Remote LANs

Information About Remote LANs

A Remote LAN (RLAN) is used for authenticating wired clients using the controller. Once the wired client successfully joins the controller, the LAN ports switch the traffic between central or local switching modes. The traffic from wired client is treated as wireless client traffic.

The RLAN in Access Point (AP) sends the authentication request to authenticate the wired client. The authentication of wired client in RLAN is similar to the central authenticated wireless client.

The supported AP models are:

- Cisco Catalyst 9124 Series Access Points
- Cisco Catalyst 9105AXW
- Cisco Aironet OEAP 1810 series
- Cisco Aironet 1815T series
- Cisco Aironet 1810W series
- Cisco Aironet 1815W
- Cisco Catalyst IW6300 Heavy Duty Series Access Points
- Cisco 6300 Series Embedded Services Access Points

Information About Ethernet (AUX) Port

The second Ethernet port in Cisco Aironet 1850, 2800, and 3800 Series APs is used as a link aggregation (LAG) port, by default. It is possible to use this LAG port as an RLAN port when LAG is disabled.

The following APs use LAG port as an RLAN port:

- 1852E
- 1852I
- 2802E
- 2802I
- 3802E
- 3802I
- 3802P
- 4802

Limitation for RLAN

- RLAN supports only a maximum of four wired clients regardless of the AP model.
- RLAN support with Virtual Routing and Forwarding (VRF) is not available.

Limitations for Using AUX port in Cisco 2700 Access Points

- RLAN supports AUX port and non-native VLAN for this port.
- Local mode supports wired client traffic on central switch. Whereas, FlexConnect mode does not support central switch.
- FlexConnect mode supports wired client traffic on local switch and not on central switch.
- AUX port cannot be used as a trunk port. Even switches or bridges cannot be added behind the port.
- AUX port does not support dot1x.

Role of Controller

- The controller acts as an authenticator, and Extensible Authentication Protocol (EAP) over LAN (EAPOL) messages from the wired client reaching the controller through an AP.
- The controller communicates with the configured Authentication, Authorization, and Accounting (AAA) server.
- The controller configures the LAN ports for an AP and pushes them to the corresponding AP.

Note

- The RLAN feature is supported on Fabric.
- RLAN is supported in APs that have more than one Ethernet port.
- In RLAN (local mode - local switching mode), if you want to use the AP native VLAN for client IP, the VLAN should be configured as either **no vlan** or **vlan 1** in the RLAN policy profile. For example, if the native VLAN ID is 80, do not use the number 80 in the RLAN policy profile. Also, do not use VLAN name *VLANxxxx* to configure VLAN in the RLAN policy profile.

  When a new client is connected to an AP, the client's details are available in the controller initially. However, after the CAPWAP DOWN/UP state, the client details are no longer listed in the controller.
- APs in local mode central switching do not support VLAN tagged traffic from RLAN clients, and the traffic gets dropped.
- The VLAN name (without any numerals) configured in remote-lan-policy does not provide the mapped VLAN ID for central switching.

Configuring Remote LANs (RLANs)

Enabling or Disabling all RLANs

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	[**no**] **ap remote-lan shutdown** **Example:** `Device(config)# [no] ap remote-lan shutdown`	Enables or disables all RLANs.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating RLAN Profile (GUI)

Procedure

Step 1 Choose **Configuration > Tags & Profiles > Remote LAN**.

Step 2 Click **Add**.

Step 3 Enter the **Profile Name**, **RLAN ID** and enable or disable the **Status** toggle button. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 Click **Apply to Device**.

Creating RLAN Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap remote-lan profile-name** *remote-lan-profile-name rlan-id* **Example:** `Device(config)# ap remote-lan profile-name rlan_profile_name 3`	Configures remote LAN profile. • *remote-lan-profile*—Is the remote LAN profile name. Range is from 1 to 32 alphanumeric characters. • *rlan-id*—Is the remote LAN identifier. Range is from 1 to 128. **Note** You can create a maximum of 128 RLANs. You cannot use the *rlan-id* of an existing RLAN while creating another RLAN. Both RLAN and WLAN profile cannot have the same names. Similarly, RLAN and WLAN policy profile cannot have the same names.

