Cisco Aironet® 1815T (Teleworker) Access Point Deployment Guide

First Published: 2017-08-18

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

Introduction

Technology Use Case

Providing employees access to corporate network and services from a remote environment poses challenges for both the end user and IT operations. For the home-based teleworker, it is critical that access to business services be reliable and consistent, providing an experience that is as similar as sitting in a cubicle or office in the organization's facility. In addition, the solution must also support a wide range of teleworking employees who have varying skill sets, making it critical to have a streamlined and simplified way to implementdevices that allow for access to the corporate environment.

Cisco Aironet® 1815 Teleworker Access Point provides secure communications from a controller to an access point at a remote location, seamlessly extending the corporate WLAN over the Internet to an employee's residence. The user's experience at the remote location is the same as it would be at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the access point and the controller ensures that all communications have the highest level of security.

Use Case:Teleworker with Wireless Devices

Teleworkers require always-on secure access to networked business services from a remote home office. Wireless access provides easy mobility and setup within the home office, and consistent device configuration allows for easy mobilitybetween the home office and on site at the corporate location.

This design guide enables the following network capabilities:

- Common wireless device configuration for onsite and teleworker wireless access
- Authentication through IEEE 802.1x for employees and encryption for all information sent and received to the organization’s main location
- Simplified IT provisioning for the home office, which reduces setup time and supports varying levels of end-user skills
- Mobility and flexibility for voice endpoints at the teleworker location

CHAPTER 2

Design Overview

Design Overview

The Cisco OfficeExtend solution is specifically designed for the teleworker who primarily uses wireless devices. The solution consists of the following components:

- Cisco Aironet 1815T(Teleworker) Access Point
- Cisco 2500, Cisco 3504, Cisco 5500 Series, Cisco 2500 Series, Cisco 5500, Cisco 8500 Series Wireless LAN Controller

Deployment Components

The OfficeExtend deployment is built around three main components: Cisco wireless LAN controllers, Cisco OfficeExtend Access Points and Corporate Firewall.

Cisco Wireless LAN Controllers

Cisco wireless LAN controllers are responsible for system-wide WLAN functions, such as security policies, intrusion prevention, RF management, quality of service (QoS), and mobility. They work in conjunction with Cisco OfficeExtend Access Points to support business-critical wireless applications for teleworkers. Cisco wireless LAN controllers provide the control, scalability, security, and reliability that network managers need to build a secure, scalable teleworker environment.

To allow users to connect their corporate devices to the organization's on-site wireless network, the Cisco OfficeExtend teleworking solution offers the same wireless Secure Set Identifiers (SSIDs) at teleworker's home as those that support data and voice inside the organization.

Cisco OfficeExtend Access Points

Cisco Aironet 1815T(Teleworker) Access Point cannot act independently of a wireless LAN controller (WLC). As the access point communicates with the WLC resources, it will download its configuration and synchronize its software/firmware image, if required. Cisco Aironet 1815T(Teleworker) Access Point establishes a secure Datagram Transport Layer Security (DTLS) connection between the access point and the controller to offer remote WLAN connectivity using the same profile as at the corporate office. Secure tunneling allows all traffic to be validated against centralized security policies and minimizes the management overhead associated with home-based firewalls.

Cisco OfficeExtend delivers full 802.11ac wireless performance and avoids congestion caused by residential devices because it operates simultaneously in the 2.4-GHz and the 5-GHz radio frequency bands. The Cisco Aironet 1815T(Teleworker) Access Point provides wired and wireless segmentation of home and corporate traffic, which allows for home device connectivity without introducing security risks to corporate policy.

Corporate Firewall

The Wireless LAN Controller should be placed in DMZ and the corporate Firewall must allow CAPWAP Control and CAPWAP Data traffic through the Firewall to the Wireless LAN Controller.The general configuration on the firewall is to allow CAPWAP control and CAPWAP management port numbers through the firewall.

