



Configuring Voice or Data WLAN Connectivity

The Cisco Aironet 1815 Teleworker Access Point supports a maximum of 8 wireless LANs and remote LAN. Configure the SSIDs to separate voice and data traffic, which is essential in any good network design in order to ensure proper treatment of the respective IP traffic, regardless of the medium it is traversing. In this procedure, you add an interface that allows devices on the wireless data network to communicate with the rest of your organization.

- [Creating Wireless LAN Data Interface, page 1](#)
- [Creating the Wireless LAN Voice Interface, page 3](#)
- [Creating the Remote LAN Interface, page 4](#)
- [Configuring the Data Wireless LAN, page 6](#)
- [Configure Voice Wireless LAN, page 8](#)
- [Configure the Remote LAN, page 11](#)

Creating Wireless LAN Data Interface

To create wireless LAN data interface, perform the following steps:

Procedure

- Step 1** In **Controller > Interfaces**, click **New**.
- Step 2** Enter the **Interface Name**. (Example: Wireless-Data)
- Step 3** Enter the **VLAN Id**, and then click **Apply**. (Example: 244)

The screenshot shows the Cisco Controller configuration interface. The top navigation bar includes links for Save Configuration, Ping, Logout, and Refresh. The main menu has tabs for MONITOR, WLANs, CONTROLLER (selected), WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. On the left, a sidebar lists various configuration categories: General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main content area is titled 'Interfaces > New' and contains two input fields: 'Interface Name' with the value 'Wireless-Data' and 'VLAN Id' with the value '244'. At the top right of the main area are '< Back' and 'Apply' buttons.

- Step 4** In the **Port Number** box, enter the WLC interface that connects to the LAN distribution switch. (Example: 2)
- Step 5** In the **IP Address** box, enter the IP address to assign to the WLC interface. (Example: 10.4.144.5)
- Step 6** Enter the **Netmask**. (Example: 255.255.252.0)
- Step 7** In the **Gateway** box, enter the IP address of the VLAN interface defined in Configuring LAN Distribution Switch, Procedure 1, “Configure the distribution switch,” Step 2. (Example: 10.4.144.1)
- Step 8** In the **Primary DHCP Server** box, enter the IP address of your organization’s DHCP server, and then click **Apply**. (Example: 10.4.48.10)

The screenshot shows the Cisco Controller configuration interface for editing an interface. The top navigation bar and main menu are the same as in the previous screenshot. The sidebar is also the same. The main content area is titled 'Interfaces > Edit' and contains several sections of configuration data for the 'Wireless-Data' interface. The 'General Information' section shows the Interface Name as 'Wireless-Data' and the MAC Address as 'd0:d0:fd:1f:59:e0'. The 'Configuration' section includes checkboxes for Guest Lan and Quarantine, and a text box for Quarantine Vlan Id set to '0'. The 'Physical Information' section includes text boxes for Port Number (2), Backup Port (0), and Active Port (0), and a checkbox for Enable Dynamic AP Management. The 'Interface Address' section includes text boxes for VLAN Identifier (244), IP Address (10.4.144.5), Netmask (255.255.252.0), and Gateway (10.4.144.1). The 'DHCP Information' section includes text boxes for Primary DHCP Server (10.4.48.10) and Secondary DHCP Server. The 'Access Control List' section includes a dropdown menu for ACL Name set to 'none'. A note at the bottom states: 'Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.'

Creating the Wireless LAN Voice Interface

You must add an interface that allows devices on the wireless voice network to communicate with the rest of the organization.

To create wireless LAN voice interface, perform the following steps:

Procedure

- Step 1** In **Controller > Interfaces**, click **New**.
- Step 2** Enter the **Interface Name**. (Example: Wireless-Voice)
- Step 3** Enter the **VLAN Id**, and then click **Apply**. (Example: 248)

The screenshot shows the Cisco Controller web interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'CONTROLLER' tab is selected. The left sidebar shows the 'Controller' menu with sub-items: General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main content area is titled 'Interfaces > New' and contains two input fields: 'Interface Name' with the value 'Wireless-Voice' and 'VLAN Id' with the value '248'. There are '< Back' and 'Apply' buttons at the bottom right of the form area.

