Configuring IPv6 WLAN Security

Prerequisites for IPv6 WLAN Security

A client VLAN must be mapped to the WLAN configured on the controller

Restrictions for IPv6 WLAN Security

RADIUS Server Support

- If multiple RADIUS servers are configured for redundancy, the user database must be identical in all the servers for the backup to work properly.

Radius ACS Support

- You must configure RADIUS on both your Cisco Secure Access Control Server (ACS) and your controller
- RADIUS is supported on Cisco Secure ACS version 3.2 and later releases.

Information About IPv6 WLAN Security

Information About RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol that provides centralized security for users attempting to gain management access to a network. It serves as a back-end database similar to Local EAP and provides authentication and accounting services.

- Authentication—The process of verifying users when they attempt to log into the controller

  Users must enter a valid username and password for the controller to authenticate users to the RADIUS server. If multiple databases are configured, then specify the sequence in which the backend database must be tried.

- Accounting— The process of recording user actions and changes.

  Whenever a user successfully executes an action, the RADIUS accounting server logs the changed attributes, the user ID of the person who made the change, the remote host where the user is logged in, the date and time when the command was executed, the authorization level of the user, and a description of the action performed and the values provided. If the RADIUS accounting server is unreachable, the users can continue their sessions uninterrupted.

User Datagram Protocol— RADIUS uses User Datagram Protocol (UDP) for its transport. It maintains a database and listens on UDP port 1812 for incoming authentication requests and UDP port 1813 for incoming accounting requests. The controller, which requires access control, acts as the client and requests AAA services from the server. The traffic between the controller and the server is encrypted by an algorithm defined in the protocol and a shared secret key configured on both devices.

Configures multiple RADIUS accounting and authentication servers. For example, you can have one central RADIUS authentication server but several RADIUS accounting servers in different regions. If you configure multiple servers of the same type and the first one fails or becomes unreachable, the controller automatically tries the second one, then the third one if necessary, and so on.

When RADIUS method is configured for the WLAN, the controller will use the RADIUS method configured for the WLAN. When the WLAN is configured to use local EAP, the RADIUS method configured on the WLAN points to Local. The WLAN must also be configured with the name of the local EAP profile to use.

If no RADIUS method is configured in the WLAN, the controller will use the default RADIUS method defined in global mode.

