



Configuring RADIUS or a Local Authenticator in a Wireless LAN

This module describes how to enable and configure RADIUS in a wireless LAN (WLAN), which is a protocol that provides detailed accounting information and flexible administrative control over the authentication and authorization processes. RADIUS is facilitated through authentication, authorization, and accounting (AAA) and can be enabled only through AAA commands.

This module also describes how to configure a Cisco 800, 1800, 2800, or 3800 series integrated services router, hereafter referred to as an access point or AP, as a local authenticator. The AP can serve as a standalone authenticator for a small wireless LAN or provide backup authentication service. As a local authenticator, an AP performs Lightweight Extensible Authentication Protocol (LEAP) and MAC-based authentication for up to 50 client devices.

You can configure your APs to use the local authenticator when they cannot reach the main servers, or you can configure your APs to use the local authenticator or as the main authenticator if you do not have a RADIUS server. When you configure the local authenticator as a backup to your main servers, the APs periodically check the link to the main servers and stop using the local authenticator automatically when the link to the main servers is restored.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Configuring RADIUS or a Local Authenticator in a Wireless LAN”](#) section on page 28.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Contents

- [Prerequisites for Configuring RADIUS or a Local Authenticator in a Wireless LAN, page 2](#)
- [Information About Configuring RADIUS or a Local Authenticator in a Wireless LAN, page 2](#)
- [How to Configure RADIUS or a Local Authenticator in a Wireless LAN, page 5](#)
- [Configuration Examples for a RADIUS Server or a Local Authenticator in a Wireless LAN, page 26](#)
- [Additional References, page 27](#)
- [Feature Information for Configuring RADIUS or a Local Authenticator in a Wireless LAN, page 28](#)

Prerequisites for Configuring RADIUS or a Local Authenticator in a Wireless LAN

The following prerequisites apply to configuring RADIUS or a local authenticator in a wireless LAN:

- Read the “Wireless LAN Overview” module.
- Read the “Configuring a Basic Wireless LAN Connection” module.

Information About Configuring RADIUS or a Local Authenticator in a Wireless LAN

Before you configure a RADIUS server or local authenticator in a wireless LAN, you should understand the following concepts:

- [Network Environments Recommended to Use RADIUS for Access Security in a Wireless LAN, page 2](#)
- [RADIUS Operation in a Wireless LAN, page 3](#)
- [Local Authentication in a Wireless LAN, page 4](#)
- [Configuration Overview for a Local Authenticator in a Wireless LAN, page 5](#)

Network Environments Recommended to Use RADIUS for Access Security in a Wireless LAN

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

is normally a multiuser system running RADIUS server software from Cisco (Cisco Secure Access Control Server version 3.0), Livingston, Merit, Microsoft, or another software provider. For more information, refer to the RADIUS server documentation.

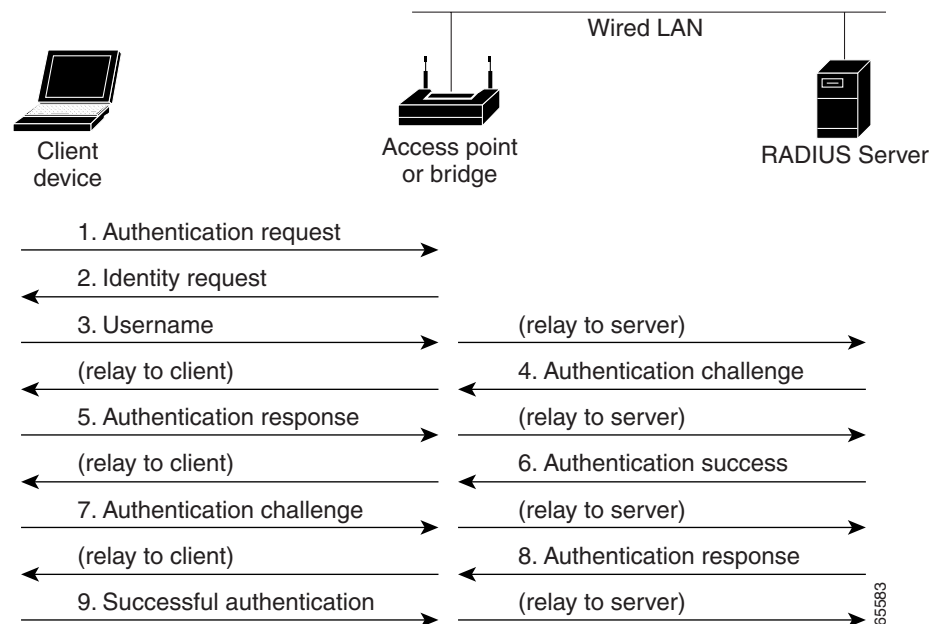
Use RADIUS in these network environments, which require access security:

- 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 is customized to work with the Kerberos security system.
- Turnkey network security environments in which applications support the RADIUS protocol, such as 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 to grant access to network resources.
- Networks already using RADIUS. You can add a Cisco AP containing a RADIUS client to the network.
- Networks that require resource accounting. You can use RADIUS accounting independently of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, showing the amount of resources (such as time, packets, bytes, and so forth) used during the session. An Internet service provider might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

RADIUS Operation in a Wireless LAN

When a wireless user attempts to log in and authenticate to an AP whose access is controlled by a RADIUS server, authentication to the network occurs in the steps shown in [Figure 8](#).

Figure 8 Sequence for EAP Authentication



In Steps 1 through 9 in [Figure 8](#), a wireless client device and a RADIUS server on the wired LAN use 802.1x and Extensible Authentication Protocol (EAP) to perform a mutual authentication through the AP. The RADIUS server sends an authentication challenge to the client. The client uses a one-way

encryption of the user-supplied password to generate a response to the challenge and sends that response to the RADIUS server. Using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. When the RADIUS server authenticates the client, the process repeats in reverse, and the client authenticates the RADIUS server.

When mutual authentication is complete, the RADIUS server and the client determine a Wired Equivalent Privacy (WEP) key that is unique to the client and provides the client with the appropriate level of network access, thereby approximating the level of security in a wired switched segment to an individual desktop. The client loads this key and prepares to use it for the login session.

During the login session, the RADIUS server encrypts and sends the WEP key, called a *session key*, over the wired LAN to the AP. The AP encrypts its broadcast key with the session key and sends the encrypted broadcast key to the client, which uses the session key to decrypt it. The client and AP activate WEP and use the session and broadcast WEP keys for all communications during the remainder of the session.

There is more than one type of EAP authentication, but the AP behaves the same way for each type: It relays authentication messages from the wireless client device to the RADIUS server and from the RADIUS server to the wireless client device. See the “[Separating a Wireless Network by Configuring Multiple SSIDs](#)” section in the “[Securing a Wireless LAN](#)” module for instructions on setting up client authentication using a RADIUS server.

Local Authentication in a Wireless LAN

To provide local authentication service or backup authentication service in case of a WAN link or a server failure, you can configure an AP to act as a local authentication server. The AP can authenticate clients using LEAP or MAC-based authentication.

The Cisco 800, 1800, 1841, and 2801 series APs can locally authenticate up to 50 clients, the Cisco 2811 and 2821 APs can authenticate up to 100 clients, the Cisco 2851 AP can authenticate up to 200 clients, the Cisco 3825 AP can authenticate up to 500 clients, and the Cisco 3845 AP can locally authenticate up to 1000 clients. The AP performs up to 5 authentications per second.

Small wireless LANs that do not have access to a RADIUS server could be made more secure with 802.1x authentication. Also, on wireless LANs that use 802.1x authentication, the APs rely on RADIUS servers housed at a distant location to authenticate client devices and the authentication traffic must cross a WAN link. If the WAN link fails or the APs cannot access the RADIUS servers for any other reason, client devices cannot access the wireless network even if the work they want to do is entirely local and typically authorized.