- Step 4** In the **Port Number** box, enter the WLC interface that connects to the LAN distribution switch. (Example: 2)
- Step 5** In the **IP Address** box, enter the IP address to assign to the WLC interface. (Example: 10.4.148.5)
- Step 6** Enter the **Netmask**. (Example: 255.255.252.0)
- Step 7** In the **Gateway** box, enter the IP address of the VLAN interface defined in Configuring LAN Distribution Switch, Procedure 1, “Configure the distribution switch,” Step 2. (Example: 10.4.148.1)
- Step 8** In the **Primary DHCP Server** box, enter the IP address of your organization’s DHCP server, and then click Apply. (Example: 10.4.48.10)

The screenshot shows the Cisco Controller configuration page for a Remote LAN Interface. The page is titled "Interfaces > Edit" and includes a navigation menu on the left with options like General, Inventory, Interfaces, and Network Routes. The main content area is divided into several sections:

- General Information:** Interface Name (wireless-voice), MAC Address (do:d0:fd:1f:59:e0).
- Configuration:** Guest Lan (checkbox), Quarantine (checkbox), Quarantine Vlan Id (0).
- Physical Information:** Port Number (2), Backup Port (0), Active Port (0), Enable Dynamic AP Management (checkbox).
- Interface Address:** VLAN Identifier (248), IP Address (10.4.148.5), Netmask (255.255.252.0), Gateway (10.4.148.1).
- DHCP Information:** Primary DHCP Server (10.4.48.10), Secondary DHCP Server.
- Access Control List:** ACL Name (none).

A note at the bottom states: "Note: Changing the Interface parameters causes the VLANs to be temporarily disabled and thus may result in loss of connectivity for some clients."

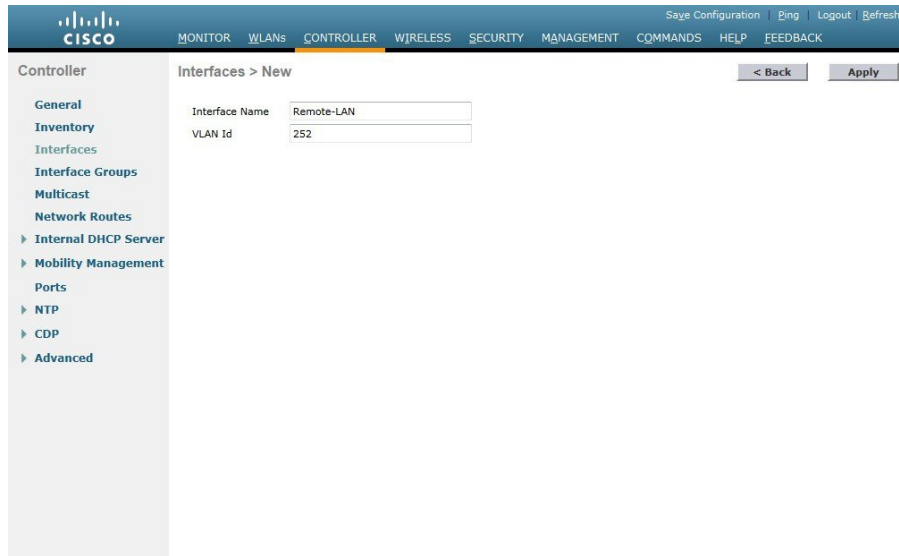
Creating the Remote LAN Interface

Next, you add an interface that allows devices on the remote LAN network to communicate with the rest of the organization.

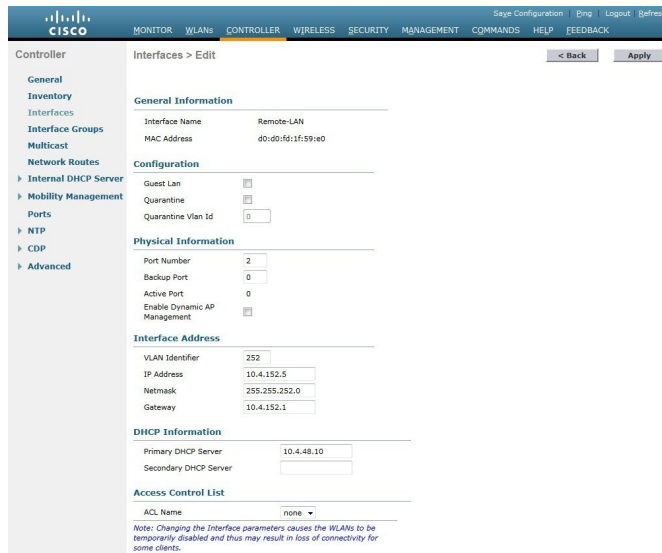
To create remote LAN interface, perform the following steps:

Procedure

- Step 1** In **Controller > Interfaces**, click **New**.
- Step 2** Enter the **Interface Name**. (Example: Remote-LAN)
- Step 3** Enter the **VLAN Id**, and then click **Apply**. (Example: 252)



- Step 4** In the **Port Number** box, enter the WLC interface that connects to the LAN distribution switch. (Example: 2)
- Step 5** In the **IP Address** box, enter the IP address to assign to the WLC interface. (Example: 10.4.152.5)
- Step 6** Enter the **Netmask**. (Example: 255.255.252.0)
- Step 7** In the **Gateway** box, enter the IP address of the VLAN interface defined in Configuring LAN Distribution Switch, Procedure 1, “Configure the distribution switch,” Step 2. (Example: 10.4.152.1)
- Step 8** In the **Primary DHCP Server** box, enter the IP address of your organization’s DHCP server, and then click **Apply**. (Example: 10.4.48.10)



Configuring the Data Wireless LAN

Wireless data traffic is different from voice traffic in that it can more efficiently handle delay and jitter as well as greater packet loss. For the data wireless LAN, keep the default QoS settings and segment the data traffic onto the data wired VLAN.

To configure the data wireless LAN, perform the following steps:

Procedure

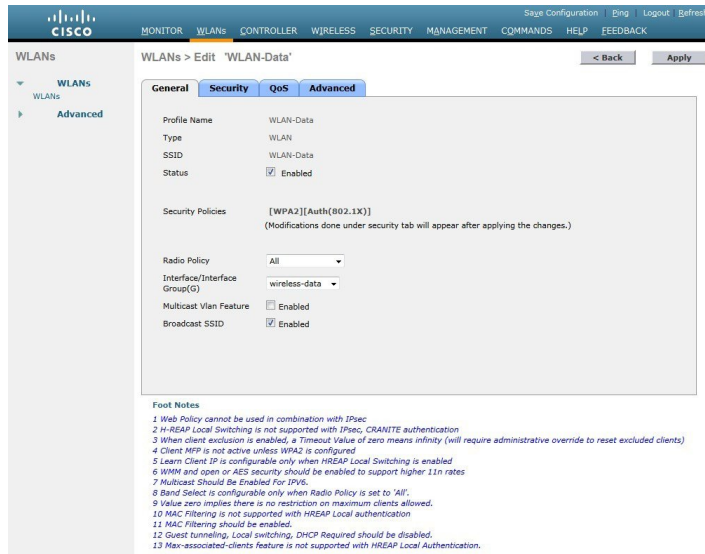
Step 1 Navigate to **WLANs**.

Step 2 Click the **WLAN ID** of the SSID created during platform setup.

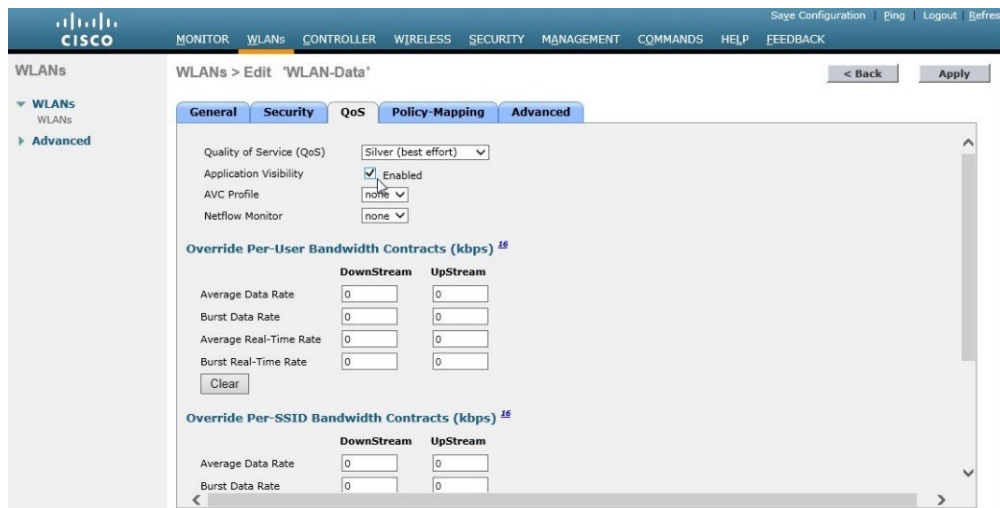
The screenshot shows the Cisco WLAN configuration page. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WLANs' section is active, showing a table with one entry. The table has columns for 'WLAN ID', 'Type', 'Profile Name', 'WLAN SSID', 'Admin Status', and 'Security Policies'. The entry has a WLAN ID of 1, Type of WLAN, Profile Name of WLAN-Data, WLAN SSID of WLAN-Data, Admin Status of Enabled, and Security Policies of [WPA2][Auth(802.1X)].