Configuring RLAN Profile Parameters (GUI)

Procedure

Step 1 Choose **Configuration > Tags & Profiles > Remote LAN**.

Step 2 On the **RLAN Profile** tab, click **Add**.

The **Add RLAN Profile** window is displayed.

Step 3 In the **General** tab:

a) Enter a **Name** and **RLAN ID** for the RLAN profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

b) Set the number of client connections per RLAN in the **Client Association Limit** field.

The range depends on the maximum number of clients supported by the platform.

c) To enable the profile, set the status as **Enable**.

Step 4 In the **Security** > **Layer2** tab

a) To enable 802.1x for an RLAN, set the **802.1x** status as **Enabled**.

Note You can activate either web or 802.1x authentication list at a time.

b) Choose the authorization list name from the **MAC Filtering** drop-down list.

c) Choose the 802.1x for an RLAN authentication list name from the **Authentication List** drop-down list.

Step 5 In the **Security** > **Layer3** tab

a) To enable web authentication for an RLAN, set the **Web Auth** status as **Enabled**.

Note You can activate either web or 802.1x authentication list at a time.

b) Choose the web authentication parameter map from the **Webauth Parameter Map** drop-down list.

c) Choose the web authentication list name from the **Authentication List** drop-down list.

Step 6 In the **Security** > **AAA** tab

a) Set the **Local EAP Authentication** to enabled. Also, choose the required **EAP Profile Name** from the drop-down list.

Step 7 Save the configuration.

Configuring RLAN Profile Parameters (CLI)

Before you begin

The configurations in this section are not mandatory for an RLAN profile.

In case of central switching mode, you need to configure both central switching and central DHCP.

Note The fabric profile configuration is required only for fabric RLAN support.

Procedure

	Command or Action	Purpose
Step 1	**client association limit** *client-connections* **Example:** `Device(config-remote-lan)# client association limit 1`	Configures client connections per RLAN. *client-connections*—Is the maximum client connections per RLAN. Range is from 0 to 10000. 0 refers to unlimited.
Step 2	**fabric-profile** *fabric-profile-name* **Example:** `Device(config-remote-lan)# fabric-profile sample-fabric-profile-name`	Configures fabric profile for RLAN.
Step 3	**ip access-group web** *IPv4-acl-name* **Example:** `Device(config-remote-lan)# ip access-group web acl_name`	Configures RLAN IP configuration commands. *IPv4-acl-name*—Refers to the IPv4 ACL name or ID.
Step 4	**local-auth** *profile name* **Example:** `Device(config-remote-lan)# local-auth profile_name`	Sets EAP Profile on an RLAN. *profile name*—Is the EAP profile on an RLAN.
Step 5	**mac-filtering** *mac-filter-name* **Example:** `Device(config-remote-lan)# mac-filtering mac_filter`	Sets MAC filtering support on an RLAN. *mac-filter-name*—Is the authorization list name.
Step 6	**security dot1x authentication-list** *list-name* **Example:** `Device(config-remote-lan)# security dot1x authentication-list dot1_auth_list`	Configures 802.1X for an RLAN. *list-name*—Is the authentication list name.
Step 7	**security web-auth authentication-list** *list-name* **Example:** `Device(config-remote-lan)# security web-auth authentication-list web_auth_list`	Configures web authentication for an RLAN. *list-name*—Is the authentication list name. **Note** You can activate either web or dot1x authentication list at a time.
Step 8	[**no**] **shutdown** **Example:** `Device(config-remote-lan)# shutdown`	Enables or disables RLAN profile.
Step 9	**end** **Example:** `Device(config-remote-lan)# end`	Returns to privileged EXEC mode.

Creating RLAN Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Remote LAN** > **RLAN Policy**

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Policy Name**.

Step 4 Click **Apply to Device**.