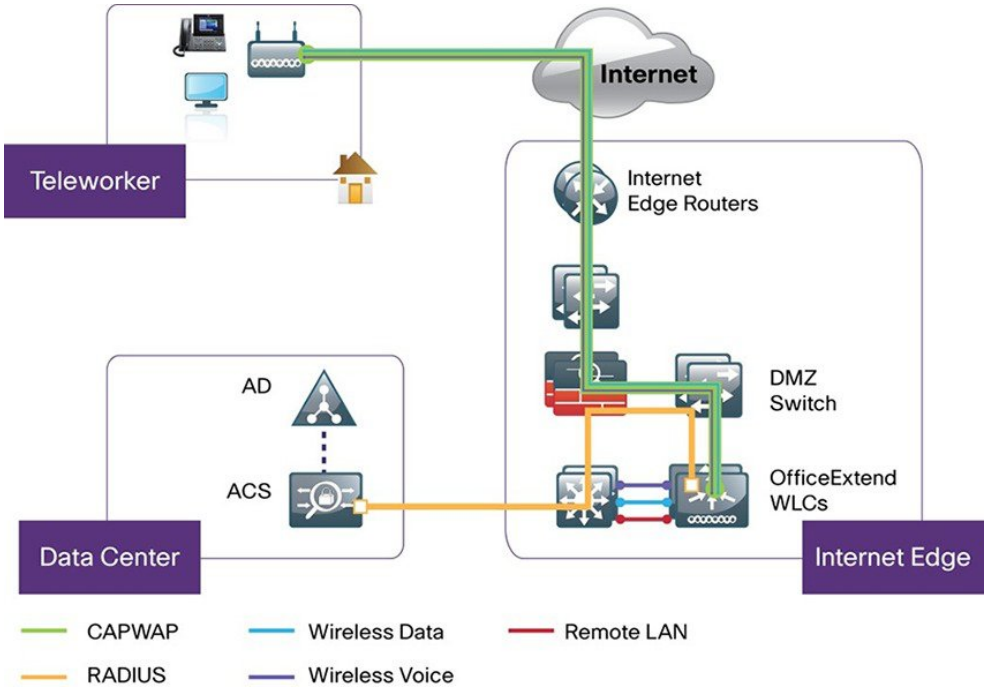
Note The UDP 5246 and 5247 ports need to be opened on the firewall for communication between the Wireless LAN controller and the Cisco OfficeExtend Access Point 1810.

Design Models

For the most flexible and secure deployment of Cisco OfficeExtend, deploy a dedicated controller pair for Cisco OfficeExtend using the Cisco 8500 and 5500 LAN Controllers. In the dedicated design model, the controller is directly connected to the Internet edge demilitarized zone (DMZ) and traffic from the Internet is

terminated in the DMZ versus on the internal network, while client traffic is still directly connected to the internal network.

Figure 1: Cisco OfficeExtend dedicated design model



Cisco Aironet 1815T(Teleworker) Workflow

The following steps describe the workflow carried out by the teleworker to connect the 1815T Access Point to the corporate Wireless LAN Controller:

- A user is given an 1815T Access Point primed with the IP address of the corporate Wireless LAN controller. Alternatively, the teleworker can prime the 1815T Access Point by entering the IP address of the Wireless LAN Controller in the local configuration screen of the OfficeExtend Access Point
- The teleworker connects the WAN port on OfficeExtend Access Point to one of the home internet router LAN interfaces
- The 1815T Access Point will obtain an IP address from the home internet router and will initiate a join request to the corporate Wireless LAN Controller
- After the 1815T Access Point joins the corporate Wireless LAN Controller, it advertises the corporate SSID, extending the same security methods and services across the WAN to the teleworker's remote home location
- If Remote LAN (RLAN) is configured on Wired LAN ports of the 1815T Access Points, devices can be connected to the corporate network via the Wired LAN ports
- Teleworker can additionally configure a Personal SSID on the 1815T Access Point for home networking

CHAPTER 3

Understanding ports on Cisco Aironet 1815t

Interfaces

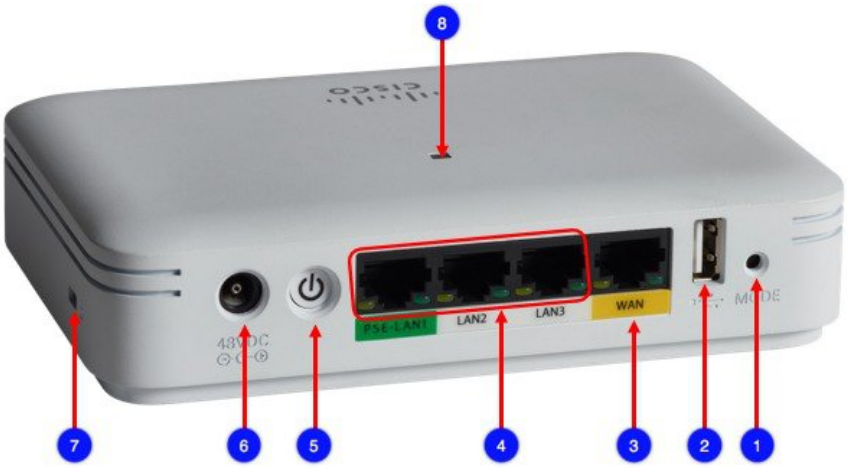
The Cisco AIR-AP1815T has the following interfaces:

