# 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 9105AXW
- Cisco Aironet OEAP 1810 series
- Cisco Aironet 1815T series
- Cisco Aironet 1810W series
- Cisco Aironet 1815W

### 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**

- RLAN is supported in APs that have more than one Ethernet port.

- 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**<br><br>**Example:**<br><br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | | **[no] ap remote-lan shutdown**<br><br>**Example:**<br><br>`Device(config)# [no] ap remote-lan shutdown` | Enables or disables all RLANs. |
| **Step 3** | | **end**<br><br>**Example:**<br><br>`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**<br><br>**Example:**<br><br>`Device# configure terminal` | Enters global configuration mode. |

|  | Command or Action | Purpose |
|---|---|---|
| Step 2 | **ap remote-lan profile-name** *remote-lan-profile-name rlan-id*<br><br>**Example:**<br><br>Device(config)# **ap remote-lan profile-name rlan_profile_name 3** | Configures remote LAN profile.<br><br>• *remote-lan-profile*—Is the remote LAN profile name. Range is from 1 to 32 alphanumeric characters.<br><br>• *rlan-id*—Is the remote LAN identifier. Range is from 1 to 128.<br><br>**Note** You can create a maximum of 128 RLANs. You cannot use the *rlan-id* of an existing RLAN while creating another RLAN.<br><br>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.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **client association limit** *client-connections* <br><br>**Example:** <br>`Device(config-remote-lan)# client association limit 1` | Configures client connections per RLAN. <br><br>*client-connections*—Is the maximum client connections per RLAN. Range is from 0 to 10000. 0 refers to unlimited. |
| **Step 2** | **ip access-group web** *IPv4-acl-name* <br><br>**Example:** <br>`Device(config-remote-lan)# ip access-group web acl_name` | Configures RLAN IP configuration commands. <br><br>*IPv4-acl-name*—Refers to the IPv4 ACL name or ID. |
| **Step 3** | **local-auth** *profile name* <br><br>**Example:** <br>`Device(config-remote-lan)# local-auth profile_name` | Sets EAP Profile on an RLAN. <br><br>*profile name*—Is the EAP profile on an RLAN. |
| **Step 4** | **mac-filtering** *mac-filter-name* <br><br>**Example:** <br>`Device(config-remote-lan)# mac-filtering mac_filter` | Sets MAC filtering support on an RLAN. <br><br>*mac-filter-name*—Is the authorization list name. |
| **Step 5** | **security dot1x authentication-list** *list-name* <br><br>**Example:** <br>`Device(config-remote-lan)# security dot1x authentication-list dot1_auth_list` | Configures 802.1X for an RLAN. <br><br>*list-name*—Is the authentication list name. |
| **Step 6** | **security web-auth authentication-list** *list-name* <br><br>**Example:** | Configures web authentication for an RLAN. <br><br>*list-name*—Is the authentication list name. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-remote-lan)# security web-auth authentication-list web_auth_list` | **Note** You can activate either web or dot1x authentication list at a time. |
| Step 7 | **[no] shutdown**<br><br>**Example:**<br>`Device(config-remote-lan)# shutdown` | Enables or disables RLAN profile. |
| Step 8 | **end**<br><br>**Example:**<br>`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**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| Step 2 | **ap remote-lan-policy policy-name** *profile name*<br><br>**Example:**<br>`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)

**Procedure**

|  | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **central switching**<br><br>**Example:**<br><br>`Device(config-remote-lan-policy)#`<br>`central switching` | Configures central switching. |
| **Step 2** | **central dhcp**<br><br>**Example:**<br><br>`Device(config-remote-lan-policy)#`<br>`central dhcp` | Configures central DHCP. |
| **Step 3** | **exclusionlist timeout** *timeout*<br><br>**Example:**<br><br>`Device(config-remote-lan-policy)#`<br>`exclusionlist timeout 200` | Sets exclusion-listing on RLAN.<br><br>*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*<br><br>**Example:**<br><br>`Device(config-remote-lan-policy)# vlan`<br>` vlan1` | Configures VLAN name or ID.<br><br>- *vlan*—Is the vlan name. |
| **Step 5** | **Example:** |  |

| | Command or Action | Purpose |
|---|---|---|
| | Device(config-remote-lan-policy)# **ipv6 acl ipv6_acl** | |
| Step 6 | **aaa-override**<br><br>**Example:**<br>Device(config-remote-lan-policy)# **aaa-override** | Configures AAA policy override. |
| Step 7 | **session-timeout** *timeout in seconds*<br><br>**Example:**<br>Device(config-remote-lan-policy)# **session-timeout 21** | Configures client session timeout.<br><br>*timeout in seconds*—Defines the duration of a session. Range is from 20 to 86400 seconds. |
| Step 8 | **host-mode** {**multidomain** *voice domain* \| **multihost** \|**singlehost**}<br><br>**Example:**<br>Device(config-remote-lan-policy)# **host-mode multidomain** | Configures host mode for remote-LAN 802.1x.<br><br>*voice domain*—Is the RLAN voice domain VLAN ID. Range is from 0 to 65535.<br><br>You can configure the following IEEE 802.1X authentication modes:<br><br>• 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.<br><br>• 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.<br><br>• 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 9 | **violation-mode** {**protect** \| **replace** \| **shutdown**}<br><br>**Example:**<br>Device(config-remote-lan-policy)# **violation-mode protect** | Configures violation mode for Remote-LAN 802.1x.<br><br>When a security violation occurs, a port is protected based on the following configured violation actions:<br><br>• Shutdown—Disables the port. |