Creating RLAN Policy Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap remote-lan-policy policy-name** *profile name* **Example:** `Device(config)# ap remote-lan-policy policy-name rlan_policy_prof_name`	Configures RLAN policy profile and enters wireless policy configuration mode.

Configuring RLAN Policy Profile Parameters (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Remote LAN**.

Step 2 On the **Remote LAN** page, click **RLAN Policy** tab.

Step 3 On the **RLAN Policy** page, click the name of the **Policy** or click **Add** to create a new one.

The **Add/Edit RLAN Policy** window is displayed.

Step 4 In the **General** tab:

a) Enter a **Name** and **Description** for the policy profile.
b) Set **Central Authentication** to **Enabled** state.
c) Set **Central DHCP** to **Enabled** state.
d) Set the **PoE** check box to enable or disable state.
e) To enable the policy, set the status as **Enable**.

Step 5 In the **Access Policies** Tab, choose the VLAN name or number from the **VLAN** drop-down list.

Note When central switching is disabled, the VLAN in the RLAN policy cannot be configured as the AP's native VLAN. To use the AP's native VLAN for client IP, the VLAN should be configured as either **no vlan** or **vlan 1** in the RLAN policy profile.

Step 6 From the **Host Mode** drop-down list, choose the **Host Mode** for the remote-LAN802.1x from the following options:

- Single-Host Mode—Is the default host mode. In this mode, the switch port allows only a single host to be authenticated and passes traffic one by one.
- Multi-Host Mode—The first device to authenticate opens up to the switch port, so that all other devices can use the port. You need not authenticate other devices independently, if the authenticated device becomes authorized the switch port is closed.
- Multi-Domain Mode—The authenticator allows one host from the data domain and another from the voice domain. This is a typical configuration on switch ports with IP phones connected.

Note
- For an RLAN profile with open-auth configuration, you must map the RLAN-policy with single host mode. Mapping RLAN-policy with multi-host or multi-domain mode is not supported.
- The controller does not assign data versus voice VLAN, based on traffic. RLAN only supports multiple VLAN assignments through 802.1x AAA override. You must create data and voice VLANs and then assign these VLANs to respective clients, based on their authentication through the 802.1x AAA override.

Step 7 Configure IPv6 ACL or Flexible NetFlow.

- Under the **Access Policies** > **Remote LAN ACL** section, choose the **IPv6 ACL** from the drop-down list.
- Under the **Access Policies** > **AVC** > **Flow Monitor IPv6** section, check the **Egress Status** and **Ingress Status** check boxes and choose the policies from the drop-down lists.

Step 8 Click the **Advanced** tab.

a) Configure the violation mode for Remote-LAN 802.1x from the **Violation Mode** drop-down list, choose the violation mode type from the following options:
   - Shutdown—Disables the port
   - Replace—Removes the current session and initiates authentication for the new host. This is the default behavior.
   - Protect—Drops packets with unexpected MAC addresses without generating a system message.

b) Enter the **Session Timeout (sec)** value to define the client's duration of a session.

   The range is between 20 and 86400 seconds.

c) Under **AAA Policy Params** section, check the **AAA Override** check box to enable AAA override.

d) Under the **Exclusionlist Params** section, check the **Exclusionlist** check box and enter the **Exclusionlist Timeout** value.

   This sets the exclusion time for a client. The range is between 0 and 2147483647 seconds. 0 refers to no timeout.

Step 9 Save the configuration.

Configuring RLAN Policy Profile Parameters (CLI)

Before you begin

RLAN does not support the following features:

- Central Web Authentication (CWA)
- Quality of Service (QoS)
- Bi-Directional Rate Limiting (BDRL)
- Identity PSK (iPSK)