Information About Local EAP

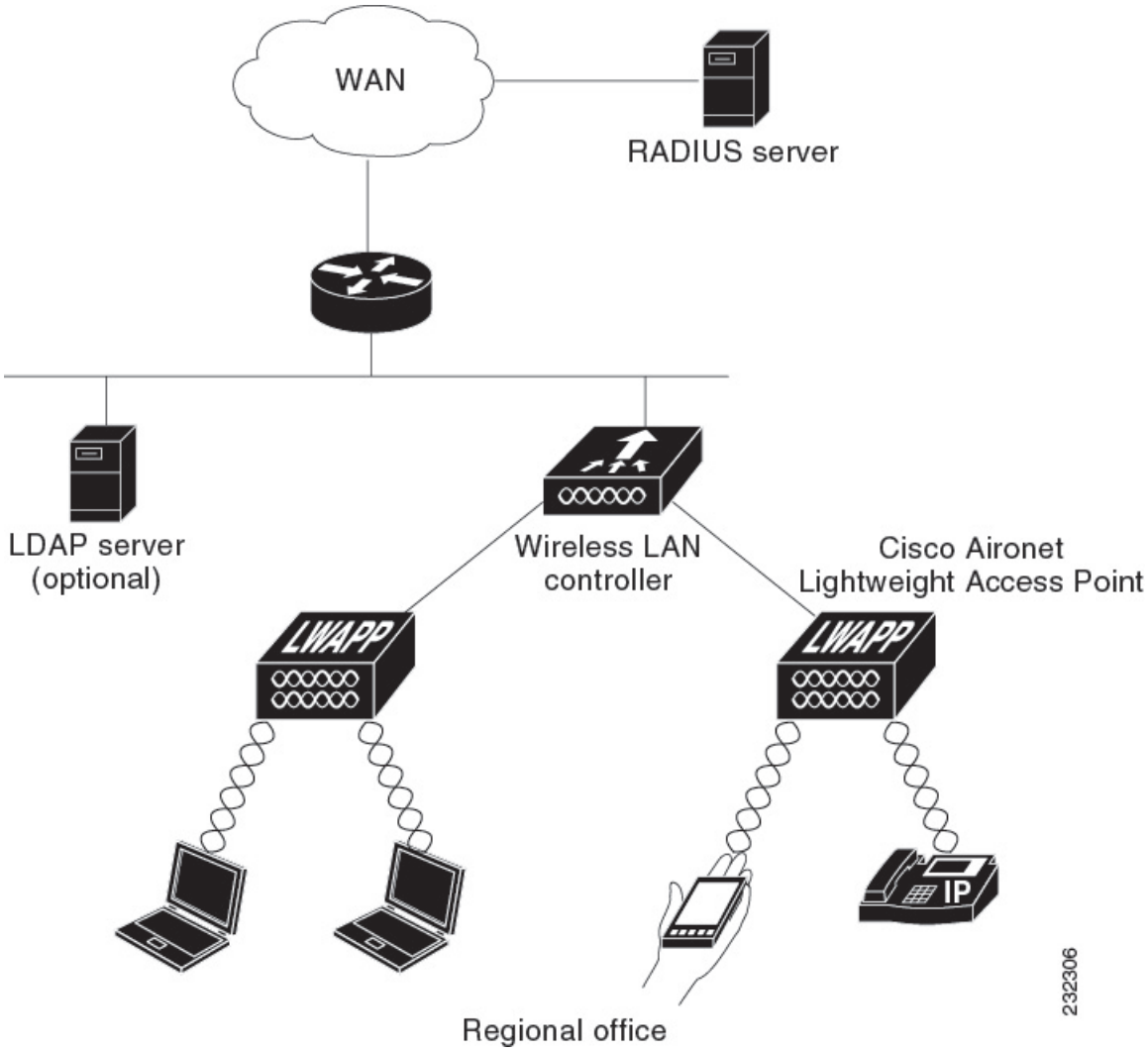
Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that maintain connectivity to wireless clients when the back-end system is disrupted or the external authentication server goes down. When you enable local EAP, the controller serves as the authentication server and the local user database, which removes dependence on an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP back-end database to authenticate users. Local EAP supports LEAP, EAP-FAST, EAP-TLS, PEAPv0/MSCHAPv2, and PEAPv1/GTC authentication between the controller and wireless clients.

Without an EAP profile name being provided, or if a name was provided for an EAP profile that does not exist, then EAP by default allows no EAP method for local authentication.

Note The LDAP back-end database supports these local EAP methods: EAP-TLS, EAP-FAST/GTC, and PEAPv1/GTC. LEAP, EAP-FAST/MSCHAPv2, and PEAPv0. MSCHAPv2 is supported only if the LDAP server is set up to return a clear-text password.

Note Controller support Local EAP authentication against external LDAP databases such as Microsoft Active Directory and Novell's eDirectory. For more information about configuring the controller for Local EAP authentication against Novell's eDirectory, see the Configure Unified Wireless Network for Authentication Against Novell's eDirectory Database whitepaper.

