Configuring Remote-LAN

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for Configuring Remote-LAN

- The Remote-LAN feature is supported in Cisco IOS XE Denali 16.3.1 release and later. This feature is available on the Cisco Aironet 1810W Series AP, which offer compact, wall plate-mountable access point.

Restrictions for Remote-LAN

- Same profile names or IDs cannot be used for both WLANs and remote LANs.
- Only three clients can connect to a Cisco Aironet 1810W Series AP through local Gigabit Ethernet ports. Each port supports only one client.

- Remote-LAN profiles can be mapped only to an AP group. Hence, an AP should be in an AP group to configure Remote-LAN profile in its local Gigabit Ethernet ports.
- The Default AP group cannot be configured for Remote-LAN.

Information About Remote-LAN

Remote-LAN is similar to a WLAN, the only difference being that a WLAN is used for wireless connection, but a Remote-LAN is used for wired ports. Cisco Aironet 1810W Series AP come with three local Gigabit Ethernet ports, one uplink Gigabit Ethernet port, and one passive passthrough RJ-45 port. Configuring a Remote-LAN profile on a local Gigabit Ethernet port enables the traffic from wired devices to connect to the ports tunneled back to a wireless controller.

Configuring Remote-LAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**remote-lan** *profile-name id* **Example:** `Device(config)# remote-lan test-lan 3`	Specifies the Remote-LAN profile name. • id—Unique number entered during configuration tasks. Range is from 1 to 64.
Step 2	**session-timeout** *session-time* **Example:** `Device(config-remote-lan)# session-timeout 50`	Sets the duration of session, in seconds. Range is from 0 to 86400.
Step 3	**client vlan** *vlan-identifier* **Example:** `Device(config-remote-lan)# client vlan test-vlan`	Enables an interface group on the Remote-LAN. • vlan-identifier—Specifies the VLAN identifier. It can be the VLAN name, VLAN ID, or VLAN group name.
Step 4	**client association limit** *max-number-of-clients* **Example:** `Device(config-remote-lan)# client association limit 200`	Sets the maximum number of clients that can be connected to the Remote-LAN profile.
Step 5	**ip access-group** *acl-name* **Example:** `Device(config-remote-lan)# ip access-group  acl-name`	Configures the IPv4 ACL name or ID.

	Command or Action	Purpose
Step 6	**security webauth parameter-map parameter-name** **Example:** `Device(config-remote-lan)# security web-auth parameter-map parameter-22`	Specifies the parameter map name.
Step 7	**security dot1x** **Example:** `Device(config-remote-lan)# security dot1x`	Specifies 802.1X security.
Step 8	**security dot1x authentication** *list-name* **Example:** `Device(config-remote-lan)# security dot1x authentication-list LIST1`	Sets the Authentication List name.
Step 9	**exclusionlist timeout** *time-sec* **Example:** `Device(config-remote-lan)# exclusionlist timeout 30`	Sets time in seconds, after which a client is excluded. Range is from 0 to 2147483647. The value 0 stands for no timeout.
Step 10	**aaa-override** **Example:** `Device(config-remote-lan)# aaa-override`	Overrides the AAA policy.
Step 11	**local-auth EAP-Profile** **Example:** `Device(config-remote-lan)# local-auth EAP-Profile`	Enables the EAP profile on a Remote-LAN.
Step 12	**ip dhcp server** *ip-address* **Example:** `Device(config-remote-lan)# ip dhcp server 10.76.47.11`	Configures DHCP parameters for Remote-LAN.
Step 13	**ip access-group web** *acl-name* **Example:** `Device(config-remote-lan)# ip access-group web acl-test`	Configures the IPv4 Remote-LAN Web ACL.
Step 14	**accounting-list** *list-name* **Example:** `Device(config-remote-lan)# accounting-list list-LIST1`	Sets the accounting list for IEEE 802.1x.

	Command or Action	Purpose
Step 15	**mac-filtering** *list-name* **Example:** `Device(config-remote-lan)# mac-filtering test-10`	Sets MAC filtering support on Remote-LAN.
Step 16	**no shutdown** **Example:** `Device(config-remote-lan)# no shutdown`	Enables Remote-LAN.

Configuration Examples for Remote-LAN

The following example shows a summary of all the Remote-LANs:

```
Device# show remote-lan summary
Number of Remote-LANs: 1

Remote-LAN Profile Name                     VLAN Status
-----------------------------------------------------
2          test                             1    DOWN
```

The following example shows a Remote-LAN configuration by ID:

```
Device# show remote-lan id 2
Remote-LAN Profile Name     : test
================================================
Identifier                                     : 2
Status                                         : Disabled
Universal AP Admin                             : Disabled
Max Associated Clients per Remote-LAN          : 0
AAA Policy Override                            : Enabled
Number of Active Clients                       : 0
Exclusionlist Timeout                          : 21474
Session Timeout                                : 864 seconds
Interface                                      : default
Interface Status                               : Up
Remote-LAN ACL                                  : testacl
DHCP Server                                    : 10.5.7.9
DHCP Address Assignment Required               : Disabled
Local EAP Authentication                       : testeapprofile
Mac Filter Authorization list name             : testmaclist
Accounting list name                           : testlist
802.1x authentication list name                : dotxauth
Security
    802.11 Authentication                      : Open System
    802.1X                                     : Enabled
        Encryption                             : 104-bit WEP
```

