Remote Site IEEE 802.1X Local Authentication Service

First Published: May 23, 2003
Last Updated: March 30, 2011

The Remote Site IEEE 802.1X Local Authentication Service feature provides the ability to configure an access point or wireless-aware router to act as a local RADIUS server. Configuring local authentication service provides a backup authentication service in the event of a WAN link or server failure.

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 for Remote Site IEEE 802.1X Local Authentication Service" section on page 16.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

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

Restrictions for Configuring Remote Site IEEE 802.1X Local Authentication Service

The following are restrictions of the local authentication service feature:

- The local authentication server does not synchronize its database with the main RADIUS servers. It is necessary to manually configure the local authentication server with client usernames and passwords.
- LEAP is the only supported authentication protocol.
- Although multiple local authentication servers can exist on one network, only one authentication server can be configured on any single device.

Information About Configuring Remote Site IEEE 802.1x Local Authentication Service

On typical wireless LANs that use 802.1X authentication, access points and wireless-aware routers rely on remote site RADIUS servers to authenticate client devices. This authentication traffic must cross a WAN link. If the WAN link fails, or if the access points and routers cannot reach the RADIUS servers, then the client devices cannot access the wireless network even if their requirements for access are strictly local.

To provide for local authentication service or backup authentication service in the event of a WAN link or server failure, you can configure an access point or wireless-aware router to act as a local RADIUS server. The access point or wireless-aware router can authenticate Light Extensible Authentication Protocol (LEAP)–enabled wireless client devices and allow them to join your network.

Because the local authentication device does not synchronize its database with the main RADIUS servers. You must configure the local authentication server with client usernames and passwords. The local authentication server also permits you to specify a VLAN and a list of service set identifiers (SSIDs) that a client is allowed to use.

Follow these guidelines when you configure an access point or wireless-aware router as a local authentication server:

- To prevent performance degradation, configure local authentication service on an access point or a wireless-aware router that does not have a high CPU load.
- Physically secure the access point or router to protect its configuration.

Table 1 shows the maximum number of clients that can be configured on a local authentication server.

Table 1 Maximum Number of Clients That Can be Configured on a Local Authentication Server

Local Authentication Server	Maximum Number of Clients
Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200	50
Cisco 2610XM, Cisco 2611XM routers	50
Cisco 2620XM, Cisco 2621XM routers	50
Cisco 2650XM, Cisco 2651XM routers	50

Table 1 Maximum Number of Clients That Can be Configured on a Local Authentication Server

Local Authentication Server	Maximum Number of Clients
Cisco 2691 routers	50
Cisco 2811 routers	50
Cisco 2821 routers	50
Cisco 2851 routers	50
Cisco 3725 routers	50
Cisco 3745 routers	50
Cisco 3825 routers	50
Cisco 3845 routers	50

Note Users that are associated to the local authentication server might notice a drop in performance during authentication of client devices. However, if your wireless LAN contains only one access point, you can configure that device as both the 802.1X authenticator and the local authentication server.

You configure access points and routers to use the local authentication server when they cannot reach the main servers or when a RADIUS server is not available.

The access points and wireless-aware routers stop using the local authentication server automatically when the link to the main servers is restored.

If your local authentication server also serves client devices, you must enter the local authentication server access point or router as a network access server (NAS). When a LEAP client associates to the local authentication server access point, the access point uses itself to authenticate the client.

Caution The access point or wireless-aware router that you use as an authentication server contains detailed authentication information about your wireless LAN, so you should secure it physically to protect its configuration.

How to Configure Remote Site IEEE 802.1X Local Authentication Service

This section contains the following procedures:

Configuring the Local Authentication Server

Perform this task to configure the access point as a local authentication server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server local**
5. **nas** *ip-address* **key** *shared-key*

DETAILED STEPS

	Command	Purpose
Step 1	`Router> enable` **Example:** `Router> enable`	Enables privileged EXEC mode.
Step 2	`Router# configure terminal` **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# aaa new-model` **Example:** `Router(config)# aaa new-model`	Enables AAA.
Step 4	`Router(config)# radius-server local` **Example:** `Router(config)# radius-server local`	Enables the access point or router as a local authentication server and enters configuration mode for the authentication server.
Step 5	`Router(config-radsrv)# nas` *`ip-address`* **`key`** *`shared-key`* **Example:** `Router(config)# nas 192.168.12.17 key shared256`	Adds an access point or wireless domain services (WDS) device to the list of units that use the local authentication server. Enter the IP address of the access point or WDS device, and the shared key used to authenticate communication between the local authentication server and other access points. You must enter this shared key on the WDS devices that use the local authentication server. Each access point and candidate WDS that uses the local authentication server is a network access server (NAS). If an access point is the local authentication server that also serves client devices, you must enter the local authentication server 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 and candidate WDS device that uses the local authentication server.