Figure 1: Local EAP Example



Related Topics

Creating a Local User, on page 4
Creating an Client VLAN and Interface, on page 4
Configuring an EAP Profile, on page 6
Creating a Client VLAN, on page 18
Creating 802.1x WLAN Using an External RADIUS Server, on page 19

How to Configure IPv6 WLAN Security

Configuring Local Authentication

Creating a Local User

SUMMARY STEPS

1. configure terminal
2. username aaa_test
3. password 0 aaa_test
4. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global command mode.
Step 2	**username aaa_test** **Example:** `Controller(config)# username aaa_test`	Creates a username.
Step 3	**password 0 aaa_test** **Example:** `Controller(config)# usernameaaa_test password 0 aaa_test`	Assigns a password for the username.
Step 4	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit the global configuration mode.

```
Controller# configure terminal
Controller(config)# username aaa_test password 0 aaa_test
Controller(config)# end
```

Related Topics

Information About IPv6 WLAN Security, on page 1

Creating an Client VLAN and Interface

SUMMARY STEPS

1. configure terminal

2. **vlan**
3. **exit**
4. **interface vlan `vlan_ID`**
5. **ip address**
6. **ipv6 address**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global command mode.
Step 2	**vlan** **Example:** `Controller(config)# vlan 137`	Creates a VLAN.
Step 3	**exit** **Example:** `Controller (config-vlan)# exit`	Exits VLAN configuration mode.
Step 4	**interface vlan `vlan_ID`** **Example:** `Controller (config)# interface vlan 137`	Associates the VLAN to an interface.
Step 5	**ip address** **Example:** `Controller(config-if)# ip address 10.7.137.10 255.255.255.0`	Assigns an IP address to the VLAN interface.
Step 6	**ipv6 address** **Example:** `Controller(config-if)#ipv6 address 2001:db8::20:1/64`	Assigns an IPv6 address to the VLAN interface.
Step 7	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit the global configuration mode.

Example

```
Controller# configure terminal
Controller(config)# vlan 137
Controller(config-vlan)#exit
Controller(config)#interface vlan 137
Controller(config-if)#ip address 10.7.137.10 255.255.255.0
```

```
Controller(config-if)#ipv6 address 2001:db8::20:1/64
Controller(config-if)#end
```

Related Topics

Information About IPv6 WLAN Security, on page 1

Configuring an EAP Profile

SUMMARY STEPS

1. **eap profile name**
2. **method leap**
3. **method tls**
4. **method peap**
5. **method fast**
6. **method mschapv2**
7. **method md5**
8. **method gtc**
9. **method fast profile my-fast**
10. **description my_local eap profile**
11. **exit**
12. **eap method fast profile myFast**
13. **authority-id** [identity|information]
14. **local-key 0 key-name**
15. **pac-password 0 password**
16. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**eap profile name** **Example:** `Controller(config)# eap profile wcm_eap_prof`	Creates an EAP profile.
Step 2	**method leap** **Example:** `Controller(config-eap-profile)# method leap`	Configures EAP-LEAP method on the profile.
Step 3	**method tls** **Example:** `Controller(config-eap-profile)# method tls`	Configures EAP-TLS method on the profile.
Step 4	**method peap** **Example:** `Controller(config-eap-profile)# method peap`	Configures PEAP method on the profile.

	Command or Action	Purpose
Step 5	**method fast** **Example:** `Controller(config-eap-profile)# method fast`	Configures EAP-FAST method on the profile.
Step 6	**method mschapv2** **Example:** `Controller(config-eap-profile)# method mschapv2`	Configures EAP-MSCHAPV2 method on the profile.
Step 7	**method md5** **Example:** `Controller(config-eap-profile)# method md5`	Configures EAP-MD5 method on the profile.
Step 8	**method gtc** **Example:** `Controller(config-eap-profile)# method gtc`	Configures EAP-GTC method on the profile.

Step 9	**method fast profile my-fast**
	Example:
	`Controller(config-eap-profile)# eap method fast profile my-fast`
	`Controller (config-eap-profile)#description my_local eap profile`
		Creates a EAP profile named my-fast.

Step 10	**description my_local eap profile** **Example:** `Controller (config-eap-profile)#description my_local eap profile`	Provides a description for the local profile.
Step 11	**exit** **Example:** `Controller (config-eap-profile)# exit`	Exits the eap-profile configuration mode.
Step 12	**eap method fast profile myFast** **Example:** `Controller (config)# eap method fast profile myFast`	Configures the EAP method profile.

