Using an Access Point as a Local Authenticator

This module describes how to use a wireless device in the role of an access point as a local authenticator, serving as a standalone authenticator for a small wireless LAN, or providing backup authentication service. As a local authenticator, the access point performs LEAP, EAP-FAST, and MAC-based authentication for up to 50 client devices.

This document contains the following sections:

Understanding Local Authentication

Many small wireless LANs could be made more secure with 802.1x authentication, but they do not have access to a RADIUS server. Of the many wireless LANs that use 802.1x authentication, access points rely on RADIUS servers housed in distant locations to authenticate client devices, and the authentication traffic must cross a WAN link. If the WAN link fails, or if the access points cannot access the RADIUS servers for any reason, client devices are unable to access the wireless network even if the work they want to do is entirely local. (For detailed instructions on setting up RADIUS servers to be used by your access points for authentication, see the *Radius and TACACS+ Servers in a Wireless Environment* document on Cisco.com.

To provide local authentication service or backup authentication service for a WAN link failure or circumstance where a server fails, you can configure an access point to act as a local authentication server. The access point can authenticate up to 50 wireless client devices using LEAP, EAP-FAST, or MAC-based authentication. The access point performs up to 5 authentications per second.

You configure the local authenticator access point manually with client usernames and passwords because it does not synchronize its database with RADIUS servers. You can specify a VLAN and a list of SSIDs that a client is allowed to use.

Note If your wireless LAN contains only one access point, you can configure the access point as both the 802.1x authenticator and the local authenticator. However, users associated to the local authenticator access point might notice a drop in performance while the access point authenticates client devices.

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

You can configure your access points to use the local authenticator as the main authenticator if you do not have a RADIUS server. When you configure the local authenticator as a backup to your RADIUS servers, the access points periodically check the link to the authentication servers and stops local authentication automatically when the link to the main servers is restored.

Caution The access point you use as an authenticator contains detailed authentication information for your wireless LAN. You should secure it physically to protect its configuration.

Configuring a Local Authenticator

This section provides instructions for setting up an access point as a local authenticator and includes these sections:

Guidelines for Local Authenticators

Follow these guidelines when configuring an access point as a local authenticator:

- Use an access point that does not serve a large number of client devices. When the access point acts as an authenticator, performance might degrade for associated client devices.
- Secure the access point physically to protect its configuration.

Configuration Overview

You complete these major steps when you set up a local authenticator:

1. On the local authenticator, create a list of access points authorized to use the authenticator to authenticate client devices. Each access point that uses the local authenticator is a network access server (NAS).

   Note If your local authenticator access point also serves client devices, you must enter the local authenticator access point as a NAS. When a client associates to the local authenticator access point, the access point uses itself to authenticate the client.

2. On the local authenticator, create user groups and configure parameters to be applied to each group (optional).
3. On the local authenticator, create a list of up to 50 LEAP users, EAP-FAST users, or MAC addresses that the local authenticator is authorized to authenticate.

Note You do not have to specify which type of authentication that you want the local authenticator to perform. It automatically performs LEAP, EAP-FAST, or MAC-address authentication for the users based on the authentication request.

4. On the access points that use the local authenticator to authenticate their clients, enter the local authenticator as a RADIUS server. When a client associates to the local authenticator access point, the access point uses its local authentication list to authenticate the client.

Configuring the Local Authenticator Access Point

To configure the access point as a local authenticator, follow these steps, beginning in privileged EXEC mode:

	Command	Description
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**aaa new-model**	Enables AAA.
Step 3	**radius-server local**	Enables the access point as a local authenticator and enter configuration mode for the authenticator.
Step 4	**nas** *ip-address* **key** *shared-key*	Adds an access point to the list of units that use the local authenticator. Enter the access point IP address and the shared key used to authenticate communication between the local authenticator and other access points. You must enter this shared key on the devices that use the local authenticator. If your local authenticator also serves client devices in the roll of an access point, you must configure the local authenticator access point as a NAS. **Note** Leading spaces in the key string 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. Repeat this step to add each access point that uses the local authenticator.
Step 5	**group** *group-name*	(Optional) Enters user group configuration mode and configure a user group to which you can assign shared settings.

