **Example:** `Router(config-if)# call guard-timer 2000 on-expiry accept`	Sets a CAS guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request.

Step 6	**end**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode and 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.

To provide username configuration capability for large-scale dial-out, the **dialer aaa**command is implemented with the new **suffix** and **password** keywords.

To configure the suffix and password in RADIUS access requests, perform the following task.

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:** `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 the AAA access control model.
Step 4	**aaa route download** *time* **Example:** `Router(config)# aaa route download 450`	Enables the download static route feature and sets the amount of time between downloads.

	Command or Action	Purpose
Step 5	**aaa authorization configuration default** **Example:** `Router(config)# aaa authorization configuration default`	Downloads static route configuration information from the AAA server using TACACS+ or RADIUS.
Step 6	**interface dialer** *number* **Example:** `Router(config)# interface dialer 1`	Defines a dialer rotary group and enters interface configuration mode.
Step 7	**dialer aaa** **Example:** `Router(config-if)# dialer aaa`	Allows a dialer to access the AAA server for dialing information.
Step 8	**dialer aaa suffix** *suffix* **password** *password* **Example:** `Router(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:** `Router(config-if)# exit`	Exits interface configuration mode and returns to privileged EXEC mode.

Monitoring and Maintaining RADIUS

To monitor and maintain RADIUS, use the following commands.

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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug radius** **Example:** `Router# debug radius`	Displays information associated with RADIUS.
Step 3	**show radius statistics** **Example:** `Router# show radius statistics`	Displays the RADIUS statistics for accounting and authentication packets.
Step 4	**show aaa servers** **Example:** `Router# 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:** `Router# exit`	Exits the router session.

Configuration Examples for RADIUS

Example RADIUS Authentication and Authorization

The following example shows how to configure the router 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 router 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 IOS 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 will be 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:

```
radius-server host host1 non-standard
radius-server key myRaDiUSpassWoRd
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
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 RADIUS authentication, authorization, and accounting configuration example are defined as follows:

- The **radius-server host 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 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 router or access server will query 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 will be 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 RADIUS Server with Server-Specific Values

The following example shows how to configure server-specific timeout, retransmit, and key values for the RADIUS server with IP address 172.31.39.46:

```
radius-server host 172.31.39.46 timeout 6 retransmit 5 key rad123
```

Example Multiple RADIUS Servers with Global and Server-Specific Values

The following example shows how to configure two RADIUS servers with specific timeout, retransmit, and key values. In this example, the **aaa new-model** command enables AAA services on the router, and specific AAA commands define the AAA services. The **radius-server retransmit** command changes the global retransmission value to 4 for all RADIUS servers. The **radius-server host** command configures specific timeout, retransmission, and key values for the RADIUS server hosts with IP addresses 172.16.1.1 and 172.29.39.46.

```
! Enable AAA services on the router and define those services.
aaa new-model
aaa authentication login default group radius
aaa authentication login console-login none
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
enable password tryit1
!
! Change the global retransmission value for all RADIUS servers.
radius-server retransmit 4
!
! Configure per-server specific timeout, retransmission, and key values.
! Change the default auth-port and acct-port values.
radius-server host 172.16.1.1 auth-port 1612 acct-port 1616 timeout 3 retransmit 3 key
radkey
!
! Configure per-server specific timeout and key values. This server uses the global
! retransmission value.
radius-server host 172.29.39.46 timeout 6 key rad123
```

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 will be 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 Server Group

The following example shows how to create server group radgroup1 with three different RADIUS server members, each using the default authentication port (1645) and accounting port (1646):

```
aaa group server radius radgroup1
```

```
 server 172.16.1.11
 server 172.17.1.21
 server 172.18.1.31
```

The following example shows how to create server group radgroup2 with three RADIUS server members, each with the same IP address but with unique authentication and accounting ports:

```
aaa group server radius radgroup2
 server 172.16.1.1 auth-port 1000 acct-port 1001
 server 172.16.1.1 auth-port 2000 acct-port 2001
 server 172.16.1.1 auth-port 3000 acct-port 3001
```

Example Multiple RADIUS Server Entries Using AAA Server Groups

The following example shows how to configure the network access server to recognize two different RADIUS server groups. One of these groups, group1, has two different host entries on the same RADIUS server configured for the same services. The second host entry configured acts as failover backup to the first one. Each group is individually configured for deadtime; deadtime for group 1 is one minute, and deadtime for group 2 is two minutes.

Note In cases where both global commands and server commands are used, the server command will take precedence over the global command.

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group group1
! The following commands define the group1 RADIUS server group and associate servers
! with it and configures a deadtime of one minute.
aaa group server radius group1
 server 10.1.1.1 auth-port 1645 acct-port 1646
 server 10.2.2.2 auth-port 2000 acct-port 2001
 deadtime 1
! The following commands define the group2 RADIUS server group and associate servers
! with it and configures a deadtime of two minutes.
aaa group server radius group2
 server 10.2.2.2 auth-port 2000 acct-port 2001
 server 10.3.3.3 auth-port 1645 acct-port 1646
 deadtime 2
! The following set of commands configures the RADIUS attributes for each host entry
! associated with one of the defined server groups.
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server host 10.2.2.2 auth-port 2000 acct-port 2001
radius-server host 10.3.3.3 auth-port 1645 acct-port 1646
```

Example AAA Server Group Selection Based on DNIS

The following example shows how to select RADIUS server groups based on DNIS to provide specific AAA services:

```
! This command enables AAA.
aaa new-model
!
! The following set of commands configures the RADIUS attributes for each server
! that will be associated with one of the defined server groups.
radius-server host 172.16.0.1 auth-port 1645 acct-port 1646 key cisco1
radius-server host 172.17.0.1 auth-port 1645 acct-port 1646 key cisco2
radius-server host 172.18.0.1 auth-port 1645 acct-port 1646 key cisco3
radius-server host 172.19.0.1 auth-port 1645 acct-port 1646 key cisco4
radius-server host 172.20.0.1 auth-port 1645 acct-port 1646 key cisco5
! The following commands define the sg1 RADIUS server group and associate servers
! with it.
aaa group server radius sg1
  server 172.16.0.1
  server 172.17.0.1
! The following commands define the sg2 RADIUS server group and associate a server
! with it.
aaa group server radius sg2
  server 172.18.0.1
! The following commands define the sg3 RADIUS server group and associate a server
! with it.
aaa group server radius sg3
  server 172.19.0.1
! The following commands define the default-group RADIUS server group and associate
! a server with it.
aaa group server radius default-group
  server 172.20.0.1
! The next set of commands configures default-group RADIUS server group parameters.
aaa authentication ppp default group default-group
aaa accounting network default start-stop group default-group
!
! The next set of commands enables DNIS mapping and maps DNIS numbers to the defined
! RADIUS server groups. In this configuration, all PPP connection requests using
! DNIS 7777 are sent to the sg1 server group. The accounting records for these
! connections (specifically, start-stop records) are handled by the sg2 server group.
! Calls with a DNIS of 8888 use server group sg3 for authentication and server group
! default-group for accounting. Calls with a DNIS of 9999 use server group
! default-group for authentication and server group sg3 for accounting records
! (stop records only). All other calls with DNIS other than the ones defined use the
! server group default-group for both authentication and stop-start accounting records.
aaa dnis map enable
aaa dnis map 7777 authentication ppp group sg1
aaa dnis map 7777 accounting network start-stop group sg2
aaa dnis map 8888 authentication ppp group sg3
aaa dnis map 9999 accounting network stop-only group sg3
```

Example AAA Preauthentication

The following is a simple configuration that specifies that the DNIS number be used for preauthentication:

```
aaa preauthentication
 group radius
 dnis required
```

The following example shows a configuration that specifies that both the DNIS number and the CLID number be used for preauthentication. DNIS preauthentication will be performed first, followed by CLID preauthentication.

```
aaa preauthentication
 group radius
 dnis required
 clid required
```

The following example specifies that preauthentication be performed on all DNIS numbers except the two DNIS numbers specified in the DNIS group called “dnis-group1”:

```
aaa preauthentication
 group radius
 dnis required
 dnis bypass dnis-group1
dialer dnis group dnis-group1
 number 12345
 number 12346
```