Step 13	**authority-id** `[identity|information]`
	Example:
	`Controller(config-eap-method-profile)# authority-id identity my_identity`
	`Controller(config-eap-method-profile)#authority-id information my_information`
		Configure the authority ID and information for the EAP method profile.

Step 14	**local-key 0 key-name** **Example:**	Configures the local server key.

	Command or Action	Purpose
	`Controller(config-eap-method-profile)# local-key 0 test`	
Step 15	**pac-password 0 password** **Example:** `Controller(config-eap-method-profile)# pac-password 0 test`	Configures the PAC password for manual PAC provisioning.
Step 16	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit the global configuration mode.

Example

```
Controller(config)#eap profile wcm_eap_prof
Controller(config-eap-profile)#method leap
Controller(config-eap-profile)#method tls
Controller(config-eap-profile)#method peap

Controller(config-eap-profile)#method mschapv2
Controller(config-eap-profile)#method md5
Controller(config-eap-profile)#method gtc
Controller(config-eap-profile)#eap method fast profile my-fast

Controller (config-eap-profile)#description my_local eap profile
Controller(config-eap-profile)# exit
Controller (config)# eap method fast profile myFast
Controller(config-eap-method-profile)#authority-id identity my_identity
Controller(config-eap-method-profile)#authority-id information my_information
Controller(config-eap-method-profile)#local-key 0 test
Controller(config-eap-method-profile)#pac-password 0 test
Controller(config-eap-method-profile)# end
```

Related Topics

Information About IPv6 WLAN Security, on page 1

Creating a Local Authentication Model

SUMMARY STEPS

1. **aaa new-model**
2. **authentication dot1x default local**
3. **dot1x method_list local**
4. **aaa authentication dot1x dot1x_name local**
5. **aaa authorization credential-download name local**
6. **aaa local authentication auth-name authorization authorization-name**
7. **session ID**
8. **dot1x system-auth-control**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**aaa new-model** **Example:** `Controller(config)# aaa new-model`	Creates a AAA authentication model.
Step 2	**authentication dot1x default local** **Example:** `Controller(config)# aaa authentication dot1x default local`	Implies that the dot1x must use the default local RADIUS when no other method is found.
Step 3	**dot1x method_list local** **Example:** `Controller(config)# aaa authentication dot1x wcm_local local`	Assigns the local authentication for wcm_local method list.
Step 4	**aaa authentication dot1x dot1x_name local** **Example:** `Controller(config)# aaa authentication dot1x aaa_auth local`	Configures the local authentication for the dot1x method.
Step 5	**aaa authorization credential-download name local** **Example:** `Controller(config)# aaa authorization credential-download wcm_author local`	Configures local database to download EAP credentials from Local/RADIUS/LDAP.
Step 6	**aaa local authentication auth-name authorization authorization-name** **Example:** `Controller(config)# aaa local authentication wcm_local authorization wcm_author`	Selects local authentication and authorization.
Step 7	**session ID** **Example:** `Controller(config)# aaa session-id common`	Configures a session ID for AAA.
Step 8	**dot1x system-auth-control** **Example:** `Controller(config)# dot1x system-auth-control`	Enables dot.1x system authentication control.

Example

```
Controller(config)# aaa new-model
Controller(config)# aaa authentication dot1x default local
Controller(config)# aaa authentication dot1x wcm-local local
Controller(config)# aaa authentication dot1x aaa_auth local
Controller(config)# aaa authorization credential-download wcm_author local
```

```
Controller(config)# aaa local authentication wcm_local authorization wcm_author
Controller(config)# aaa session-id common
Controller(config)# dot1x system-auth-control
```

Creating a Client WLAN

Note This example uses 802.1x with dynamic WEP. You can use any other security mechanism supported by the wireless client and configurable on the controller