	Command	Description
Step 6	**vlan** *vlan*	(Optional) Specifies a VLAN to be used by members of the user group. The access point moves group members into that VLAN, overriding other VLAN assignments. You can assign only one VLAN to the group.
Step 7	**ssid** *ssid*	(Optional) Enters up to 20 SSIDs to limit members of the user group to those SSIDs. The access point 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 8	**reauthentication time** *seconds*	(Optional) Enters the number of seconds after which access points should reauthenticate members of the group. Reauthentication provides users with a new encryption key. The default setting is 0, which means that group members are never required to reauthenticate.
Step 9	**block count** *count* **time** { *seconds* | **infinite** }	(Optional) To help protect against password guessing attacks, you can lock out members of a user group for a length of time after a set number of passwords are entered incorrectly. • count—The number of failed passwords that triggers a lockout of the username. • time—The number of seconds the user is prevented from authenticating with any password, including the correct password. If you enter **infinite**, an administrator must manually unblock the locked username. See the "Unblocking Locked Usernames" section on page 9 for instructions on unblocking client devices.
Step 10	**exit**	Exits group configuration mode and return to authenticator configuration mode.

	Command	Description
Step 11	**user** *username* { **password** | **nthash** } *password* [**group** *group-name*] [**mac-auth-only**]	Enters the LEAP and EAP-FAST users allowed to authenticate using the local authenticator. You must enter a username and password for each user. If you only know the NT value of the password, which you can often find in the authentication server database, you can enter the NT hash as a string of hexadecimal digits. To add a client device for MAC-based authentication, enter the client MAC address as both the username and password parameters. Enter the MAC address as 12 hexadecimal digits without dots or dashes between the numbers. For example, for the MAC address 0009.5125.d02b, enter *00095125d02b* as both the username and the password. To limit the user to MAC authentication only, enter **mac-auth-only**. 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.
Step 12	**end**	Returns to privileged EXEC mode.

This example shows how to set up a local authenticator used by three access points with three user groups and several users:

```
AP# configure terminal
AP(config)# radius-server local
AP(config-radsrv)# nas 10.91.6.159 key 110337
AP(config-radsrv)# nas 10.91.6.162 key 110337
AP(config-radsrv)# nas 10.91.6.181 key 110337
AP(config-radsrv)# group clerks
AP(config-radsrv-group)# vlan 87
AP(config-radsrv-group)# ssid batman
AP(config-radsrv-group)# ssid robin
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# group cashiers
AP(config-radsrv-group)# vlan 97
AP(config-radsrv-group)# ssid deer
AP(config-radsrv-group)# ssid antelope
AP(config-radsrv-group)# ssid elk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# group managers
AP(config-radsrv-group)# vlan 77
AP(config-radsrv-group)# ssid mouse
AP(config-radsrv-group)# ssid chipmunk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# exit
```

```
AP(config-radsrv)# user jsmith password twain74 group clerks
AP(config-radsrv)# user stpatrick password snake100 group clerks
AP(config-radsrv)# user nick password uptown group clerks
AP(config-radsrv)# user 00095125d02b password 00095125d02b group clerks mac-auth-only
AP(config-radsrv)# user 00095125d02b password 00095125d02b group cashiers
AP(config-radsrv)# user 00079431f04a password 00079431f04a group cashiers
AP(config-radsrv)# user carl password 272165 group managers
AP(config-radsrv)# user vic password lid178 group managers
AP(config-radsrv)# end
```

Configuring Other Access Points to Use the Local Authenticator

You add the local authenticator to the list of servers on the client access point the same way that you add other servers.

Note If your local authenticator access point also serves client devices, you must configure the local authenticator to use itself to authenticate client devices.

On the other access points that use the local authenticator access point for client authentication, use the **radius-server host** command to identify the local authenticator as a RADIUS server. The order in which the access point attempts to use the servers matches the order in which you list the servers in the configuration. If you are configuring the access point to use RADIUS for the first time, enter the main RADIUS servers first, and enter the local authenticator last.

Note You must enter **1812** as the authentication port and **1813** as the accounting port. The local authenticator listens on UDP port 1813 for RADIUS accounting packets. It discards the accounting packets but sends acknowledgement packets back to the clients to prevent clients from assuming that the RADIUS server is down.

Use the **radius-server deadtime** command to set an interval during which the access point does not attempt to use servers that do not respond, thus avoiding the wait for a request to time out before trying the next configured server. A server marked as dead is skipped by the subsequent authentication requests for the duration of time that you specify, up to 1440 minutes (24 hours).