Configuration of authentication on a local authenticator must be done manually with client usernames and passwords. The local authenticator does not synchronize its database with the RADIUS servers. Also, a VLAN and a list of SSIDs that a client is allowed to use can be configured.



Note

If your wireless LAN contains only one AP, you can configure the AP as both the 802.1x authenticator and the local authenticator. However, users associated to the local authenticator might notice a decrease in performance during the authentication process.

You can configure your APs to use the local authenticator when they cannot reach the main servers, or you can configure your APs to use the local authenticator or as the main authenticator if you do not have a RADIUS server. When you configure the local authenticator as a backup to your main servers, the APs periodically check the link to the main servers and stop using the local authenticator automatically when the link to the main servers is restored.

**Note**

The AP you use as an authenticator contains detailed authentication information for your wireless LAN. Physically secure it to protect its configuration.

Configuration Overview for a Local Authenticator in a Wireless LAN

These are the typical steps you will follow to set up a local authenticator. The task is fully described in the “[Configuring Local or Backup Authentication Service](#)” section.

1. On the local authenticator, create a list of APs authorized to use the authenticator to authenticate client devices. Each AP that uses the local authenticator is a network access server (NAS). If the local authenticator AP serves client devices directly, include the local authenticator AP as a NAS.
2. Create user groups and configure parameters to be applied to each group (optional).
3. Create a list of up to 1000 LEAP users or MAC addresses that the local authenticator is authorized to authenticate; the number of authorized users depends on the model of the AP. Verify the limit of your AP before creating the list.

You do not have to specify which type of authentication you want the local authenticator to perform. It automatically performs LEAP or MAC-address authentication for the users in its user database.

4. On the client APs that use a local authenticator AP for security, enter the local authenticator as a RADIUS server. If your local authenticator AP also serves client devices, you must enter the local authenticator as a RADIUS server in the local authenticator configuration. When a client associates to the local authenticator AP, the AP uses itself to authenticate the client.

How to Configure RADIUS or a Local Authenticator in a Wireless LAN

This section describes how to configure RADIUS or a local authenticator in a wireless LAN.

How to Configure RADIUS in a Wireless LAN

This section describes how to configure RADIUS in a wireless LAN.

At a minimum, you must identify the host or hosts that run the RADIUS server software and define the method lists for RADIUS authentication. You can optionally define method lists for RADIUS authorization and accounting.

Method List Overview

A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on a user. You can use method lists to designate one or more security protocols to be used, thus ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on users; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

This section contains the following tasks:

- [Identifying the RADIUS Server Host in a Wireless LAN, page 6](#) (required)
- [Configuring RADIUS Login Authentication for a Wireless LAN, page 10](#) (required)
- [Defining and Associating a AAA Server Group to a RADIUS Server, page 13](#) (optional)
- [Enabling RADIUS Accounting for a Wireless LAN, page 16](#) (optional)
- [Configuring Global Communication Settings Between an Access Point and a RADIUS Server, page 17](#) (optional)
- [Configuring the Access Point to Recognize and Use Vendor-Specific Attributes, page 19](#) (optional)
- [Configuring a Vendor-Proprietary RADIUS Server Host, page 21](#) (optional)

Identifying the RADIUS Server Host in a Wireless LAN

Perform this task to identify the RADIUS server host in a wireless LAN.

You also need to configure some settings on the RADIUS server. These settings include the IP address of the AP and the key string to be shared by both the server and the AP. For more information, refer to your RADIUS server documentation.

RADIUS Security Server Identification and Encryption

You identify RADIUS security servers by their hostname or IP address, hostname and specific User Datagram Protocol (UDP) port numbers, or their IP address and specific UDP port numbers. The combination of the IP address and the UDP port number creates a unique identifier allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. 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—such as accounting—the second host entry configured acts as a failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the AP tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order that they are configured.)

A RADIUS server and the AP 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 AP.