- One 10/100/1000 BASE-T (Ethernet) WAN Interface
- Three 10/100/1000 BASE-T (Ethernet) LAN Interfaces
  - Auto-MDIX (automatically support either straight through or crossover cables)
  - 802.3af PSE power on one LAN 1 Ethernet Interface
- Local Power DC Jack
- Recovery push button (enables partial or full system configuration recovery)
- One multi-color LED Status indicator
  - Colors supported are Red, Green, Amber
- Multi-color LED Link Status indicator for each LAN Port
- Antennas
  - 2x2 AP

Interfaces as noted in Figure below	Interfaces as shown on AIR-AP1815T	Description
1	Mode	When pressed for more than 20s, it will reset the AIR-AP1815T to factory defaults
2	USB	USB (Future Use)
3	WAN	WAN Port for connectivity to the internet

Interfaces as noted in Figure below	Interfaces as shown on AIR-AP1815T	Description
4	PSE-LAN1, LAN2, LAN3	LAN Ethernet Ports, PSE-LAN1 and LAN2 can be tunneled back to WLC. LAN 3 is a dedicated LAN port for accessing local UI of the AIR-AP1815T.
5	Power On/Off Push Button	Power On/Off Push Button
6	48V DC	48V DC port to connect AIR-PWR-D
7	Security	Kensington Security Slot
8	LED	Multi-color LED Status indicator. Colors supported are Red, Green, Amber

Note LAN 3 is a dedicated local interface used to access the local UI of the Access Point. PSE-LAN1 and LAN2 can also be used as local interface if no RLAN is configured on them.



CHAPTER 4

Software Features on Cisco Aironet AIR-AP1815T

The Cisco Aironet® 1815T(Teleworker) Access Point supports a number of features:

- **Access Point Mode**
  - Cisco Aironet 1815t supports FlexConnect Mode with sub mode as OEAP
- **DTLS**
  - Control–DTLS is enabled for Control
  - Data–DTLS is enabled for client traffic tunneled back to the corporate Wireless LAN Controller
- **CDP and LLDP**
  - Ethernet Ports– Cisco Aironet 1815t does not support CDP or LLDP on Ethernet ports. LAN1 (PSE) has fixed power (not negotiable)
- **Authentication and Security**
  - Advanced Encryption Standard (AES) for Wi-Fi Protected Access 2 (WPA2)
  - 802.1X, RADIUS authentication, authorization and accounting (AAA) on WLAN and RLAN
  - 802.11i
  - MAC filtering
- **Personal SSID support**
  - Personal SSID support for local home networking
  - LAN 3 is a dedicated local port for local AP access
- **WLAN and RLAN**
  - A total of 8 (WLAN + RLAN) is supported on Cisco Aironet 1815T. One can have more than 8 (WLAN + RLAN) associated on the AP group but only the first 8 (WLAN + RLAN) would be usable.

CHAPTER 5

Configuring WLC

Configure the WLC for NAT

The Internet edge firewall translates the IP address of the WLC management interface in the DMZ to a publicly reachable IP address so Cisco Aironet 1815 Teleworker Access Point at teleworker locations can reach the WLC. However, in order for the Cisco Aironet 1815T(Teleworker) Access Point to communicate with the WLC, the publicly reachable address must also be configured on the WLC management interface.

To configure the WLC for NAT, perform the following steps:

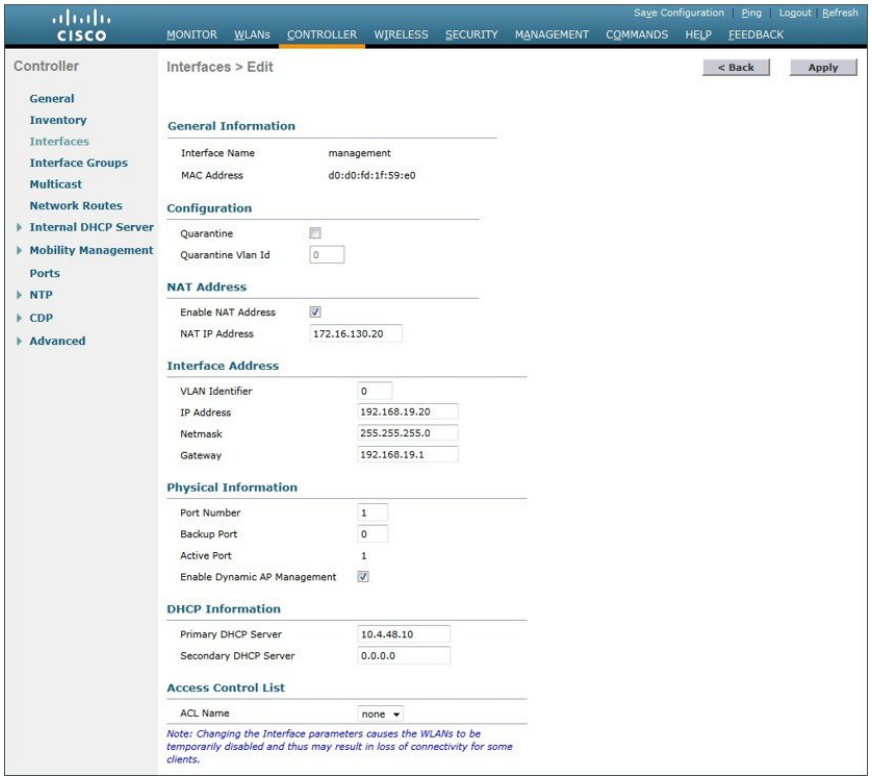
Procedure

Step 1 In **Controller** > **Interfaces**, click the management interface.

Step 2 Select Enable NAT Address.

Step 3 In the NAT IP Address box, enter the publicly reachable IP address, and then click Apply. (Example: 172.16.130.20)

Note The NAT IP Address must be the external, globally unique IP address that the Wireless LAN Controller displays on the Internet. This allows the WLC to place this IP address into the CAPWAP discovery response packet prior to encryption. The address shown here is an RFC-1918, private IP address and is used in this guide only for documentation purposes.



Configuring the Time Zone

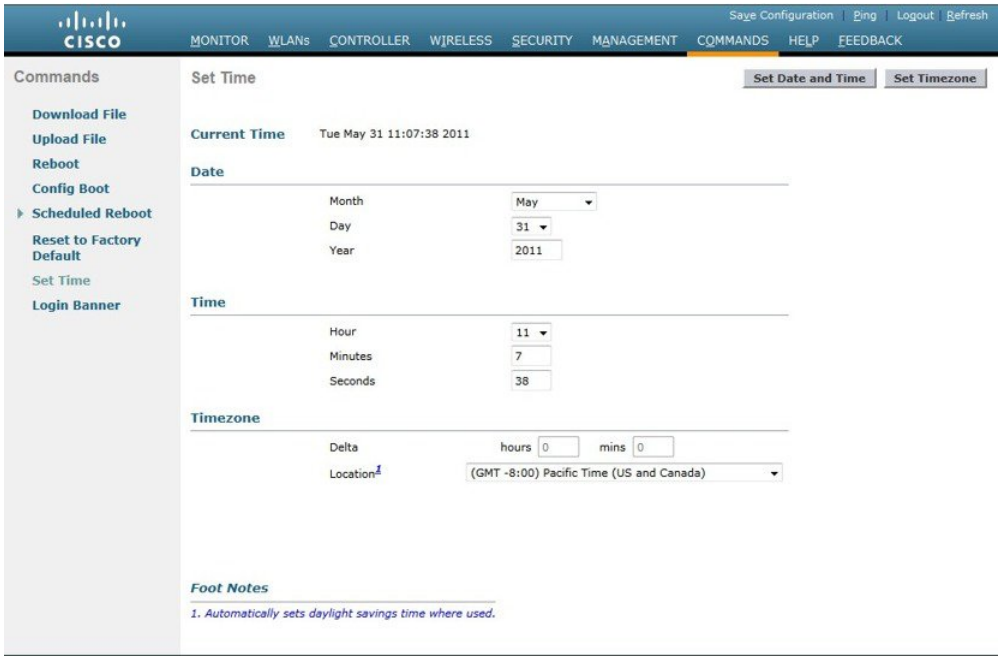
To configure the time zone, perform the following steps:

Procedure

Step 1 Navigate to **Commands** > **Set Time**.

Step 2 In the Location list, choose the time zone that corresponds to the locationof the WLC.

Step 3 Click Set Timezone.