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	WLAN-Data	WLAN-Data	Enabled	[WPA2][Auth(802.1X)]

Step 3 On the General tab, in the Interface list, choose the interface created in Procedure 1.(Example: Wireless-Data) Next, enable Application Visibility and Control (AVC).



Step 4 Navigate to the **QoS** tab, select **Application Visibility**, click **Apply**, and then click **Save Configuration**, and agree to confirmation questions.



Step 5 On the **Advanced** tab, clear Coverage Hole Detection, enable DHCP Addr. Assignment Required, clear Aironet IE , enable Allow AAA Override, and then click **Apply**.

The screenshot shows the Cisco Aironet configuration interface for a WLAN. The 'Advanced' tab is selected, displaying various configuration options. The 'Apply' button is highlighted.

WLANs > Edit 'WLAN-Data'

General | **Security** | **QoS** | **Policy-Mapping** | **Advanced**

Advanced

Allow AAA Override Enabled

Coverage Hole Detection Enabled

Enable Session Timeout 1800 Session Timeout (secs)

Aironet IE Enabled

Diagnostic Channel Enabled

Override Interface ACL IPv4 None IPv6 None

Layer2 Acl None

P2P Blocking Action Disabled

Client Exclusion Enabled 60 Timeout Value (secs)

Maximum Allowed Clients #

Static IP Enabled

DHCP

DHCP Server Override

DHCP Addr. Assignment Required

OEAP

Split Tunnel (Printers) Enabled

Management Frame Protection (MFP)

MFP Client Protection #

DTIM Period (in beacon intervals)

802.11a/n (1 - 255)

802.11b/g/n (1 - 255)