Configuring User Groups on the Local Authentication Server

Perform this optional task (beginning in local RADIUS server configuration mode) to configure user groups on the local authentication server.

Note If you do not wish to configure user groups on the local authentication server, skip this task and go to the "Creating the User List on the Local Authentication Server" section on page 7.

SUMMARY STEPS

1. **group** *group-name*
2. **vlan** *vlan*
3. **ssid** *ssid*
4. **reauthentication time** *seconds*
5. **block count** *count* **time** {*seconds* | **infinite**}
6. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	`Router(config-radsrv)# group group-name`	Enters user group configuration mode and configures a user group to which you can assign shared settings.
Step 2	`Router(config-radsrv-group)# 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 3	`Router(config-radsrv-group)# ssid ssid`	(Optional) Enters up to 20 service set identifiers (SSIDs) to limit members of the user group to those SSIDs. The access point checks whether the client's SSID matches an SSID in the list. If the SSID does not match, the client is disassociated.
Step 4	`Router(config-radsrv-group)# reauthentication time seconds`	(Optional) Configures the number of seconds after which access points should reauthenticate members of the group. 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 5	`Router(config-radsrv-group)# block count count time {seconds | infinite}`	(Optional) To help protect against password-guessing attacks, you can lock out group members for a length of time after a set number of incorrect passwords. • Count—The number of failed passwords that triggers a lockout of the username. • Time—The number of seconds that the lockout should last. If you enter **infinite**, an administrator must manually unblock the locked username. For more information, see the "Unblocking Usernames" section on page 6.
Step 6	`Router(config-radsrv-group)# exit`	Returns to authenticator configuration mode.

Unblocking 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 the following command in privileged EXEC mode on the local authentication server.

```
Router# clear radius local-server user username
```

Creating the User List on the Local Authentication Server

Perform the required task described in the following paragraphs to create a user list on the local authentication server and to configure the users that are allowed to authenticate using the local authentication server.

Note If you do not wish to configure users on the local authentication server, skip this task and go to the "Saving the Configuration on the Local Authentication Server" section on page 7.

You must enter a username and password for each user. If you know only the NT hash 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 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.

Beginning in local RADIUS server configuration mode, enter the **user** command for each username:

```
Router(config-radsrv)# user username {password | nthash} password [group group-name]
```

Saving the Configuration on the Local Authentication Server

Perform this optional task to save the current configuration.

SUMMARY STEPS

1. **end**
2. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	`Router(config-radsrv)# end`	Returns to privileged EXEC mode.
Step 2	`Router# copy running-config startup-config`	Saves your entries in the configuration file.

Configuring Access Points or Routers to Use the Local Authentication Server

Perform this required task to add the local authentication server to the list of servers on the client access point or wireless-aware router.

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

On the wireless devices that use the local authentication server, use the **radius-server host** command in privileged EXEC mode to enter the local authentication server as a RADIUS server. The order in which the devices attempt to use the servers matches the order in which you enter the servers in the device configuration. If you are configuring the device to use a RADIUS server for the first time, enter the main RADIUS servers first, and enter the local authentication server last.

Note You must enter **1812** as the authentication port and **1813** as the accounting port. The local authentication server listens on User Datagram Protocol (UDP) port 1813 for RADIUS accounting packets. It discards the accounting packets but sends acknowledge packets back to the RADIUS clients to prevent the clients from reacting as though the server is down.

Use the **radius-server deadtime** command in global configuration mode to set an interval during which the access point or router 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 additional requests for the duration of minutes that you specify, up to 1440 (24 hours).

To remove the local authentication server from the access point or router configuration, use the **no radius-server host** command in global configuration mode.