The following is a sample AAA configuration with DNIS preauthentication:

```
aaa new-model
aaa authentication login CONSOLE none
aaa authentication login RADIUS_LIST group radius
aaa authentication login TAC_PLUS group tacacs+ enable
aaa authentication login V.120 none
aaa authentication enable default enable group tacacs+
aaa authentication ppp RADIUS_LIST if-needed group radius
aaa authorization exec RADIUS_LIST group radius if-authenticated
aaa authorization exec V.120 none
aaa authorization network default group radius if-authenticated
aaa authorization network RADIUS_LIST if-authenticated group radius
aaa authorization network V.120 group radius if-authenticated
aaa accounting suppress null-username
aaa accounting exec default start-stop group radius
aaa accounting commands 0 default start-stop group radius
aaa accounting network default start-stop group radius
aaa accounting connection default start-stop group radius
aaa accounting system default start-stop group radius
aaa preauthentication
 dnis password Cisco-DNIS
aaa nas port extended
!
radius-server configure-nas
radius-server host 10.0.0.0 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.255.255.255 auth-port 1645 acct-port 1646 non-standard
radius-server retransmit 2
radius-server deadtime 1
radius-server attribute nas-port format c
radius-server unique-ident 18
radius-server key MyKey
```

Note To configure preauthentication, you must also set up preauthentication profiles on the RADIUS server.

Example RADIUS User Profile with RADIUS Tunneling Attributes

The following example shows a RADIUS user profile (Merit Daemon format) that includes RADIUS tunneling attributes. This entry supports two tunnels, one for L2F and the other for L2TP. The tag entries with :1 support L2F tunnels, and the tag entries with :2 support L2TP tunnels.

```
cisco.com Password = "PASSWORD3", Service-Type = Outbound
Service-Type = Outbound,
Tunnel-Type = :1:L2F,
Tunnel-Medium-Type = :1:IP,
Tunnel-Client-Endpoint = :1:"10.0.0.2",
Tunnel-Server-Endpoint = :1:"10.0.0.3",
Tunnel-Client-Auth-Id = :1:"l2f-cli-auth-id",
Tunnel-Server-Auth-Id = :1:"l2f-svr-auth-id",
Tunnel-Assignment-Id = :1:"l2f-assignment-id",
Cisco-Avpair = "vpdn:nas-password=l2f-cli-pass",
Cisco-Avpair = "vpdn:gw-password=l2f-svr-pass",
Tunnel-Preference = :1:1,
Tunnel-Type = :2:L2TP,
Tunnel-Medium-Type = :2:IP,
Tunnel-Client-Endpoint = :2:"10.0.0.2",
Tunnel-Server-Endpoint = :2:"10.0.0.3",
Tunnel-Client-Auth-Id = :2:"l2tp-cli-auth-id",
Tunnel-Server-Auth-Id = :2:"l2tp-svr-auth-id",
Tunnel-Assignment-Id = :2:"l2tp-assignment-id",
Cisco-Avpair = "vpdn:l2tp-tunnel-password=l2tp-tnl-pass",
Tunnel-Preference = :2:2
```

Example Guard Timer

The following example shows an ISDN guard timer that is set at 8000 milliseconds. A call will be rejected if the RADIUS server has not responded to a preauthentication request when the timer expires.

```
interface serial 1/0/0:23
```

```
 isdn guard-timer 8000 on-expiry reject
aaa preauthentication
 group radius
 dnis required
```

The following example shows a CAS guard timer that is set at 20,000 milliseconds. A call will be accepted if the RADIUS server has not responded to a preauthentication request when the timer expires.

```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
 cas-custom 0
 call guard-timer 20000 on-expiry accept
aaa preauthentication
group radius
dnis required
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
AAA and RADIUS commands	*Cisco IOS Security Command Reference*
RADIUS attributes	“ RADIUS Attributes Overview and RADIUS IETF Attributes ” module
AAA	• “Configuring Authentication” module • “Configuring Authorization” module • “Configuring Accounting” module
L2F, L2TP, VPN, or VPDN	*Cisco IOS Dial Technologies Configuration Guide* and *Cisco IOS VPDN Configuration Guide*
Modem configuration and management	*Cisco IOS Dial Technologies Configuration Guide*
RADIUS port identification for PPP	*Cisco IOS Wide-Area Networking Configuration Guide*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2139	*RADIUS Accounting*
RFC 2865	*Remote Authentication Dial-In User Service (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	11.1	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 routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information. RADIUS is a fully open protocol, distributed in source code format, that can be modified to work with any security system currently available. This feature was introduced in Cisco IOS Release 11.1.
Radius Statistics via SNMP	15.1(1)S 15.1(4)M	This feature provides statistics related to RADIUS traffic and private radius servers. The following commands were modified: **show aaa servers**, **show radius statistics**.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.