The timeout, retransmission, and encryption key values can be configured globally per server for all RADIUS servers or in some combination of global and per-server settings. To apply these settings globally to all RADIUS servers communicating with the AP, use the **radius-server timeout**, **radius-server retransmit**, and **radius-server key** commands, respectively. To apply these values on a specific RADIUS server, use the **radius-server host** command.



Note

If you configure both global and per-server functions (timeout, retransmission, and key commands) on the AP, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands. For information on configuring these setting on all RADIUS servers, see [“Configuring Global Communication Settings Between an Access Point and a RADIUS Server, page 17”](#).


RADIUS and AAA are disabled by default.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Router(config)# aaa new-model	Enables AAA.

Command or Action	Purpose
<p>Step 4</p> <pre>radius-server host {hostname ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]</pre> <p>Example: Router(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1</p>	<p>Specifies the IP address or hostname of the remote RADIUS server host.</p> <ul style="list-style-type: none"> • (Optional) For auth-port <i>port-number</i>, specify the UDP destination port for authentication requests. • (Optional) For acct-port <i>port-number</i>, specify the UDP destination port for accounting requests. • (Optional) For timeout <i>seconds</i>, specify the time interval that the AP waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the radius-server timeout global configuration command setting. If no timeout is set with the radius-server host command, the setting of the radius-server timeout command is used. • (Optional) For retransmit <i>retries</i>, specify the number of times a RADIUS request is re-sent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the radius-server host command, the setting of the radius-server retransmit global configuration command is used. • (Optional) For key <i>string</i>, specify the authentication and encryption key used between the AP and the RADIUS daemon running on the RADIUS server. <p> 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. 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 are part of the key.</p> <ul style="list-style-type: none"> • To configure the AP to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The AP software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.

	Command or Action	Purpose
Step 5	<code>end</code>	Returns to privileged EXEC mode.
	Example: <code>Router(config)# end</code>	
Step 6	<code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.
	Example: <code>Router# copy running-config startup-config</code>	

What to Do Next

After you identify the RADIUS host, configure RADIUS login authentication. See the “[Configuring RADIUS Login Authentication for a Wireless LAN](#)” section.

You can configure the AP to use AAA server groups to group existing server hosts for authentication by completing the optional task in the “[Defining and Associating a AAA Server Group to a RADIUS Server](#)” section.

Configuring RADIUS Login Authentication for a Wireless LAN

Perform this task to configure RADIUS login authentication for a wireless LAN.

Authentication Method List Overview

To configure RADIUS authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `aaa new-model`
4. `aaa authentication login {default | list-name} method1 [method2...]`
5. `line [console | tty | vty] line-number [ending-line-number]`
6. `login authentication {default | list-name}`

7. `radius-server attribute 32 include-in-access-req format %h`
8. `end`
9. `copy running-config startup-config`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>aaa new-model</p> <p>Example: Router(config)# aaa new-model</p>	<p>Enables AAA.</p>
Step 4	<p>aaa authentication login {default list-name} method1 [method2...]</p> <p>Example: Router(config)# aaa authentication login default local</p>	<p>Creates a login authentication method list.</p> <ul style="list-style-type: none"> To create a default list that is used when a named list is <i>not</i> specified in the login authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. For the <i>method1 argument</i>, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. <p>Select one of these methods:</p> <ul style="list-style-type: none"> line—Use the line password for authentication. You must define a line password before you can use this authentication method. Use the password password line configuration command. local—Use the local username database for authentication. You must enter username information in the database. Use the username password global configuration command. radius—Use RADIUS authentication. You must identify the RADIUS server host before you can use this authentication method. For more information, see the “Identifying the RADIUS Server Host in a Wireless LAN” section.
Step 5	<p>line [console tty vty] line-number [ending-line-number]</p> <p>Example: Router(config)# line 10</p>	<p>Configures the lines to which you want to apply the authentication list, and enters line configuration mode.</p>

