Configuring Remote LANs

Configuring Remote LANs (CLI)

Creating an RLAN Profile (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap remote-lan profile-name** *remote-lan-profile-name rlan-id*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**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 and enters RLAN configuration mode. • *remote-lan-profile*: The remote LAN profile name. Range is from 1 to 32 alphanumeric characters. • *rlan-id*: The remote LAN identifier. Range is from 1 to 128.

	Command or Action	Purpose
		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 profiles cannot have the same names. Similarly, RLAN and WLAN policy profile cannot have the same names.
Step 4	**end** **Example:** `Device(config-remote-lan)# end`	Exits RLAN configuration mode and returns to privileged EXEC mode.

Configuring RLAN Profile Parameters (CLI)

Before you begin

Note 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap remote-lan profile-name** *remote-lan-profile-name rlan-id*
4. **client association limit** *client-connections*
5. **ip access-group web** *IPv4-acl-name*
6. **ipv6 traffic-filter web** *IPv6-acl-name*
7. **local-auth** *profile name*
8. **mac-filtering** *mac-filter-name*
9. **mdns-sd-interface** {**drop** | **gateway**}
10. **security dot1x authentication-list** *list-name*
11. **security web-auth authentication-list** *list-name*
12. **no shutdown**
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**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 and enters RLAN configuration mode.
Step 4	**client association limit** *client-connections* **Example:** `Device(config-remote-lan)# client association limit 1`	Configures client connections per RLAN. *client-connections*: The maximum client connections per RLAN. Range is from 0 to 10000. 0 refers to unlimited client connections.
Step 5	**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*: The IPv4 ACL name or ID.
Step 6	**ipv6 traffic-filter web** *IPv6-acl-name* **Example:** `Device(config-remote-lan)# ipv6 traffic-filter web ipv6-acl`	Configures RLAN IP configuration commands. *IPv6-acl-name*: The IPv6 ACL name or ID.
Step 7	**local-auth** *profile name* **Example:** `Device(config-remote-lan)# local-auth profile_name`	Sets EAP profile on an RLAN.
Step 8	**mac-filtering** *mac-filter-name* **Example:** `Device(config-remote-lan)# mac-filtering mac_filter`	Sets MAC filtering support on an RLAN.
Step 9	**mdns-sd-interface** {**drop** | **gateway**} **Example:** `Device(config-remote-lan)# mdns-sd-interface gateway`	Enables MDNS gateway for the RLAN.
Step 10	**security dot1x authentication-list** *list-name* **Example:** `Device(config-remote-lan)# security dot1x authentication-list dot1_auth_list`	Configures 802.1X for an RLAN.
Step 11	**security web-auth authentication-list** *list-name* **Example:**	Configures web authentication for an RLAN.

	Command or Action	Purpose
	`Device(config-remote-lan)# security web-auth authentication-list web_auth_list`	**Note** You can activate either web authentication or dot1x authentication at a time.
Step 12	**no shutdown** **Example:** `Device(config-remote-lan)# no shutdown`	Enables RLAN profile.
Step 13	**end** **Example:** `Device(config-remote-lan)# end`	Exits RLAN configuration mode and returns to privileged EXEC mode.

Creating an RLAN Policy Profile (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap remote-lan-policy policy-name** *profile name*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**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 RLAN policy configuration mode.
Step 4	**end** **Example:** `Device(config)# ap remote-lan-policy policy-name rlan_policy_prof_name`	Exits RLAN policy configuration mode and returns to privileged EXEC mode.

Configuring RLAN Policy Profile Parameters (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap remote-lan-policy policy-name** *profile name*
4. **central switching**
5. **central dhcp**
6. **exclusionlist timeout** *timeout*
7. **ipv4** {**acl** *ipv6_acl* | **dhcp** {**required** | **server** *ip-address*}}
8. **ipv6 acl** *ipv6-acl*
9. **aaa-policy** *policy-name*
10. **aaa-override**
11. **accounting-list** *list-name*
12. **mdns-sd service-policy** *service-policy-name*
13. **session-timeout** *timeout in seconds*
14. **host-mode** {**multidomain** *voice domain* | **multihost** |**singlehost**}
15. **violation-mode** {**protect** | **replace** | **shutdown**}
16. **poe**
17. **power-level** *level*
18. **pre-auth**
19. **user-defined-network** [**drop-unicast**]
20. **shutdown**
21. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**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 RLAN policy configuration mode.
Step 4	**central switching** **Example:** `Device(config-remote-lan-policy)# central switching`	Configures central switching.