Procedure

	Command or Action	Purpose
Step 1	**central switching** **Example:** `Device(config-remote-lan-policy)# central switching`	Configures central switching.
Step 2	**central dhcp** **Example:** `Device(config-remote-lan-policy)# central dhcp`	Configures central DHCP.
Step 3	**exclusionlist timeout** *timeout* **Example:** `Device(config-remote-lan-policy)# exclusionlist timeout 200`	Sets exclusion-listing on RLAN. *timeout*—Sets the time, up to which the client will be in excluded state. Range is from 0 to 2147483647 seconds. 0 refers to no timeout.
Step 4	**vlan** *vlan* **Example:** `Device(config-remote-lan-policy)# vlan vlan1`	Configures VLAN name or ID. - *vlan*—Is the vlan name.
Step 5	**aaa-override** **Example:** `Device(config-remote-lan-policy)# aaa-override`	Configures AAA policy override.
Step 6	**session-timeout** *timeout in seconds* **Example:** `Device(config-remote-lan-policy)# session-timeout 21`	Configures client session timeout. *timeout in seconds*—Defines the duration of a session. Range is from 20 to 86400 seconds.

	Command or Action	Purpose
		Note If the session timeout is less than 300 seconds for Dot1x clients, the session timeout is set as one day that is, equal to 86400 seconds.
Step 7	**host-mode** {**multidomain** *voice domain* | **multihost** |**singlehost**} **Example:** `Device(config-remote-lan-policy)# host-mode multidomain`	Configures host mode for remote-LAN 802.1x. *voice domain*—Is the RLAN voice domain VLAN ID. Range is from 0 to 65535. You can configure the following IEEE 802.1X authentication modes: • Multi-Domain Mode—The authenticator allows one host from the data domain and another from the voice domain. This is a typical configuration on switch ports with IP phones connected. • Multi-Host Mode—The first device to authenticate opens up to the switch port, so that all other devices can use the port. You need not authenticate other devices independently, if the authenticated device becomes authorized the switch port is closed. • Single-Host Mode—Is the default host mode. In this mode, the switch port allows only a single host to be authenticated and passes traffic one by one.
Step 8	**violation-mode** {**protect** | **replace** | **shutdown**} **Example:** `Device(config-remote-lan-policy)# violation-mode protect`	Configures violation mode for Remote-LAN 802.1x. When a security violation occurs, a port is protected based on the following configured violation actions: • Shutdown—Disables the port. • Replace—Removes the current session and initiates authentication for the new host. This is the default behavior. • Protect—Drops packets with unexpected MAC addresses without generating a system message. In the single-host authentication mode, a violation is triggered when more than one device is detected in data VLAN. In a multi-host

	Command or Action	Purpose
		authentication mode, a violation is triggered when more than one device is detected in data VLAN or voice VLAN.
Step 9	[**no**] **poe** **Example:** `Device(config-remote-lan-policy)# poe`	Enables or disables PoE.
Step 10	[**no**] **shutdown** **Example:** `Device(config-remote-lan-policy)# shutdown`	Enables or disables an RLAN policy profile.
Step 11	**end** **Example:** `Device(config-remote-lan-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Policy Tag and Mapping an RLAN Policy Profile to an RLAN Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config)# wireless tag policy remote-lan-policy-tag`	Configures policy tag and enters policy tag configuration mode.
Step 3	**remote-lan** *remote-lan-profile-name* **policy** *rlan-policy-profile-name* **port-id** *port-id* **Example:** `Device(config-policy-tag)# remote-lan rlan_profile_name policy rlan_policy_profile port-id 2`	Maps an RLAN policy profile to an RLAN profile. • *remote-lan-profile-name*—Is the name of the RLAN profile. • *rlan-policy-profile-name*—Is the name of the policy profile. • *port-id*—Is the LAN port number on the access point. Range is from 1 to 4.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config-policy-tag)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring LAN Port (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap name** *ap name* **lan port-id** *lan port id* {**disable** | **enable**} **Example:** `Device# ap name L2_1810w_2 lan port-id 1 enable`	Configures a LAN port. • enable—Enables the LAN port. • disable—Disables the LAN port.

Attaching Policy Tag to an Access Point (GUI)

Procedure

Step 1 Choose **Configuration > Wireless > Access Points**.

Step 2 Select the AP to attach the Policy Tag.