SUMMARY STEPS

1. **configure terminal**
2. **wlan `wlan name` <identifier> `SSID`**
3. **broadcast-ssid**
4. **no security wpa**
5. **security dot1x**
6. **security** dot1x authentication-list *wcm-local*
7. **local-auth `wcm_eap_prof`**
8. **client vlan** *137*
9. **no shutdown**
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global command mode.
Step 2	**wlan `wlan name` <identifier> `SSID`** **Example:** `Controller(config)# wlan wlanProfileName 1 ngwcSSID`	Creates a WLAN.
Step 3	**broadcast-ssid** **Example:** `Controller(config-wlan)# broadcast-ssid`	Configures to broadcast the SSID on a WLAN.
Step 4	**no security wpa** **Example:** `Controller(config-wlan)# no security wpa`	Disables the wpa for WLAN to enable 802.1x.
Step 5	**security dot1x** **Example:** `Controller(config-wlan)# security dot1x`	Configures the 802.1x encryption security for the WLAN.

	Command or Action	Purpose
Step 6	**security** dot1x authentication-list *wcm-local* **Example:** `Controller(config-wlan)# security dot1x authentication-list wcm-local`	Configures the server group mapping to the WLAN for dot1x authentication.
Step 7	**local-auth wcm_eap_prof** **Example:** `Controller (config-wlan)# local-auth wcm_eap_profile`	Configures the eap profile on the WLAN for local authentication.
Step 8	**client vlan** *137* **Example:** `Controller(config-wlan)# client vlan 137`	Associates the VLAN to a WLAN.
Step 9	**no shutdown** **Example:** `Controller(config-wlan)# no shutdown`	Enables the WLAN.
Step 10	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit the global configuration mode.

Example

```
Controller# config terminal
Controller(config)#wlan wlanProfileName 1 ngwcSSID
Controller(config-wlan)#broadcast-ssid
Controller(config-wlan)#no security wpa
Controller(config-wlan)#security dot1x
Controller(config-wlan)#security dot1x authentication-list wcm-local
Controller (config-wlan)# local-auth wcm_eap_prof
Controller(config-wlan)#client vlan 137
Controller(config-wlan)#no shutdown
Controller(config-wlan)#end
Controller#
```

Related Topics

Creating Client VLAN for WPA2+AES, on page 13

Configuring Local Authentication with WPA2+AES

SUMMARY STEPS

1. **configure terminal**
2. **aaa new model**
3. **dot1x system-auth-control**
4. **aaa authentication dot1x default local**
5. **aaa local authorization credential-download default local**

6. **aaa local authentication default authorization default**
7. **eap profile wcm_eap_profile**
8. **method leap**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global command mode.
Step 2	**aaa new model** **Example:** `Controller(config)# aaa new-model`	Creates a AAA authentication model.
Step 3	**dot1x system-auth-control** **Example:** `Controller(config)# dot1x system-auth-control`	Enables dot1x system authentication control.
Step 4	**aaa authentication dot1x default local** **Example:** `Controller(config)# aaa authentication dot1x default local`	Configures the local authentication for the default dot1x method.
Step 5	**aaa local authorization credential-download default local** **Example:** `Controller(config)# aaa authorization credential-download default local`	Configures default database to download EAP credentials from local server.
Step 6	**aaa local authentication default authorization default** **Example:** `Controller(config)# aaa local authentication default authorization default`	Selects the default local authentication and authorization.
Step 7	**eap profile wcm_eap_profile** **Example:** `Controller(config)#eap profile wcm_eap_profile`	Creates an EAP profile.
Step 8	**method leap** **Example:** `Controller(config)# method leap`	Configures EAP-LEAP method on the profile.
Step 9	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit the global configuration mode.

```
Controller# configure terminal
Controller(config)# aaa new-model
Controller(config)# dot1x system-auth-control
Controller(config)# aaa authentication dot1x default local
Controller(config)# aaa authorization credential-download default local
Controller(config)# aaa local authentication default authorization default
Controller(config)#eap profile wcm_eap_profile
Controller(config)# method leap
Controller(config)# end
```

Creating Client VLAN for WPA2+AES

Create a VLAN for the WPA2+AES type of local authentication. This VLAN is later mapped to a WLAN.