	Command or Action	Purpose
Step 5	**central dhcp** **Example:** `Device(config-remote-lan-policy)# central dhcp`	Configures central DHCP.
Step 6	**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 7	**ipv4** {**acl** *ipv6_acl* | **dhcp** {**required** | **server** *ip-address*}} **Example:** `Device(config-remote-lan-policy)# ipv4 dhcp server 10.1.1.1`	Configures an IPv4 DHCP server for the RLAN.
Step 8	**ipv6 acl** *ipv6-acl* **Example:** `Device(config-remote-lan-policy)# ipv6 acl ipv6_acl`	Configures an IPv6 ACL.
Step 9	**aaa-policy** *policy-name* **Example:** `Device(config-remote-lan-policy)# aaa-policy aaa_policy1`	Configures AAA policy.
Step 10	**aaa-override** **Example:** `Device(config-remote-lan-policy)# aaa-override`	Configures AAA policy override.
Step 11	**accounting-list** *list-name* **Example:** `Device(config-remote-lan-policy)# accounting-list rlan_acct_list1`	Sets the accounting list for IEEE 802.1x.
Step 12	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config-remote-lan-policy)# mdns-sd service-policy mdns-service-policy`	Configures an MDNS service policy.
Step 13	**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.
Step 14	**host-mode** {**multidomain** *voice domain* | **multihost** |**singlehost**} **Example:**	Configures host mode for remote-LAN 802.1x. *voice domain*: The RLAN voice domain VLAN ID. Range is from 0 to 65535.

	Command or Action	Purpose
	`Device(config-remote-lan-policy)# host-mode multidomain`	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: 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 15	**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 single-host authentication mode, a violation is triggered when more than one device is detected in data VLAN. In multi-host authentication mode, a violation is triggered when more than one device is detected in data VLAN or voice VLAN.
Step 16	**poe** **Example:** `Device(config-remote-lan-policy)# poe`	Enables Power over Ethernet (PoE).
Step 17	**power-level** *level* **Example:** `Device(config-remote-lan-policy)# power-level 1`	Configures the power level to be supported on the LAN port.
Step 18	**pre-auth** **Example:** `Device(config-remote-lan-policy)# pre-auth`	Configures pre-authentication for the RLAN.

	Command or Action	Purpose
Step 19	**user-defined-network** [**drop-unicast**] **Example:** `Device(config-remote-lan-policy)# user-defined network`	Configures an user-defined network.
Step 20	**shutdown** **Example:** `Device(config-remote-lan-policy)# shutdown`	Enables RLAN policy profile.
Step 21	**end** **Example:** `Device(config-remote-lan-policy)# end`	Exits RLAN policy configuration mode and returns to privileged EXEC mode.

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **wireless tag policy** *policy-tag-name*
4. **remote-lan** *remote-lan-profile-name* **policy** *rlan-policy-profile-name* **port-id** *port-id*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**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 4	**remote-lan** *remote-lan-profile-name* **policy** *rlan-policy-profile-name* **port-id** *port-id* **Example:**	Maps an RLAN policy profile to an RLAN profile.

	Command or Action	Purpose
	`Device(config-policy-tag)# remote-lan rlan_profile_name policy rlan_policy_profile port-id 2`	
Step 5	**end** **Example:** `Device(config-policy-tag)# end`	Exit policy tag configuration mode and returns to privileged EXEC mode.

Attaching an RLAN Policy Tag to an Access Point (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap** *ap-ethernet-mac*
4. **policy-tag** *policy-tag-name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ap** *ap-ethernet-mac* **Example:** `Device(config)# ap 00a2.891c.21e0`	Configures MAP address for an AP and enters AP configuration mode.
Step 4	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag remote-lan-policy-tag`	Attaches a policy tag to the access point. *policy-tag-name*: Name of the policy tag defined earlier.
Step 5	**end** **Example:** `Device(config-ap-tag)# end`	Exits AP configuration mode and returns to privileged EXEC mode.

Configuring Remote LANs (GUI)

Creating RLAN Profile (GUI)

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**.

Configuring RLAN Profile Parameters (GUI)

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.

Creating RLAN Policy Profile (GUI)

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**.

Configuring RLAN Policy Profile Parameters (GUI)

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.

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.

Attaching Policy Tag to an Access Point (GUI)

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**.