	Command or Action	Purpose
Step 6	<pre>login authentication {default list-name}</pre> <p>Example: Router(config-line)# login authentication default</p>	<p>Applies the authentication list to a line or set of lines.</p> <ul style="list-style-type: none"> If you specify the default keyword, use the default list created with the aaa authentication login command. For the <i>list-name</i> argument, specify the list created with the aaa authentication login command.
Step 7	<pre>radius-server attribute 32 include-in-access-req format %h</pre> <p>Example: Router(config-line)# radius-server attribute 32 include-in-access-req format %h</p>	<p>Configures the AP to send its system name in the NAS_ID attribute for authentication.</p>
Step 8	<pre>end</pre> <p>Example: Router(config-line)# end</p>	<p>Returns to privileged EXEC mode.</p>
Step 9	<pre>copy running-config startup-config</pre> <p>Example: Router# copy running-config startup-config</p>	<p>(Optional) Saves your entries in the configuration file.</p>

Defining and Associating a AAA Server Group to a RADIUS Server

Perform this task to define a AAA server group and associate a particular RADIUS server with that server group.

Benefits of AAA Server Groups

You can configure the AP to use AAA server groups to group existing server hosts for authentication. You select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list, which lists the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. If you configure two different host entries on the same RADIUS server for the same service (such as accounting), the second configured host entry acts as a failover backup to the first one.


You use the **server** group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional **auth-port** and **acct-port** keywords.

SUMMARY STEPS

- enable**
- configure terminal**
- aaa new-model**
- radius-server host** {hostname | ip-address} [**auth-port** port-number] [**acct-port** port-number] [timeout seconds] [retransmit retries] [key string]

5. **aaa group server radius** *group-name*
6. **server** *ip-address*
7. **end**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>aaa new-model</p> <p>Example: Router(config)# aaa new-model</p>	<p>Enables AAA.</p>
Step 4	<p>radius-server host {hostname ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]</p> <p>Example: Router(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001</p>	<p>Specifies the IP address or hostname of the remote RADIUS server host.</p> <ul style="list-style-type: none"> (Optional) For auth-port port-number, specify the UDP destination port for authentication requests. (Optional) For acct-port port-number, specify the UDP destination port for accounting requests. (Optional) For timeout seconds, specify the time interval that the AP waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the radius-server timeout global configuration command setting. If no timeout is set with the radius-server host command, the setting of the radius-server timeout command is used. (Optional) For retransmit retries, specify the number of times a RADIUS request is re-sent to a server if that server is not responding or responding slowly. The range is from 1 to 1000. If no retransmit value is set with the radius-server host command, the setting of the radius-server retransmit global configuration command is used. (Optional) For key string, specify the authentication and encryption key used between the AP and the RADIUS daemon running on the RADIUS server. <p> 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. 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 are part of the key.</p>

	Command or Action	Purpose
Step 5	aaa group server radius <i>group-name</i> Example: Router(config)# aaa group server radius group1	Defines the AAA server group with a group name and places the AP in server group configuration mode.
Step 6	server <i>ip-address</i> Example: Router(config-sg)# server 172.20.0.1	Associates a particular RADIUS server with the defined server group. <ul style="list-style-type: none"> Repeat this step for each RADIUS server in the AAA server group. Each server in the group must be previously defined.
Step 7	end Example: Router(config-sg)# end	Returns to privileged EXEC mode.
Step 8	copy running-config startup-config Example: Router# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Enabling RADIUS Accounting for a Wireless LAN

Perform this task to enable RADIUS accounting for each Cisco IOS privilege level and for network services.

The AAA accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the AP reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa accounting network start-stop radius**
4. **ip radius source-interface bvi1**
5. **aaa accounting update periodic** *minutes*
6. **end**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa accounting network start-stop radius Example: Router(config)# aaa accounting network start-stop radius	Enables RADIUS accounting for all network-related service requests.
Step 4	ip radius source-interface bvi1 Example: Router(config)# ip radius source-interface bvi1	Configures the AP to send its bridge virtual interface (BVI) IP address in the NAS_IP_ADDRESS attribute for accounting records.
Step 5	aaa accounting update periodic minutes Example: Router(config)# aaa accounting update periodic 5	Specifies an accounting update interval in minutes.
Step 6	end Example: Router(config)# end	Returns to privileged EXEC mode.
Step 7	copy running-config startup-config Example: Router# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring Global Communication Settings Between an Access Point and a RADIUS Server