SUMMARY STEPS

1. **configure terminal**
2. **vlan** **vlan_ID**
3. **exit**
4. **interface** vlan **vlan_ID**
5. **ip address**
6. **ipv6 address**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global command mode.
Step 2	**vlan** **vlan_ID** **Example:** `Controller (config)# vlan 105`	Creates a VLAN.
Step 3	**exit** **Example:** `Controller (config-vlan)# exit`	Exits from the VLAN mode.
Step 4	**interface** vlan **vlan_ID** **Example:** `Controller(config)# interface vlan 105`	Associates the VLAN to the interface.
Step 5	**ip address** **Example:** `Controller(config-if)# ip address 10.8.105.10 255.255.255.0`	Assigns IP address to the VLAN interface.
Step 6	**ipv6 address** **Example:**	Assigns IPv6 address to the VLAN interface.

	Command or Action	Purpose
	`Controller(config-if)#ipv6 address 2001:db8::10:1/64`	
Step 7	**exit** **Example:** `Controller (config-if)# exit`	Exits from the interface mode.

```
Controller# configure terminal
Controller(config)# vlan105
Controller (config-vlan)# exit
Controller (config)# interface vlan 105
Controller(config-if)#ip address 10.8.105.10 255.255.255.0
Controller(config-if)#ipv6 address 2001:db8::10:1/64
Controller(config-if)#exit
Controller(config)#
```

Related Topics

Creating a Client WLAN , on page 10

Creating WLAN for WPA2+AES

Create a WLAN and map it to the client VLAN created for WPA2+AES.

SUMMARY STEPS

1. **configure terminal**
2. **wlan wpas2-aes-wlan 1 wpas2-aes-wlan**
3. **client vlan 105**
4. **local-auth wcm_eap_profile**
5. **security dot1x authentication-list default**
6. **no shutdown**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global command mode.

Step 2	**wlan wpas2-aes-wlan 1 wpas2-aes-wlan**
	Example:
	`Controller(config)#wlan wpa2-aes-wlan 1 wpa2-aes-wlan`
	`Controller(config-wlan)#`
		Creates a WLAN.

Step 3	**client vlan 105** **Example:**	Maps the WLAN to the client VLAN.

	Command or Action	Purpose
	`Controller(config-wlan)#client vlan 105` `Controller(config-wlan)#`	
Step 4	**local-auth wcm_eap_profile** **Example:** `Controller(config-wlan)#local-auth wcm_eap_profile`	Creates and sets the EAP profile on the WLAN.
Step 5	**security dot1x authentication-list default** **Example:** `Controller(config-wlan)#security dot1x authentication-list default`	Uses the default dot1x authentication list.

Step 6	**no shutdown**
	Example:
	`Controller(config-wlan)#no shutdown`
	`Controller(config-wlan)#`
		Enables the WLAN.

Step 7	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

```
Controller# configure terminal
Controller(config)#wlan wpa2-aes-wlan 1 wpa2-aes-wlan
Controller(config-wlan)#client vlan 105
Controller(config-wlan)#local-auth wcm_eap_profile
Controller(config-wlan)#security dot1x authentication-list default
Controller(config-wlan)#no shutdown
Controller(config-wlan)# exit
```

Configuring External RADIUS Server

Configuring RADIUS Authentication Server Host

SUMMARY STEPS

1. **configure terminal**
2. **radius server One**
3. **address ipv4 address auth-portauth_port_number acct-port acct_port_number**
4. **address ipv6 address auth-portauth_port_number acct-port acct_port_number**
5. **key 0cisco**
6.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global command mode.