Step 3 Under the **Tags** section, use the **Policy** drop-down to select a policy tag.

Step 4 Click **Update & Apply to Device**.

Attaching Policy Tag to an Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap** *ap-ethernet-mac* **Example:** `Device(config)# ap 00a2.891c.21e0`	Configures MAP address for an AP and enters AP configuration mode.
Step 3	**policy-tag** *policy-tag-name*	Attaches policy tag to the access point.

	Command or Action	Purpose
	Example: `Device(config-ap-tag)# policy-tag remote-lan-policy-tag`	*policy-tag-name*—Is the name of the policy tag defined earlier.
Step 4	**end** **Example:** `Device(config-ap-tag)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying RLAN Configuration

To view the summary of all RLANs, use the following command:

```
Device# show remote-lan summary

Number of RLANs: 1

RLAN        Profile Name                        Status
------------------------------------------------------------------
1            rlan_test_1                         Enabled
```

To view the RLAN configuration by ID, use the following command:

```
Device# show remote-lan id <id>

Remote-LAN Profile Name              : rlan_test_1
================================================
Identifier                                  : 1
Status                                      : Enabled
Mac-filtering                               : Not Configured
Number of Active Clients                    : 1
Security_8021X                              : Disabled
8021.x Authentication list name             : Not Configured
Local Auth eap Profile Name                 : Not Configured
Web Auth Security                           : Disabled
Webauth Authentication list name            : Not Configured
Web Auth Parameter Map                      : Not Configured
Client association limit                    : 0
Ipv4 Web Pre Auth Acl                       : Not Configured
Ipv6 Web Pre Auth Acl                       : Not Configured
```

To view the RLAN configuration by profile name, use the following command:

```
Device# show remote-lan name <profile-name>

Remote-LAN Profile Name     : rlan_test_1
================================================
Identifier                                    : 1
Status                                        : Enabled
Mac-filtering                                 : mac-auth
Number of Active Clients                      : 0
Security_8021x_dot1x                          : Enabled
8021.x Authentication list name               : Not Configured
Local Auth eap Profile Name                   : Not Configured
Web Auth Security                             : Disabled
Webauth Authentication list name              : Not Configured
Web Auth Parameter Map                        : Not Configured
Client association limit                      : 0
Ipv4 Web Pre Auth Acl                         : Not Configured
Ipv6 Web Pre Auth Acl                         : Not Configured
```

```
mDNS Gateway Status                          : Bridge
Fabric Profile Name                        : rlan-fabric-profile
```

To view the detailed output of all RLANs, use the following command:

```
Device# show remote-lan all

Remote-LAN Profile Name            : rlan_test_1
================================================
Identifier                         : 1
Status                             : Enabled
Mac-filtering                      : Not Configured
Number of Active Clients           : 1
Security_8021X                     : Disabled
8021.x Authentication list name    : Not Configured
Local Auth eap Profile Name        : Not Configured
Web Auth Security                  : Disabled
Webauth Authentication list name   : Not Configured
Web Auth Parameter Map             : Not Configured
Client association limit           : 0
Ipv4 Web Pre Auth Acl              : Not Configured
Ipv6 Web Pre Auth Acl              : Not Configured

Remote-LAN Profile Name            : rlan_test_2
================================================
Identifier                         : 2
Status                             : Enabled
Mac-filtering                      : Not Configured
Number of Active Clients           : 1
Security_8021X                     : Disabled
8021.x Authentication list name    : Not Configured
Local Auth eap Profile Name        : Not Configured
Web Auth Security                  : Disabled
Webauth Authentication list name   : Not Configured
Web Auth Parameter Map             : Not Configured
Client association limit           : 0
Ipv4 Web Pre Auth Acl              : Not Configured
Ipv6 Web Pre Auth Acl              : Not Configured
```

```
Device# show remote-lan policy summary
Number of Policy Profiles: 1

Profile Name                      Description                              Status
-------------------------------------------------------------------------------------------
rlan_named_pp1                Testing RLAN policy profile              Enabled
```