Configuring SNMP

To configure SNMP, perform the following tasks:

Procedure

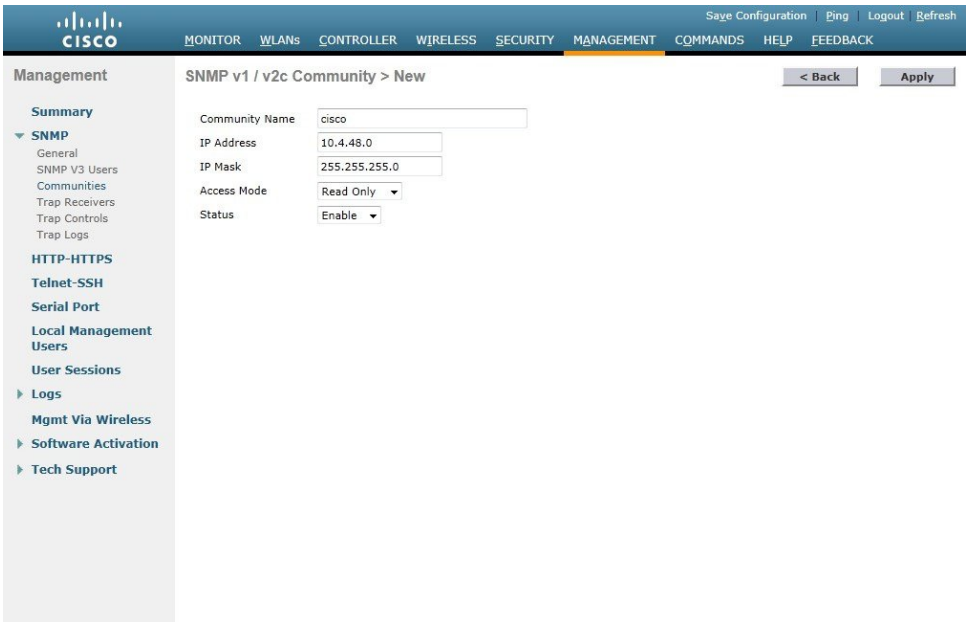
Step 1 In **Management** > **SNMP** > **Communities**, click **New**.

Step 2 Enter the **Community Name**. (Example: cisco)

Step 3 Enter the IP Address. (Example: 10.4.48.0)

Step 4 Enter the IP Mask. (Example: 255.255.255.0)

Step 5 In the **Status** list, choose **Enable**, and then click **Apply**.



Step 6 In **Management** > **SNMP** > **Communities**, click **New**.

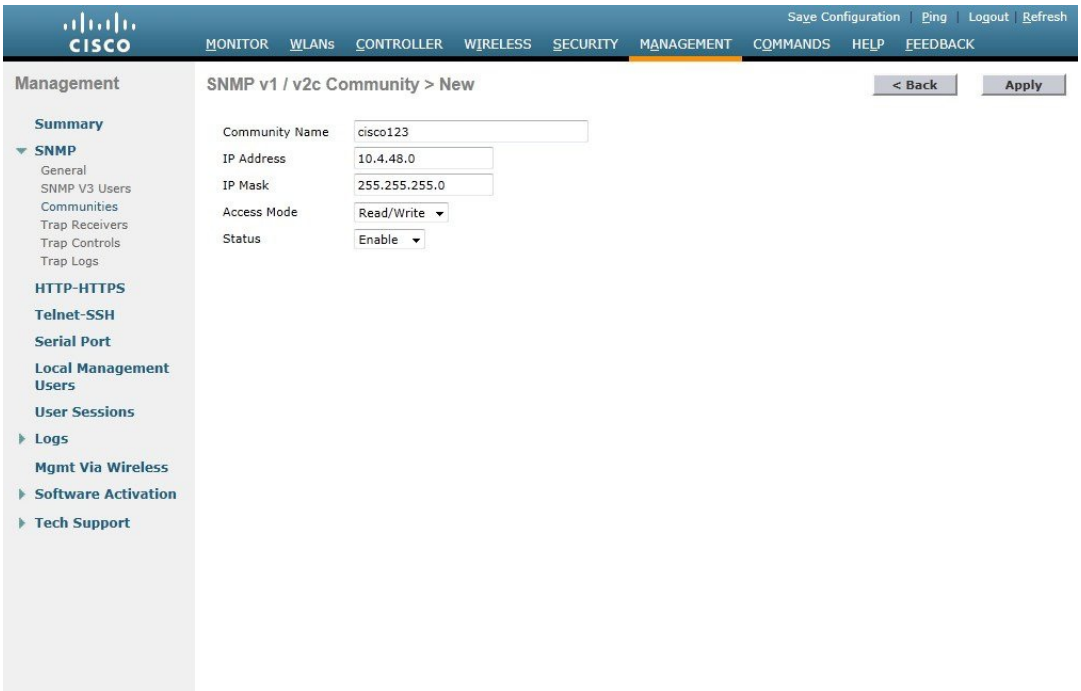
Step 7 Enter the **Community Name**. (Example: cisco123)