	Command or Action	Purpose
	`Controller# configure terminal`	
Step 2	**radius server One** **Example:** `Controller (config)# radius server One`	Creates a radius server.
Step 3	**address ipv4 address auth-portauth_port_number acct-port acct_port_number** **Example:** `Controller (config-radius-server)# address ipv4 10.10.10.10 auth-port 1812 acct-port 1813`	Configures the IPv4 address for the radius server.
Step 4	**address ipv6 address auth-portauth_port_number acct-port acct_port_number** **Example:** `Controller (config-radius-server)# address ipv6 2001:db8::25:2 auth-port 1812 acct-port 1813`	Configures the IPv6 address for the radius server.
Step 5	**key 0cisco** **Example:** `Controller (config-radius-server)# key 0 cisco`	**exit**
Step 6	**Example:** `Controller (config-radius-server)# exit`	Exits from the radius server mode.

```
Controller# configure terminal
Controller (config)# radius server One
Controller (config-radius-server)# address ipv4 10.10.10.10 auth-port 1812 acct-port 1813
Controller (config-radius-server)# address ipv6 2001:db8::25:2 auth-port 1812 acct-port
1813
Controller (config-radius-server)# key 0 cisco
Controller (config-radius-server)#exit
```

Related Topics

Configuring RADIUS Authentication Server Group , on page 16

Configuring RADIUS Authentication Server Group

SUMMARY STEPS

1. **configure terminal**
2. **aaa new-model**
3. **aaa group server radius wcm_rad**
4. **server <ip address>auth-port1812acct-port1813**
5. **aaa authentication dot1x method_list group wcm_rad**
6. **dot1x system-auth-control**
7. **aaa session-idcommon**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global command mode.
Step 2	**aaa new-model** **Example:** `Controller(config)#aaa new-model`	Creates a AAA authentication model.

Step 3	**aaa group server radius wcm_rad**
	Example:
	`Controller(config)# aaa group server radius wcm_rad`
	`Controller(config-sg-radius)#`
		Creates an radius server-group.

Step 4	**server <ip address>auth-port1812acct-port1813**
	Example:
	`Controller(config-sg-radius)# server One auth-port 1812 acct-port 1813`
	`Controller(config-sg-radius)# server Two auth-port 1812 acct-port 1813`
	`Controller(config-sg-radius)# server Three auth-port 1812 acct-port 1813`
		Adds servers to the radius group created in Step 3. Configures the UDP port for RADIUS accounting server and authentication server.

Step 5	**aaa authentication dot1x method_list group wcm_rad** **Example:** `Controller(config)# aaa authentication dot1x method_list group wcm_rad`	Maps the method list to the radius group.
Step 6	**dot1x system-auth-control** **Example:** `Controller(config)# dot1x system-auth-control`	Enables the system authorization control for the radius group.
Step 7	**aaa session-idcommon** **Example:** `Controller(config)# aaa session-id common`	Ensures that all session IDs information sent out, from the radius group, for a given call are identical.

```
Controller# configure terminal
Controller(config)# aaa new-model
Controller(config)# aaa group server radius wcm_rad
Controller(config-sg-radius)# server One auth-port 1812 acct-port 1813
Controller(config-sg-radius)# server Two auth-port 1812 acct-port 1813
Controller(config-sg-radius)# server Three auth-port 1812 acct-port 1813
Controller(config)# aaa authentication dot1x method_list group wcm_rad
Controller(config)# dot1x system-auth-control
Controller(config)# aaa session-id common
Controller(config)#
```