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. **aaa group server** {**radius** | **tacacs+**} *group-name*
6. **server ip-address auth-port 1812 acct-port 1813**
7. **aaa authentication login** *named-authentication-list*
8. **end**
9. **show running-config**
10. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	`Router> enable`	Enables privileged EXEC mode.
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# aaa new-model`	Enables authentication, authorization, and accounting (AAA). This step must be configured before the rest of the AAA configuration steps.

	Command	Purpose
Step 4	`Router(config)# radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]`	Specifies the IP address or hostname of the remote RADIUS server host. • (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 access point waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the setting made using the **radius-server timeout** command in global configuration mode. If no timeout is set with the **radius-server host** command, the setting made using the **radius-server timeout** command is used. • (Optional) For **retransmit** *retries*, specify the number of times that a RADIUS request is re-sent to a server if that server is not responding or is responding slowly. The range is 1 to 1000. If no retransmit value is set using the **radius-server host** command, the setting made using the **radius-server retransmit** command in global configuration command mode is used. • (Optional) For **key** *string*, specify the authentication and encryption key used between the access point and the RADIUS daemon running on the RADIUS server. **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. To configure the access point to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure to use a different UDP port number for each host. The access point 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.
Step 5	`aaa group server {radius | tacacs+} group-name`	Defines the AAA server-group with a group name.
Step 6	`Router(config-sg-radius)# server ip-address auth-port 1812 acct-port 1813`	Defines the AAA server IP address, authentication port, and accounting port.
Step 7	`Router(config)# aaa authentication login named-authentication-list`	Creates an authentication method list for the server group.
Step 8	`Router(config)# end`	Returns to privileged EXEC mode.
Step 9	`Router# show running-config`	Displays the current configuration for your verification.
Step 10	`Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Verifying the Configuration for Local Authentication Service

Use the **show running-config** command in global configuration mode to verify the current configuration for local authentication service.

SUMMARY STEPS

1. **enable**
2. **show running-config**

DETAILED STEPS

	Command	Purpose
Step 1	`Router> enable`	Enables privileged EXEC mode.
Step 2	`Router# show running-config`	Displays the current access point operating configuration

Monitoring and Maintaining 802.1X Local Authentication Service

To view statistics collected by the local authentication server, enter the following command in privileged EXEC mode:

```
Router# show radius local-server statistics
```

To reset local authentication server statistics to zero, enter the following command in privileged EXEC mode:

```
Router# clear radius local-server statistics
```

Configuration Examples for Remote Site IEEE 802.1X Local Authentication Service

This section provides the following configuration examples:

- Setting Up a Local Authentication Server: Example
- Setting Up Two Main Servers and a Local Authentication Server: Example
- Displaying Local Authentication Server Configuration: Example
- Displaying Local Authentication Server Statistics: Example

Setting Up a Local Authentication Server: Example

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

```
AP# configure terminal
AP(config)# aaa new-model
AP(config)# aaa group server radius RADIUS_SERVER_GROUP
AP(config-sg-radius)# server 10.0.0.1 auth-port 1812 acct-port 1813
AP(config)# aaa authentication login RADIUS_METHOD_LIST
AP(config)# radius-server host 10.0.0.1 auth-port 1812 acct-port 1813 key 110337
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 sam password rover32 group cashiers
AP(config-radsrv)# user patsy password crowder group cashiers
AP(config-radsrv)# user carl password 272165 group managers
AP(config-radsrv)# user vic password lid178 group managers
AP(config-radsrv)# end
```

Setting Up Two Main Servers and a Local Authentication Server: Example

This example shows how to set up two main servers and a local authentication server with a server deadtime of 10 minutes:

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

In this example, if the WAN link to the main servers fails, the access point or wireless-aware router completes these steps when a LEAP-enabled client device associates:

1. It tries the first server, times out multiple times, and marks the first server as dead.
2. It tries the second server, times out multiple times, and marks the second server as dead.
3. It tries and succeeds using the local authentication server.

If another client device needs to authenticate during the 10-minute deadtime interval, the access point skips the first two servers and tries the local authentication server first. After the deadtime interval, the access point tries to use the main servers for authentication. When setting a deadtime, you must balance the need to skip dead servers with the need to check the WAN link and begin using the main servers again as soon as possible.

Each time an access point or wireless-aware router tries to use the main servers while they are down, the client device that is trying to authenticate might report an authentication timeout. The client device retries and succeeds when the main servers time out and the access point or wireless-aware router tries the local authentication server. You can extend the timeout value on Cisco client devices to accommodate expected server timeouts.