Perform this task to configure global communication settings between an AP and a RADIUS server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server key {0 string | 7 string | string}**
4. **radius-server retransmit retries**
5. **radius-server deadline minutes**
6. **end**

7. copy running-config startup-config

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>radius-server key {0 string 7 string string}</p> <p>Example: Router(config)# radius-server key anykey</p>	<p>Specifies the shared secret text string used between the AP and all RADIUS servers.</p> <ul style="list-style-type: none"> The key is a text string that must match the encryption key used on the RADIUS server. 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 are part of the key.
Step 4	<p>radius-server retransmit retries</p> <p>Example: Router(config)# radius-server retransmit 5</p>	<p>Specifies the number of times the AP sends each RADIUS request to the server before giving up.</p> <ul style="list-style-type: none"> The range is from 1 to 1000; the default is 3.
Step 5	<p>radius-server deadtime minutes</p> <p>Example: Router(config)# radius-server deadtime 5</p>	<p>Causes the Cisco IOS software to mark as “dead” any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the request to time out before the software tries the next configured server.</p> <ul style="list-style-type: none"> A RADIUS server marked as dead is omitted in additional requests for the duration of minutes that you specify, up to a maximum of 1440 minutes (24 hours). <p> Note If you set up more than one RADIUS server, you must configure the RADIUS server deadtime for optimal performance.</p>
Step 6	<p>end</p> <p>Example: Router(config)# end</p>	<p>Returns to privileged EXEC mode.</p>
Step 7	<p>copy running-config startup-config</p> <p>Example: Router# copy running-config startup-config</p>	<p>(Optional) Saves your entries in the configuration file.</p>

Configuring the Access Point to Recognize and Use Vendor-Specific Attributes

Perform this task to configure the AP to recognize and use vendor-specific attributes (VSAs).

Vendor-Specific Attributes Use on Access Points

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the AP and the RADIUS server by using the vendor-specific attribute (attribute 26). A VSA allows a vendor to support its own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by 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. *Attribute* and *value* are an appropriate AV pair, and *sep* is = for mandatory attributes and the asterisk (*) for optional attributes. This allows the full set of features to be used for RADIUS.

For example, the following AV pair activates Cisco's *Multiple Named IP Address Pools* feature during IP authorization (during PPP's IPCP address assignment):

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

The following example shows how to provide a user logging in from an AP with immediate access to privileged EXEC commands:

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

Other vendors have their own unique vendor IDs, options, and associated VSAs. For more information about vendor IDs and VSAs, refer to RFC 2138, *Remote Authentication Dial-In User Service (RADIUS)*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server vsa send [accounting | authentication]**
4. **end**
5. copy running-config startup-config

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">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	Configures the AP to recognize and use VSAs as defined by RADIUS IETF attribute 26. <ul style="list-style-type: none">(Optional) Use the accounting keyword to limit the set of recognized vendor-specific attributes to only accounting attributes.(Optional) Use the authentication keyword to limit the set of recognized vendor-specific attributes to only authentication attributes.If you enter this command without keywords, both accounting and authentication vendor-specific attributes are used.
Step 4	end Example: Router(config)# end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config Example: Router# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring a Vendor-Proprietary RADIUS Server Host

Perform this task to configure a vendor-proprietary RADIUS server host and a shared secret text string.

Although an IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the AP 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 AP. You specify the RADIUS host and secret text string by using the **radius-server** global configuration commands.

SUMMARY STEPS

- enable**
- configure terminal**
- radius-server host {hostname | ip-address} non-standard**

4. **end**
5. `copy running-config startup-config`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • 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} non-standard Example: Router(config)# radius-server host samplehost 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 4	end Example: Router(config)# end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config Example: Router# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

How to Configure a Local Authenticator in a Wireless LAN

This section describes how to configure an access point in a wireless LAN as a local authenticator.