To view the LAN port configuration of a Cisco AP, use the following command:

```
Device# show ap name <ap_name> lan port summary
LAN Port status for AP L2_1815w_1
Port ID      status       vlanId      poe
---------------------------------------------
LAN1         Enabled       20          Disabled
LAN2         Enabled       20          NA
LAN3         Disabled      0           NA
```

To view the summary of all clients, use the following command:

```
Device# show wireless client summary
Number of Local Clients: 1

MAC Address       AP Name         WLAN         State    Protocol    Method     Role
-----------------------------------------------------------------------------------------
d8eb.97b6.fcc6    L2_1815w_1      1            * Run     Ethernet    None       Local
```

To view the client details with the specified username, use the following command:

```
Device# show wireless client username cisco
MAC Address        AP Name          Status      WLAN      Auth Protocol
-------------------------------------------------------------------------------------------------
0014.d1da.a977    L2_1815w_1        Run 1 *      Yes        Ethernet
d8eb.97b6.fcc6    L2_1815w_1        Run 1 *      Yes        Ethernet
```

To view the detailed information for a client by MAC address, use the following command:

```
Device# show wireless client mac-address 2cea.7f18.5bb3 detail
Client MAC Address : 2cea.7f18.5bb3
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 10.56.33.21
Client IPv6 Addresses : fe80::d60:2e8:4cc2:6212
Client Username: N/A
AP MAC Address : 4ca6.4d22.1a80
AP Name: AP3C57.31C5.799C
AP slot : 16
Client State : Associated
Policy Profile : fabric-rlan-policy
Flex Profile : default-flex-profile
Remote LAN Id: 1 <----------
Remote LAN Name: fabric-rlan <--------
Wireless LAN Network Name (SSID): fabric-rlan <----------
BSSID : 4ca6.4d22.1a81
Connected For : 211 seconds
Protocol : Ethernet <--------
Channel : 0
Port ID: 1 <-----------
Client IIF-ID : 0xa0000002
Association Id : 0
Authentication Algorithm : Open System
<--------o/p trimmed ------>
```

To view the summary of all AP tags, use the following command:

```
Device# show ap tag summary
Number of APs: 2

AP Name             AP Mac               Site Tag Name         Policy Tag Name         RF
Tag Name               Misconfigured     Tag Source
-------------------------------------------------------------------------------------------
L2_1810d_1        0008.3296.24c0       default-site-tag        default-policy-tag
default-rf-tag             No              Default
L2_1810w_2        00b0.e18c.5880       rlan-site-tag              rlan_pt_1
default-rf-tag             No              Static
```

To view the summary of all policy tags, use the following command:

```
Device# show wireless tag policy summary
Number of Policy Tags: 2

Policy Tag Name                   Description
------------------------------------------------------------------------
rlan_pt_1
default-policy-tag                default policy-tag
```

To view details of a specific policy tag, use the following command:

```
Device# show wireless tag policy detailed <rlan_policy_tag_name>
Policy Tag Name : rlan_pt_1
Description     :

Number of WLAN-POLICY maps: 0

Number of RLAN-POLICY maps: 2
```

```
REMOTE-LAN Profile Name           Policy Name                              Port Id

-------------------------------------------------------------------------------------------
rlan_test_1                       rlan_named_pp1                             1

rlan_test_1                       rlan_named_pp1                             2
```

To view the fabric client summary, use the following command:

```
Device# show wireless fabric client summary

Number of Fabric Clients : 0

MAC Address    AP Name                          WLAN State              Protocol Method
  L2 VNID    RLOC IP
```

To view the RLAN client summary, use the following command:

```
Device# show wireless client summary

Number of Clients: 1

MAC Address        AP Name       Type  ID  State    Protocol   Method   Role
-------------------------------------------------------------------------------------------
2cea.7f18.5bb3 AP3C57.31C5.799C  RLAN   1    Run    Ethernet   None    Local

Number of Excluded Clients: 0
```

Information About RLAN Authentication Fallback

From Cisco IOS XE Cupertino 17.8.1, Remote LAN (RLAN) ports on OfficeExtend Access Points (OEAPs) support the fallback mechanism for authentication from 802.1X to MAC authentication bypass (MAB) and vice versa. If a client using 802.1X as an authentication method fails to authenticate within the timeout period, the client gets authenticated using the MAB method. Similarly, if the device MAC address is not registered for MAB authentication, the authentication fails, and the client gets authenticated using the 802.1X method.