NAC

NAC State

Load Balancing and Bandwidth

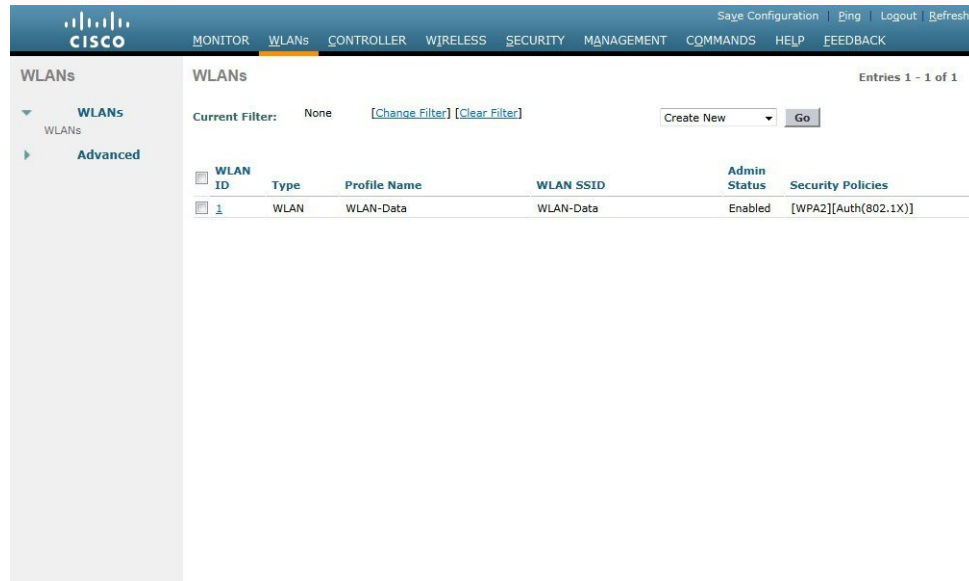
Configure Voice Wireless LAN

Wireless voice traffic is different from data traffic in that it cannot effectively handle delay and jitter as well as packet loss. To configure the voice wireless LAN, change the default QoS settings to Platinum and segment the voice traffic onto the voice wired VLAN.

To configure voice wireless LAN, perform the following steps:

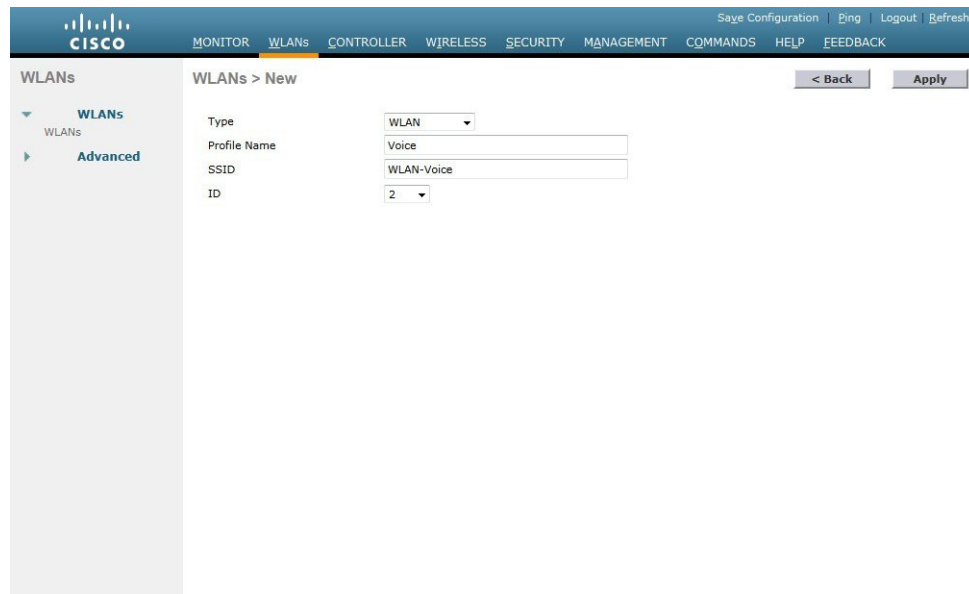
Procedure

- Step 1** Navigate to WLANs.
- Step 2** In the drop-down list, choose **Create New**, and then click **Go**.



Step 3 Enter the **Profile Name**. (Example: Voice)

Step 4 In the **SSID** box, enter the voice WLAN name, and then click **Apply**. (Example: WLAN-Voice).



Step 5 On the **General** tab, to the right of Status, select **Enabled**.

Step 6 In the **Interface** list, choose the interface created in Procedure 2. (Example: Wireless-Voice)

The screenshot shows the Cisco WLAN configuration interface for a profile named 'Voice'. The 'General' tab is selected, and the configuration includes:

- Profile Name: Voice
- Type: WLAN
- SSID: WLAN-Voice
- Status: Enabled
- Security Policies: [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
- Radio Policy: All
- Interface/Interface Group(G): wireless-voice
- Multicast Vlan Feature: Enabled
- Broadcast SSID: Enabled

Foot Notes:

- 1 Web Policy cannot be used in combination with IPsec
- 2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 4 Client MFP is not active unless WPA2 is configured
- 5 Learn Client IP is configurable only when HREAP Local Switching is enabled
- 6 WMM and open or AES security should be enabled to support higher 11n rates
- 7 Multicast Should Be Enabled For IPV6.
- 8 Band Select is configurable only when Radio Policy is set to 'All'.
- 9 Value zero implies there is no restriction on maximum clients allowed.
- 10 MAC Filtering is not supported with HREAP Local authentication
- 11 MAC Filtering should be enabled.
- 12 Guest tunneling, Local switching, DHCP Required should be disabled.
- 13 Max-associated-clients feature is not supported with HREAP Local Authentication.