This section contains the following task:

- [Configuring Local or Backup Authentication Service, page 22](#) (required if

Configuring Local or Backup Authentication Service

Perform this task to configure local or backup authentication service.

You can configure your APs to use a local authenticator when they cannot reach the main servers, or you can configure your APs to use the local authenticator or as the main authenticator if you do not have a RADIUS server. When you configure the local authenticator as a backup to your main servers, the APs periodically check the link to the main servers and stop using the local authenticator automatically when the link to the main servers is restored.

When you configure an AP as a local authenticator, use an AP that does not serve a large number of client devices. When the AP acts as an authenticator, performance might degrade for associated client devices. Also, the AP you use as an authenticator contains detailed authentication information for your wireless LAN. Physically secure it to protect its configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server local**
5. **nas ip-address key shared-key**
6. Repeat Step 5 to add each AP that uses the local authenticator
7. **group group-name**
8. **vlan vlan**
9. **ssid name**
10. **reauthentication time seconds**
11. **block count count time {seconds | infinite}**
12. **exit**
13. **user username {password | nhash} password [group group-name] [mac-auth-only]**
14. **end**
15. copy running-config startup-config

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> 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 system.
Step 4	radius-server local Example: Router(config)# radius-server local	Configures the AP or wireless-aware router as a local authentication server, and enters authenticator configuration mode.
Step 5	nas ip-address key shared-key Example: Router(config-radsrv)# nas 10.91.6.159 key 110337	Adds an AP to the list of devices that use the local authentication server. <ul style="list-style-type: none"> Enter the AP IP address and the shared key used to authenticate communication between the local authenticator and other APs. You must enter this shared key on the APs that use the local authenticator. If your local authenticator also serves client devices, you must enter the local authenticator AP as a NAS. Leading spaces in the shared key string are ignored, but spaces within and at the end of the key are used. If you use spaces in your shared key, do not enclose the key in quotation marks unless the quotation marks are part of the shared key.
Step 6	Repeat Step 5 to add each AP that uses the local authenticator.	—
Step 7	group group-name Example: Router(config-radsrv)# group clerks	(Optional) Configures a user group to which you can assign shared settings, and enters user group configuration mode.
Step 8	vlan vlan Example: Router(config-radsrv-group)# vlan 87	(Optional) Specifies a VLAN to be used by members of the user group. <ul style="list-style-type: none"> The AP moves group members into a VLAN, overriding other VLAN assignments. You can assign only one VLAN to the group.

	Command or Action	Purpose
Step 9	<p>ssid <i>name</i></p> <p>Example: Router(config-radsrv-group)# ssid anyname</p>	<p>(Optional) Creates an SSID for a radio interface.</p> <ul style="list-style-type: none"> • Enter up to 20 SSIDs to limit members of the user group to those SSIDs. • The AP checks that the SSID that the client used to associate matches one of the SSIDs in the list. If the SSID does not match, the client is disassociated.
Step 10	<p>reauthentication time <i>seconds</i></p> <p>Example: Router(config-radsrv-group)# reauthentication time 1800</p>	<p>(Optional) Specifies the number of seconds after which the AP should reauthenticate members of the group.</p> <ul style="list-style-type: none"> • The reauthentication provides users with a new encryption key. The default setting is 0, which means that group members are never required to reauthenticate.
Step 11	<p>block count <i>count</i> time {<i>seconds</i> infinite}</p> <p>Example: Router(config-radsrv-group)# block count 3 time infinite</p>	<p>(Optional) To help protect against password guessing attacks, locks out members of a user group for a length of time after a set number of incorrect passwords.</p> <ul style="list-style-type: none"> • <i>count</i>—The number of failed passwords that triggers a lockout of the username. • <i>seconds</i>—The number of seconds the lockout should last. If you use the infinite keyword, an administrator must manually unblock the locked username. • See the clear radius local-server command for information on how to unblock a locked username.
Step 12	<p>exit</p> <p>Example: Router(config-radsrv-group)# exit</p>	<p>Exits user group configuration mode and returns to authenticator configuration mode.</p>