Related Topics

Configuring RADIUS Authentication Server Host , on page 15

Creating a Client VLAN

SUMMARY STEPS

1. **configure terminal**
2. **vlan 137**
3. **exit**
4. **interface vlan 137**
5. **ip address 10.7.137.10 255.255.255.0**
6. **ipv6 address 2001:db8::30:1/64**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global command mode.
Step 2	**vlan 137** **Example:** `Controller(config)# vlan 137`	Creates a VLAN and associate it to the interface.
Step 3	**exit** **Example:** `Controller (config-vlan)# exit`	Exits from the VLAN mode.
Step 4	**interface vlan 137** **Example:** `Controller (config)# interface vlan 137`	Assigns a VLAN to an interface.
Step 5	**ip address 10.7.137.10 255.255.255.0** **Example:** `Controller(config-if)# ip address 10.7.137.10 255.255.255.0`	Assigns an IPv4 address to the VLAN interface.
Step 6	**ipv6 address 2001:db8::30:1/64** **Example:** `Controller(config-if)# ipv6 address 2001:db8::30:1/64`	Assigns an IPv6 address to the VLAN interface.
Step 7	**end** **Example:**	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

	Command or Action	Purpose
	`Controller(config)# end`	

```
Controller# configure terminal
Controller(config)# vlan137
Controller(config-vlan)# exit
Controller(config)# interface vlan137
Controller(config-if)# ip address 10.7.137.10 255.255.255.0
Controller(config-if)# ipv6 address 2001:db8::30:1/64
Controller(config-if)# end
```

Related Topics

Information About IPv6 WLAN Security, on page 1
Creating 802.1x WLAN Using an External RADIUS Server, on page 19

Creating 802.1x WLAN Using an External RADIUS Server

SUMMARY STEPS

1. **configure terminal**
2. **wlan ngwc-1x<ssid>ngwc-1x**
3. **broadcast-ssid**
4. **no security wpa**
5. **security dot1x**
6. **security dot1x authentication-list wcm-rad**
7. **client vlan 137**
8. **no shutdown**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global command mode.
Step 2	**wlan ngwc-1x<ssid>ngwc-1x** **Example:** `Controller(config)# wlan ngwc_8021x 2 ngwc_8021x`	Creates a new WLAN for 802.1x authentication.
Step 3	**broadcast-ssid** **Example:** `Controller(config-wlan)# broadcast-ssid`	Configures to broadcast the SSID on WLAN.
Step 4	**no security wpa** **Example:** `Controller(config-wlan)# no security wpa`	Disables the WPA for WLAN to enable 802.1x.

	Command or Action	Purpose
Step 5	**security dot1x** **Example:** `Controller(config-wlan)# security dot1x`	Configures the 802.1x encryption security for the WLAN.
Step 6	**security dot1x authentication-list wcm-rad** **Example:** `Controller(config-wlan)# security dot1x authentication-list wcm-rad`	Configures the server group mapping to the WLAN for dot1x authentication.
Step 7	**client vlan 137** **Example:** `Controller(config-wlan)# client vlan 137`	Associates the VLAN to a WLAN.
Step 8	**no shutdown** **Example:** `Controller(config-wlan)# no shutdown`	Enables the WLAN.
Step 9	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit the global configuration mode.

Example

```
Controller# configure terminal
Controller(config)#wlan ngwc_8021x 2 ngwc_8021x
Controller(config-wlan)# broadcast-ssid
Controller(config-wlan)# no security wpa
Controller(config-wlan)# security dot1x
Controller(config-wlan)# security dot1x authentication-list wcm-rad
Controller(config-wlan)# client vlan 137
Controller(config-wlan)# no shutdown
Controller(config-wlan)# end
```

Related Topics

Creating a Client VLAN, on page 18
Information About IPv6 WLAN Security, on page 1

Additional References

Related Documents

Related Topic	Document Title
IPv6 command reference	*IPv6 Command Reference (Catalyst 3850 Switches)IPv6 Command Reference (Cisco WLC 5700 Series)IPv6 Command Reference (Catalyst 3650 Switches)*

Related Topic	Document Title
WLAN command reference	*WLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*
WLAN configuration	*WLAN Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)WLAN Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)WLAN Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for IPv6 WLAN Security

This table lists the features in this module and provides links to specific configuration information:

Feature	Release	Modification
IPv6 WLAN Security Functionality	Cisco IOS XE 3.2SECisco IOS XE 3.3SECisco IOS XE 3.3SE	This feature was introduced.