Step 7 Click the **QoS** tab, and in the **Quality of Service (QoS)** list, choose Platinum and enable AVC.

The screenshot shows the Cisco WLAN configuration interface for a profile named 'Voice', with the 'QoS' tab selected. The configuration includes:

- Quality of Service (QoS): Platinum (voice)
- Application Visibility: Enabled
- AVC Profile: none
- Netflow Monitor: none

Override Per-User Bandwidth Contracts (kbps) ¹⁶

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

Clear

Override Per-SSID Bandwidth Contracts (kbps) ¹⁶

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0

- Step 8** Click the **Advanced** tab, and then clear **Coverage Hole Detection**, clear **Aironet IE**, enable **Allow AAA Override**, and then click **Apply**.

The screenshot shows the Cisco configuration interface for a WLAN named 'Voice'. The 'Advanced' tab is active, displaying various configuration options. The 'Allow AAA Override' checkbox is checked and labeled 'Enabled'. 'Coverage Hole Detection' is unchecked. 'Enable Session Timeout' is checked with a value of 1800. 'Aironet IE' is unchecked. 'DHCP' settings include 'DHCP Server' (unchecked) and 'DHCP Addr. Assignment' (unchecked). 'OEAP' settings include 'Split Tunnel (Printers)' (unchecked). 'Management Frame Protection (MFP)' is set to 'Optional'. 'DTIM Period (in beacon intervals)' is set to 1 for both 802.11a/n and 802.11b/g/n. 'NAC State' is set to 'None'. The 'Apply' button is highlighted with a mouse cursor.

Configure the Remote LAN

A remote LAN is similar to a WLAN except it is mapped to one of the Ethernet ports on the back of the Cisco Aironet 1815 Teleworker Access Point.

To configure the remote LAN, perform the following steps:

Procedure

- Step 1** Navigate to WLANs.
- Step 2** In the drop-down list, choose **Create New**, and then click **Go**.

The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WLANs' section is active, showing a table of existing WLANs. The table has columns for 'WLAN ID', 'Type', 'Profile Name', 'WLAN SSID', 'Admin Status', and 'Security Policies'. Two entries are listed: ID 1 (WLAN, WLAN-Data, WLAN-Data, Enabled, [WPA2][Auth(802.1X)]) and ID 2 (WLAN, Voice, WLAN-Voice, Enabled, [WPA2][Auth(802.1X)]).

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	WLAN-Data	WLAN-Data	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	Voice	WLAN-Voice	Enabled	[WPA2][Auth(802.1X)]

Step 3 In the **Type** list, choose **Remote LAN**.

Step 4 Enter the **Profile Name**, and then click **Apply**. (Example: LAN)

The screenshot shows the 'WLANs > New' configuration page. The 'Type' dropdown is set to 'Remote LAN'. The 'Profile Name' text box contains 'LAN'. The 'ID' dropdown is set to '3'. There are '< Back' and 'Apply' buttons at the top right of the form area.

Step 5 On the **General** tab, to the right of **Status**, select **Enabled**.

Step 6 In the Interface list, choose the interface created in Procedure 3. (Example: Remote-LAN)

The screenshot shows the Cisco WLAN configuration interface for 'Remote-LAN1'. The 'Security' tab is selected, and the following fields are visible:

- Profile Name: Remote-LAN1
- Type: Remote-LAN
- SSID: Remote-LAN1
- Status: Enabled
- Egress Interface: remote-lan
- NAS-ID: none

Foot Notes:

- 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 8 Value zero implies there is no restriction on maximum clients allowed.
- 17 IPv6 DHCP server configuration is not supported for remote-lan.

Step 7 Click the **Security** tab.

Step 8 On the Layer 2 tab, clear **MAC Filtering** and select **802.1x**.

The screenshot shows the Cisco WLAN configuration interface for 'Remote-LAN1' in the 'Security' tab, specifically the 'Layer 2' sub-tab. The following fields are visible:

- Layer 2 Security: 802.1X
- MAC Filtering:

Foot Notes:

- 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 8 Value zero implies there is no restriction on maximum clients allowed.
- 17 IPv6 DHCP server configuration is not supported for remote-lan.