	Command or Action	Purpose
Step 13	<pre>user username {password nthash} password [group group-name] [mac-auth-only]</pre> <p>Example: Router(config-radsrv)# user anyuser password pwd1234 group clerks</p>	<p>Specifies the LEAP users allowed to authenticate using the local authenticator.</p> <ul style="list-style-type: none"> • Enter a username and password for each user. If you do not know the user password, look up the NT value of the password in the authentication server database, and enter the NT hash as a hexadecimal string. • To add a client device for MAC-based authentication, enter the client MAC address as both the username and password. Enter 12 hexadecimal digits without a dot or dash between the numbers as the username and the password. For example, for the MAC address 0009.5125.d02b, enter <i>00095125d02b</i> as both the username and the password. • (Optional) To add the user to a user group, enter the group name. If you do not specify a group, the user is not assigned to a specific VLAN and is never forced to reauthenticate. • (Optional) To limit the user to MAC authentication only, enter mac-auth-only.
Step 14	<pre>end</pre> <p>Example: Router(config-radsrv)# end</p>	Returns to privileged EXEC mode.
Step 15	<pre>copy running-config startup-config</pre> <p>Example: Router# copy running-config startup-config</p>	(Optional) Saves your entries in the configuration file.

Configuration Examples for a RADIUS Server or a Local Authenticator in a Wireless LAN

This section contains the following example:

- [Configuring a Local Authenticator in a Wireless LAN: Example, page 26](#)

Configuring a Local Authenticator in a Wireless LAN: Example

The following example shows how to:

- Configure a local authenticator in a wireless LAN used by three APs all sharing the same key.
- Configure three user groups: sales, marketing, and managers.
- Configure individual users, each of which will authenticate to the AP using either a personal password or a MAC address.

```
configure terminal
  radius-server local
  nas 10.91.6.159 key 110337
  nas 10.91.6.162 key 110337
  nas 10.91.6.181 key 110337
  group sales
  vlan 87
  ssid name1
  ssid name2
  reauthentication time 1800
  block count 2 time 600
  group marketing
  vlan 97
  ssid name3
  ssid name4
  ssid name5
  reauthentication time 1800
  block count 2 time 600
  group managers
  vlan 77
  ssid name6
  ssid name7
  reauthentication time 1800
  block count 2 time 600
  exit
! The following three users will authenticate using their own passwords.
  user username1 password pwd1 group sales
  user username2 password pwd2 group sales
  user username3 password pwd3 group sales
! These three users will authenticate using their MAC addresses.
  user 00095125d02b password 00095125d02b group marketing mac-auth-only
  user 00095125d02b password 00095125d02b group sales mac-auth-only
  user 00079431f04a password 00079431f04a group sales mac-auth-only
  user username4 password 272165 group managers
  user username5 password 383981 group managers
end
copy running-config startup-config
```

Additional References

The following sections provide references related to configuring a RADIUS server or a local authenticator.

Related Documents

Related Topic	Document Title
Cisco IOS wireless LAN commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS Wireless LAN Command Reference</i>

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	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
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Configuring RADIUS or a Local Authenticator in a Wireless LAN

Table 5 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.4T or later appear in the table.

For information on a feature in this technology that is not documented here, see the “Cisco IOS Wireless LAN Features Roadmap” module.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

**Note**

Table 5 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 5 Feature Information for Configuring RADIUS or a Local Authenticator in a Wireless LAN

Feature Name	Releases	Feature Information
RADIUS Server per SSID	12.4T	<p>This feature allows RADIUS servers to be specified on a per-SSID basis.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Network Environments Recommended to Use RADIUS for Access Security in a Wireless LAN, page 2 • RADIUS Operation in a Wireless LAN, page 3 • Identifying the RADIUS Server Host in a Wireless LAN, page 6

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

© 2007 Cisco Systems, Inc. All rights reserved.