By default, the RLAN fallback mechanism is disabled. You should explicitly enable it. When both 802.1X and MAB are enabled, the device should pass both authentication methods for successful authentication.

Configuring RLAN Authentication Fallback (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap remote-lan profile-name** *rlan-profile-name rlan-id* **Example:** `Device(config)# ap remote-lan profile-name rlan_profile_name 3`	Configures remote LAN profile.

	Command or Action	Purpose
Step 3	**security** {**dot1x on-macfilter-failure** | **mac-filter on-dot1x-failure**} **Example:** `Device(config-remote-lan)# security dot1x on-macfilter-failure`	Enables 802.1X authentication on MAC filter failure. **Note** You can either configure 802.1X authentication on MAC filter failure or MAC filter authentication on 802.1X failure. You cannot configure both.
Step 4	**end** **Example:** `Device(config-remote-lan)# end`	Returns to privileged EXEC mode.

Modifying 802.1X EAP Timers for RLAN Clients

To adapt the 802.1X EAP timers for RLAN clients, use the following procedure.

Note When you modify the 802.1X EAP timers, ensure that the timer is long enough to allow 802.1X-capable endpoints to authenticate. A timer that is too short may result in 802.1X-capable endpoints being subject to a fallback authentication or authorization technique.

If 802.1X EAP timers are not configured using this procedure, the timer configuration done using the **wireless security dot1x request** and **wireless security dot1x identity-request** commands are applied.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap remote-lan profile-name** *rlan-profile-name rlan-id* **Example:** `Device(config)# ap remote-lan profile-name rlan_profile_name 3`	Configures the remote LAN profile.
Step 3	**security dot1x identity-request retries** *retry-num* **Example:** `Device(config-remote-lan)# security dot1x identity-request retries 20`	Configures the maximum number of EAP ID request retransmissions. Valid values range from 1 to 20.

	Command or Action	Purpose
Step 4	**security dot1x identity-request timeout** *timeout-value* **Example:** `Device(config-remote-lan)# security dot1x identity-request timeout 120`	Configures the EAP ID request-timeout value, in seconds. Valid values range from 1 to 120.
Step 5	**security dot1x request retries** *retry-num* **Example:** `Device(config-remote-lan)# security dot1x request retries 20`	Configures the maximum number of EAP request retransmissions. Valid values range from 0 to 20.
Step 6	**security dot1x request timeout** *timeout-value* **Example:** `Device(config-remote-lan)# security dot1x request timeout 120`	Configures the EAP request retransmission timeout value, in seconds. Valid values range from 1 to 120.
Step 7	**end** **Example:** `Device(config-remote-lan)# end`	Returns to privileged EXEC mode.

Verifying RLAN Authentication Fallback

To check the status of the fallback authentication mechanism, use the following command:

```
Device# show remote-lan all

Remote-LAN Profile Name     : rlan_profile_name
================================================
Identifier                                    : 3
Status                                        : Disabled
Mac-filtering                                 : Not Configured
Number of Active Clients                      : 0
Security_8021x_dot1x                          : Enabled
8021.x Authentication list name               : Not Configured
Local Auth eap Profile Name                   : Not Configured
Web Auth Security                             : Disabled
Webauth Authentication list name              : Not Configured
Web Auth Parameter Map                        : Not Configured
Client association limit                      : 0
Ipv4 Web Pre Auth Acl                         : Not Configured
Ipv6 Web Pre Auth Acl                         : Not Configured
mDNS Gateway Status                           : Bridge
Authentication Fallback Status                : MAC-filtering to Dot1X
```