The following example shows a Remote-LAN configuration by profile name:

```
Device#  show remote-lan name test
Remote-LAN Profile Name : test
================================================
```

```
Identifier : 1
Status : Disabled
Universal AP Admin : Disabled
Max Associated Clients per Remote-LAN : 0
AAA Policy Override : Disabled
Number of Active Clients : 0
Exclusionlist Timeout : 60
Session Timeout : 1800 seconds
Interface : default
Interface Status : Up
Remote-LAN ACL : unconfigured
DHCP Server : 0.0.0.0
DHCP Address Assignment Required : Disabled
Local EAP Authentication : Disabled
Mac Filter Authorization list name : Disabled
Accounting list name : Disabled
802.1x authentication list name : Disabled
Security
802.11 Authentication : Open System
802.1X : Disabled
Web Based Authentication : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled
Webauth Authentication List Name : Disabled
Webauth Parameter Map : Disabled
```

The following example shows the Remote-LAN properties of all the configured Remote-LANs:

```
Device# show remote-lan all
Remote-LAN Profile Name : test
================================================
Identifier : 1
Status : Disabled
Universal AP Admin : Disabled
Max Associated Clients per Remote-LAN : 0
AAA Policy Override : Disabled
Number of Active Clients : 0
Exclusionlist Timeout : 60
Session Timeout : 1800 seconds
Interface : default
Interface Status : Up
Remote-LAN ACL : unconfigured
DHCP Server : 0.0.0.0
DHCP Address Assignment Required : Disabled
Local EAP Authentication : Disabled
Mac Filter Authorization list name : Disabled
Accounting list name : Disabled
802.1x authentication list name : Disabled
Security
802.11 Authentication : Open System
802.1X : Disabled
Web Based Authentication : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled
Webauth Authentication List Name : Disabled
Webauth Parameter Map : Disabled
```

The following example shows a Remote-LAN configuration:

```
Device# show running-config remote-lan test
remote-lan test 1
```

```
aaa-override
accounting-list test-all-list
exclusionlist timeout 100
ip access-group test-acl
ip dhcp server 10.100.12.5
mac-filtering test-mac-list
security dot1x authentication-list test-dot1x-list
session-timeout 100
shutdown
```

The following example shows the details of the AP groups:

```
Device# show ap groups
Site Name: test-ap-group
Site Description:
Hyperlocation Operational Status: Down

WLAN ID WLAN Name Interface
-----------------------------------------------------

LAN Status PoE Remote-LAN
-------------------------------------------------------
1 Down Disabled None
2 Down None
3 Down None
```

The following example shows the details of a LAN port:

```
Device# show ap name AP00FE.C82D.E7B0 lan port 1
LAN Port status for AP AP00FE.C82D.E7B0

LanOverride Enabled

PortId Status VlanId PoE
-----------------------------------------------
LAN1 Enabled 0 Disabled
```

The following example shows the details of a LAN port summary:

```
Device# show ap name AP00FE.C82D.E7B0 lan port summary
LAN Port status for AP AP00FE.C82D.E7B0

LanOverride Enabled

Port ID Status Vlan ID PoE
-----------------------------------
LAN1 Enabled 0 Disable
LAN2 Disabled 0 Disable
LAN3 Disabled 0 Disable
```

Configuring AP Group-Specific CLIs

Use the following procedure to configure the LAN port parameters for an AP group:

Procedure

	Command or Action	Purpose
Step 1	**remote-lan** *remote-lan-name* **Example:** `Device(config-apgroup)# remote-lan test-lan`	Adds a Remote-LAN to an AP group.
Step 2	**port** *port-id* **Example:** `Device(config-apgroup)# port 1`	Configures the port ID of an AP group.
Step 3	**poe** **Example:** `Device(config-port-apgroup)# poe`	Enables a PoE on the port. **Note** PoE can be configured only for port 1.
Step 4	**remote-lan** *remote-lan-name* **Example:** `Device(config-port-apgroup)# remote-lan test-lan`	Adds a Remote-LAN ID.
Step 5	**no shutdown** **Example:** `Device(config-port-apgroup)# no shutdown`	Enables the LAN port.

Configuring PoE for a Port

The Cisco Aironet 1810W Series allows wired access via Power over Ethernet (PoE). This feature provides wired access with PoE for other devices, such as IP phones, security cameras, printers, and copiers. Only LAN Port 1 should be configured for the PoE to be enabled or disabled. By default, PoE is disabled for the port.

Procedure

	Command or Action	Purpose
Step 1	**ap name** *ap-name* **lan port-id** *port-id* **poe** **Example:** `Device# ap name AP00FE.C82D.DFB0 lan port-id 1 poe`	Enables PoE for the LAN port of an AP. **Note** PoE can be configured only for port 1.

Configuring LAN Override for an AP

LAN override can be enabled to override a LAN port configuration for a particular AP. Per-AP LAN port configurations work only when LAN override is enabled. By default, LAN override is disabled. With LAN override disabled, an AP uses AP group LAN port configurations.

Procedure

	Command or Action	Purpose
Step 1	**ap name** *ap-name* **lan override** **Example:** `Device# ap name AP00FE.C82D.DFB0 lan override`	Enables override for AP group LAN port configurations.