| | Command or Action | Purpose |
|---|---|---|
| | | • 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 authentication mode, a violation is triggered when more than one device is detected in data VLAN or voice VLAN. |
| Step 10 | [**no**] **poe**<br><br>**Example:**<br><br>Device(config-remote-lan-policy)# **poe** | Enables or disables PoE. |
| Step 11 | [**no**] **shutdown**<br><br>**Example:**<br><br>Device(config-remote-lan-policy)# **shutdown** | Enables or disables an RLAN policy profile. |
| Step 12 | **end**<br><br>**Example:**<br><br>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**<br><br>**Example:**<br><br>Device# configure terminal | Enters global configuration mode. |
| Step 2 | **wireless tag policy** *policy-tag-name*<br><br>**Example:**<br><br>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* | Maps an RLAN policy profile to an RLAN profile. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>Device(config-policy-tag)# **remote-lan rlan_profile_name policy rlan_policy_profile port-id 2** | • *remote-lan-profile-name*—Is the name of the RLAN profile.<br><br>• *rlan-policy-profile-name*—Is the name of the policy profile.<br><br>• *port-id*—Is the LAN port number on the access point. Range is from 1 to 4. |
| **Step 4** | **end**<br>**Example:**<br>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**}<br>**Example:**<br>Device# **ap name L2_1810w_2 lan port-id 1 enable** | Configures a LAN port.<br><br>• enable—Enables the LAN port.<br><br>• 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**<br><br>**Example:**<br><br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **ap** *ap-ethernet-mac*<br><br>**Example:**<br><br>`Device(config)# ap 00a2.891c.21e0` | Configures MAP address for an AP and enters AP configuration mode. |
| **Step 3** | **policy-tag** *policy-tag-name*<br><br>**Example:**<br><br>`Device(config-ap-tag)# policy-tag`<br>`remote-lan-policy-tag` | Attaches policy tag to the access point.<br><br>*policy-tag-name*—Is the name of the policy tag defined earlier. |
| **Step 4** | **end**<br><br>**Example:**<br><br>`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                               : 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 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 d8eb.97b6.fcc6 detail
Client MAC Address : d8eb.97b6.fcc6
Client IPv4 Address : 9.2.20.78
Client IPv6 Addresses : fe80::1863:292f:feaa:2cf
Client Username: N/A
AP MAC Address : 707d.b99e.c2e0
AP Name: L2_1815w_1
AP slot : 2
Client State : Associated
Policy Profile : rlan_named_pp1
Flex Profile : rlan-flex-profile
Remote LAN Id : 1
Remote LAN Name: rlan_test_1
BSSID : 707d.b99e.c2e1
Connected For : 1159 seconds
Protocol : Ethernet
Channel : 0
Port ID: 2
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Session Timeout : 1800 sec (Remaining time: 641 sec)
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Disabled
Fastlane Support : Disabled
Power Save : OFF
Current Rate : 0.0
Mobility:
  Move Count                 : 0
  Mobility Role              : Local
  Mobility Roam Type         : None
  Mobility Complete Timestamp : 07/06/2018 11:25:26 IST
Policy Manager State: Run
```

```
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 1159 seconds
Policy Type : N/A
Encryption Cipher : None
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN : 20
Access VLAN : 20
Anchor VLAN : 0
WFD capable : No
Managed WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Interface        : capwap_90000008
  IIF ID           : 0x90000008
  Authorized       : TRUE
  Session timeout  : 1800
  Common Session ID: 32130209000000136C48A29D
  Acct Session ID  : 0x00000000
  Aaa Server Details
  Server IP        :
  Auth Method Status List
   Method : None
  Local Policies:
   Service Template : wlan_svc_rlan_named_pp1_local (priority 254)
    Absolute-Timer   : 1800
    VLAN             : 20
  Server Policies:
  Resultant Policies:
    VLAN             : 20
    Absolute-Timer   : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
FlexConnect Data Switching : Central
FlexConnect Dhcp Status : Central
FlexConnect Authentication : Central
FlexConnect Central Association : No
Client Statistics:
  Number of Bytes Received : 6855
  Number of Bytes Sent : 1640
  Number of Packets Received : 105
  Number of Packets Sent : 27
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : 0 dBm
  Signal to Noise Ratio : 0 dB
Fabric status : Disabled
Client Scan Reports
Assisted Roaming Neighbor List
```

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
```