Step 9 On the **AAA Servers** tab, select **RADIUS** servers and the click **Apply**.

The screenshot shows the Cisco WLAN configuration interface for 'Remote-LAN1'. The 'AAA Servers' tab is selected, displaying the configuration for RADIUS Servers. The 'Authentication Servers' and 'Accounting Servers' sections are both enabled. The first server in both sections is configured with IP: 172.20.229.11 and Port: 1812. The 'EAP Parameters' section has the 'Enable' checkbox unchecked. The 'RADIUS Server Accounting' section has the 'Interim Update' checkbox checked and the 'Interim Interval' set to 0. The 'LDAP Servers' section has one server set to 'None'. Below the configuration area, there are 'Foot Notes' providing additional information about client exclusion, timeout values, and IPv6 DHCP support.

WLANs > Edit 'Remote-LAN1'

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

	Authentication Servers	Accounting Servers	EAP Parameters
Server 1	<input checked="" type="checkbox"/> Enabled IP:172.20.229.11, Port:1812	<input checked="" type="checkbox"/> Enabled IP:172.20.229.11, Port:1813	Enable <input type="checkbox"/>
Server 2	None	None	
Server 3	None	None	
Server 4	None	None	
Server 5	None	None	
Server 6	None	None	

RADIUS Server Accounting

Interim Update Interim Interval 0

LDAP Servers

Server 1 None

Foot Notes

3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
 8 Value zero implies there is no restriction on maximum clients allowed.
 17 IPv6 DHCP server configuration is not supported for remote-lan.

Step 10 Create an AP Group for the Teleworkers.

The screenshot shows the Cisco AP Groups configuration page. The 'Add New AP Group' form is displayed with the following fields: 'AP Group Name' set to 'Teleworkers' and 'Description' set to 'AP Group for Teleworkers'. There are 'Add' and 'Cancel' buttons below the form. Below the form, there is a table with columns for 'AP Group Name' and 'AP Group Description', showing a single entry: 'default-group'.