The following example shows how to set up two main servers and a local authenticator with a server deadtime of 10 minutes:

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001 key 77654
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646 key 77654
AP(config)# radius-server host 10.91.6.151 auth-port 1812 acct-port 1813 key 110337
AP(config)# radius-server deadtime 10
```

Assuming the WAN link to the main servers has failed, this access point completes these steps when a LEAP-enabled client device attempts to associate with the access point:

1. It tries the first server, times out multiple times, and receiving no acknowledgements, marks the first server as dead.
2. It tries the second server, times out multiple times, and receiving no acknowledgements, marks the second server as dead.
3. It tries and successfully authenticates by using the local authenticator.

During the 10-minute dead-time interval, the next client device that attempts to authenticate to the access point, the access point skips the first two servers and attempts to authenticate the client by using the local authenticator. After the dead-time interval elapses, the access point tries to use the first two servers for authentication. When setting a dead time, you must balance the need to skip dead servers with the need to maintain the links to the main RADIUS servers. Begin using the main RADIUS servers again as soon as possible.

Each time an access point tries to use one of the main servers while the link is down or the server is down, the client device trying to authenticate reports an authentication time out. You can extend the time out value on Cisco client devices to accommodate expected server time outs.

To remove the local authenticator from the access point configuration, use the **no radius-server host** ***hostname* | *ip-address*** global configuration command.

Configuring EAP-FAST Authentication

The default settings for EAP-FAST authentication are suitable for most wireless LANs. However, you can customize the credential time out values, authority ID, and server keys to match your network requirements.

Configuring PAC Settings

This section describes how to configure Protected Access Credential (PAC) settings. The first time that an EAP-FAST client device attempts to authenticate to the local authenticator, the local authenticator generates a PAC for the client. You can also generate PACs manually and use the Aironet Client Utility to import the PAC file.

PAC Expiration Times

You can limit the number of days for which PACs are valid, and set a grace period during which PACs are valid after they have expired. By default, PACs are valid for infinite days, with a grace period of infinite days. You apply the expiration time and the grace period settings to a group of users.

To configure the expiration time and grace period for PACs, use this command:

AP(config-radsrv-group)# **eapfast pac expiry** *days* [**grace** *days*]

Enter a number of days from 2 to 4095. Enter the **no** form of the command to reset the expiration time or grace period to infinite days.

In this example, PACs for the user group expire in 100 days with a grace period of two days:

```
AP(config-radsrv-group)# eapfast pac expiry 100 grace 2
```

Note If one user is not part of the user group for which the PAC is configured, then the default PAC expiry for that user is 2 days (one day default period plus one day grace period).

Generating PACs Manually

The local authenticator automatically generates PACs for EAP-FAST clients that request them. However, you might need to generate a PAC manually for some client devices. When you enter the command, the local authenticator generates a PAC file and writes it to the network location that you specify. The user imports the PAC file into the client profile.

To generate a PAC manually, use the following command:

AP# **radius local-server pac-generate** *filename username* [**password** *password*] [**expiry** *days*]

When you enter the PAC filename, enter the full path to which the local authenticator writes the PAC file (such as tftp://172.1.1.1/test/user.pac). The password is optional and, if not specified, a default password understood by the CCX client is used. Expiry is also optional and, if not specified, the default period is 1 day.

In the following example, the local authenticator generates a PAC for the username *joe*, password-protects the file with the password *bingo*, sets the PAC to expire in 10 days, and writes the PAC file to the TFTP server at 10.0.0.5:

```
AP# radius local-server pac-generate tftp://10.0.0.5 joe password bingo expiry 10
```

Configuring an Authority ID

All EAP-FAST authenticators are identified by an authority identity (AID). The local authenticator sends its AID to an authenticating client, and the client checks its database for a matching AID. If the client does not recognize the AID, it requests a new PAC.

To assign an AID to the local authenticator, use the following commands:

AP(config-radserv)# **eapfast authority id** *identifier*

AP(config-radserv)# **eapfast authority info** *identifier*

The **eapfast authority id** command assigns an AID that the client device uses during authentication.

Configuring Server Keys

The local authenticator uses server keys to encrypt PACs that it generates and to decrypt PACs when authenticating clients. The server maintains two keys, a primary key and a secondary key, and uses the primary key to encrypt PACs. By default, the server uses a default value as the primary key but does not use a secondary key unless you configure one.

When the local authenticator receives a client PAC, it attempts to decrypt the PAC with the primary key. If decryption fails with the primary, the authenticator attempts to decrypt the PAC with the secondary key if one is configured. If decryption fails, the authenticator rejects the PAC as invalid.

To configure server keys, use the following commands:

```
AP(config-radsrv)# eapfast server-key primary {[auto-generate] | [ [0 | 7] key]}
AP(config-radsrv)# eapfast server-key secondary [0 | 7] key
```

Keys can contain up to 32 hexadecimal digits. Enter **0** before the key to enter an unencrypted key. Enter **7** before the key to enter an encrypted key. Use the **no** form of the commands to reset the local authenticator to the default setting, which is to use a default value as a primary key.

Possible PAC Failures Caused by Access Point Clock

The local authenticator uses the access point clock to both generate PACs and to determine whether PACs are valid. However, relying on the access point clock can lead to PAC failures.

If your local authenticator access point receives its time setting from an NTP server, there is an interval between boot up and synchronization with the NTP server during which the access point uses its default time setting. If the local authenticator generates a PAC during that interval, the PAC might be expired when the access point receives a new time setting from the NTP server. If an EAP-FAST client attempts to authenticate during the interval between boot and NTP-synch, the local authenticator might reject the client's PAC as invalid.

If your local authenticator does not receive its time setting from an NTP server and it reboots frequently, PACs generated by the local authenticator might not expire when they should. The access point clock is reset when the access point reboots, so the elapsed time on the clock would not reach the PAC expiration time.

Limiting the Local Authenticator to One Authentication Type

By default, a local authenticator access point performs LEAP, EAP-FAST, and MAC-based authentication for client devices. However, you can limit the local authenticator to perform only one or two authentication types. Use the **no authentication** command to restrict the authenticator to an authentication type:

AP(config-radsrv)# **no authentication** [**eapfast**] [**leap**] [mac]

Because all authentication types are enabled by default, enter the **no** form of the command to disable authentication types. For example, if you want the authenticator to perform only LEAP authentication, you enter these commands:

```
AP(config-radsrv)# no authentication eapfast
AP(config-radsrv)# no authentication mac
```

Unblocking Locked Usernames

You can unblock usernames before the lockout time expires, or when the lockout time is set to infinite. To unblock a locked username, enter this command in privileged Exec mode on the local authenticator:

AP# **clear radius local-server user** *username*

Viewing Local Authenticator Statistics

To view statistics collected by the local authenticator, enter this command in privileged EXEC mode:

AP# **show radius local-server statistics**

This example shows local authenticator statistics:

```
Successes              : 0           Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 0
Unknown NAS            : 0           Invalid packet from NAS: 0

NAS : 10.91.6.158
Successes              : 0           Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 0
Corrupted packet       : 0           Unknown RADIUS message : 0
No username attribute  : 0           Missing auth attribute : 0
Shared key mismatch    : 0           Invalid state attribute: 0
Unknown EAP message    : 0           Unknown EAP auth type  : 0
Auto provision success : 0           Auto provision failure : 0
PAC refresh            : 0           Invalid PAC received   : 0

Username                  Successes  Failures  Blocks
nicky                             0         0       0
jones                             0         0       0
jsmith                            0         0       0
Router#sh radius local-server statistics
Successes              : 1           Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 0
Unknown NAS            : 0           Invalid packet from NAS: 0

NAS : 100.0.0.53
Successes              : 1           Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 0
Corrupted packet       : 0           Unknown RADIUS message : 0
No username attribute  : 0           Missing auth attribute : 0
Shared key mismatch    : 0           Invalid state attribute: 0
Unknown EAP message    : 0           Unknown EAP auth type  : 0

Username                  Successes  Failures  Blocks
clients_aaa                           1        0       0
```

The first section of statistics lists cumulative statistics from the local authenticator.

The second section lists stats for each access point (NAS) authorized to use the local authenticator. The EAP-FAST statistics in this section include these stats:

- Auto provision success—the number of PACs generated automatically
- Auto provision failure—the number of PACs not generated because of an invalid handshake packet or invalid username or password
- PAC refresh—the number of PACs renewed by clients
- Invalid PAC received—the number of PACs received that were expired, that the authenticator could not decrypt, or that were assigned to a client username not in the authenticator's database

The third section lists stats for individual users. If a user is blocked and the lockout time is set to infinite, *blocked* appears at the end of the stat line for that user. If the lockout time is not infinite, *Unblocked in x seconds* appears at the end of the stat line for that user.

To reset local authenticator statistics to zero, use this command in privileged EXEC mode:

AP# **clear radius local-server statistics**

Using Debug Messages

To control the display of debug messages for the local authenticator, enter this command in privileged EXEC mode:

AP# **debug radius local-server** {**client** | **eapfast** | **error** | **packets**}

Use the command options to display this debug information:

- Use the **client** option to display error messages related to failed client authentications.
- Use the **eapfast** option to display error messages related to EAP-FAST authentication. Use the sub-options to select specific debugging information:
  - **encryption** —displays information on the encryption and decryption of received and transmitted packets
  - **events**—displays information on all EAP-FAST events
  - **pac**—displays information on events related to PACs, such as PAC generation and verification
  - **pkts**—displays packets sent to and received from EAP-FAST clients
- Use the **error** option to display error messages related to the local authenticator.
- Use the **packets** option to turn on display of the content of RADIUS packets sent and received.