Displaying Local Authentication Server Configuration: Example

The following is sample output for configuration of a local authentication server on the Cisco 2621 router.

```
2621-1# show run
Building configuration...

Current configuration : 2954 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2621-1
!
!
aaa new-model
!
!
aaa group server radius RADIUS_LEAP_GROUP
 server 10.0.0.1 auth-port 1812 acct-port 1813
!
aaa authentication login AUTH_LEAP group RADIUS_LEAP_GROUP
aaa session-id common
ip subnet-zero
!
!
ip dhcp pool 2621-dhcp-pool
   network 10.0.0.0 255.0.0.0
!
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
```

```
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
!
interface FastEthernet1/1
 switchport mode trunk
 no ip address
!
interface FastEthernet1/2
 no ip address
 shutdown
!
interface FastEthernet1/3
 no ip address
 shutdown
!
interface FastEthernet1/4
 no ip address
 shutdown
!
interface FastEthernet1/5
 no ip address
!
!
interface GigabitEthernet1/0
 no ip address
 shutdown
!
interface Vlan1
 ip address 10.0.0.1 255.0.0.0
!
ip classless
!
ip http server
no ip http secure-server
!
!
!
radius-server local
  nas 10.0.0.1 key 0 cisco
  user ap-1 nthash 7 101B2A415547345A5F25790801706510064152425325720D7D04075D523D4F780A
  user ap-5 nthash 7 144231535C540C7A77096016074B51332753030D0877705A264F450A09720A7307
  user user1 nthash 7 1350344A5B5C227B78057B10107A452232515402097C77002B544B45087D0E7200
!
radius-server host 10.0.0.1 auth-port 1812 acct-port 1813
radius-server key cisco
!
wlccp authentication-server infrastructure AUTH_LEAP
wlccp authentication-server client leap AUTH_LEAP
wlccp wds priority 255 interface Vlan1
!
line con 0
line aux 0
line vty 0 4
!
!
!
end
```

Displaying Local Authentication Server Statistics: Example

The following is sample output for configuration for the **show radius local-server statistics** command:

```
router-2621-1# show radius local-server statistics
Successes              : 11262       Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 8
Unknown NAS            : 0           Invalid packet from NAS: 0

NAS : 10.0.0.1
Successes              : 11262       Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 8
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

Maximum number of configurable users: 50, current user count: 11
Username                  Successes  Failures  Blocks
vayu-ap-1                      2235         0       0
vayu-ap-2                      2235         0       0
vayu-ap-3                      2246         0       0
vayu-ap-4                      2247         0       0
vayu-ap-5                      2247         0       0
vayu-11                           3         0       0
vayu-12                           5         0       0
vayu-13                           5         0       0
vayu-14                          30         0       0
vayu-15                           3         0       0
scm-test                          1         8       0

router-2621-1#
```

The first section shows cumulative statistics from the local authentication server. The second section shows statistics for each access point (NAS) that is authorized to use the local authentication server. The third section shows statistics for individual users. If a user is blocked and the lockout time is set to infinite, *Blocked* appears at the end of the line of statistics for that user. If the lockout time is not set to infinite, *Unblocked in x seconds* appears at the end of the statistics line for that user.

Additional References

Related Documents

Related Topic	Document Title
Comprehensive set of software configuration commands	*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*
Configuration commands for wireless roaming	*Configuring Fast Secure Roaming*

MIBs

MIB	MIBs Link
Non.	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

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 Remote Site IEEE 802.1X Local Authentication Service

Table 2 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 2 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.

Table 2 Feature Information for Remote Site IEEE 802.1X Local Authentication Service

Feature Name	Releases	Feature Information
Remote Site IEEE 802.1X Local Authentication Service	12.2(11)JA 12.3(11)T	The Remote Site IEEE 802.1X Local Authentication Service feature provides the ability to configure an access point or wireless-aware router to act as a local RADIUS server. Configuring local authentication service provides a backup authentication service in the event of a WAN link or server failure. This feature was introduced in Cisco IOS Release 12.2(11)JA on Cisco Aironet access points. This feature was integrated in Cisco IOS Release 12.3(11)T on the Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700 series, and Cisco 3800 series routers.