WLANs > AP Groups

Entries 1 - 1 of 1 Add Group

Add New AP Group

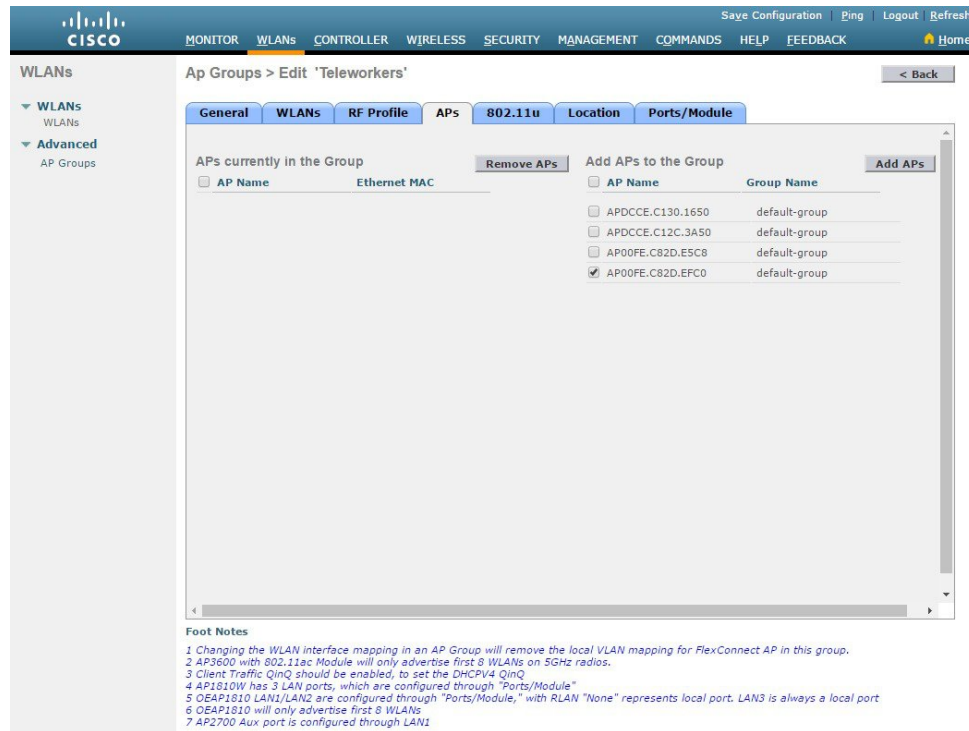
AP Group Name Teleworkers

Description AP Group for Teleworkers

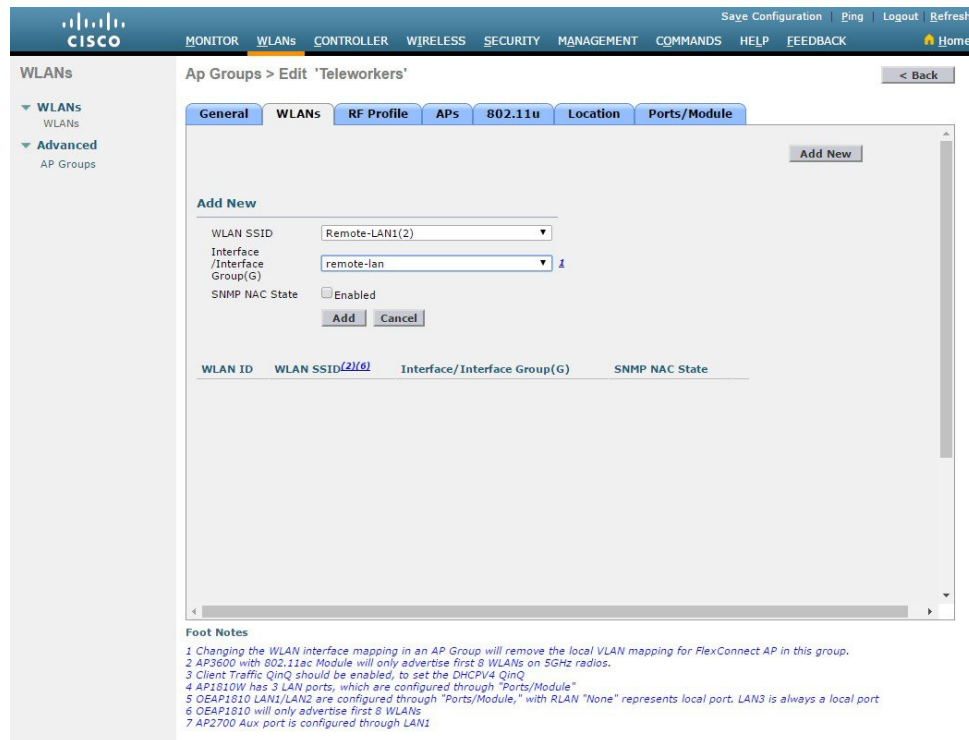
Add Cancel

AP Group Name	AP Group Description
default-group	

Step 11 Add the Cisco Aironet 1815T(Teleworker) Access Point to the AP Group.



Step 12 Associate the WLAN and RLAN to the AP Group.



Step 13 Assign VLANs to Wired LAN ports. One can Enable/Disable Wired LAN ports along with PoE on PSE LAN1 port.

The screenshot shows the Cisco configuration interface for the 'Teleworkers' AP Group. The 'Ports/Module' tab is selected, displaying the following configuration options:

LAN Ports

LAN (s)	ENABLE	POE	RLAN
LAN1 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Remote-LAN
LAN2	<input checked="" type="checkbox"/>		Remote-LAN
LAN3	<input type="checkbox"/>		None

External module 3G/4G

LAN	ENABLE	RLAN
Module	<input type="checkbox"/>	None

Foot Notes

- 1 Changing the WLAN Interface mapping in an AP Group will remove the local VLAN mapping for FlexConnect AP in this group.
- 2 AP3600 with 802.11ac Module will only advertise first 8 WLANs on 5GHz radios.
- 3 Client Traffic QinQ should be enabled, to set the DHCPV4 QinQ
- 4 AP1810W has 3 LAN ports, which are configured through "Ports/Module"
- 5 OEAP1810 LAN1/LAN2 are configured through "Ports/Module," with RLAN "None" represents local port. LAN3 is always a local port.
- 6 OEAP1810 will only advertise first 8 WLANs
- 7 AP2700 Aux port is configured through LAN1