Step 8 Enter the **IP Address**. (Example: 10.4.48.0)

Step 9 Enter the **IP Mask**. (Example: 255.255.255.0)

Step 10 In the **Access Mode** list, choose Read/Write.

Step 11 In the **Status** list, choose **Enable**, and then click **Apply**.

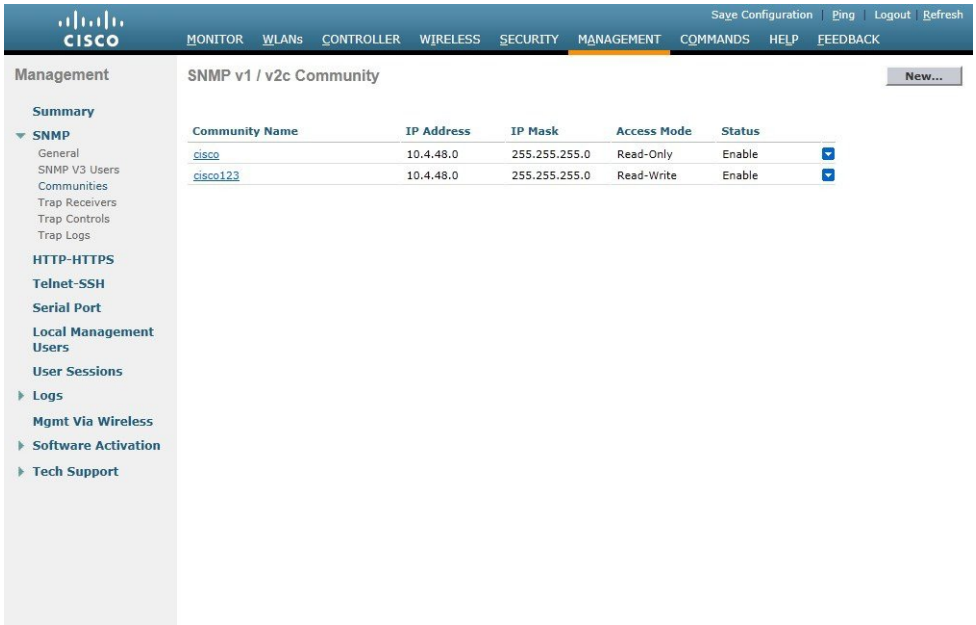


Step 12 Navigate to **Management** > **SNMP** > **Communities**.

Step 13 Point to the blue box for the public community, and then click **Remove**.

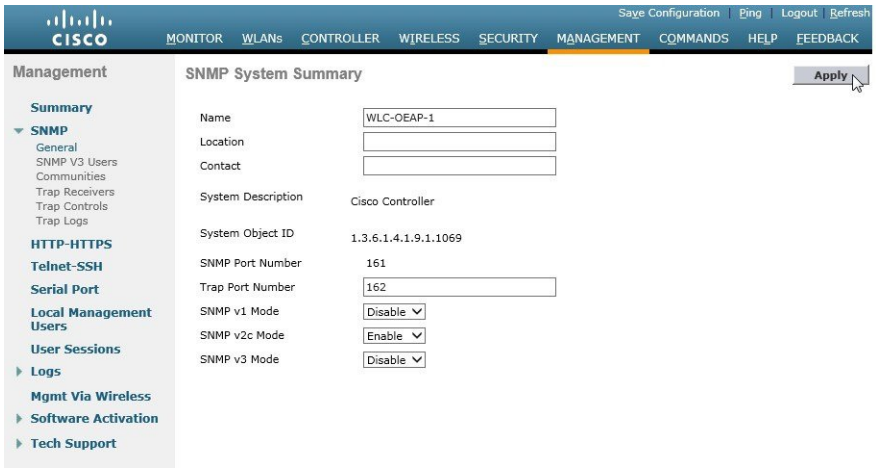
Step 14 On the "Are you sure you want to delete?" message,click **OK** .

Step 15 Repeat Step 13 and Step 14 for the private community.



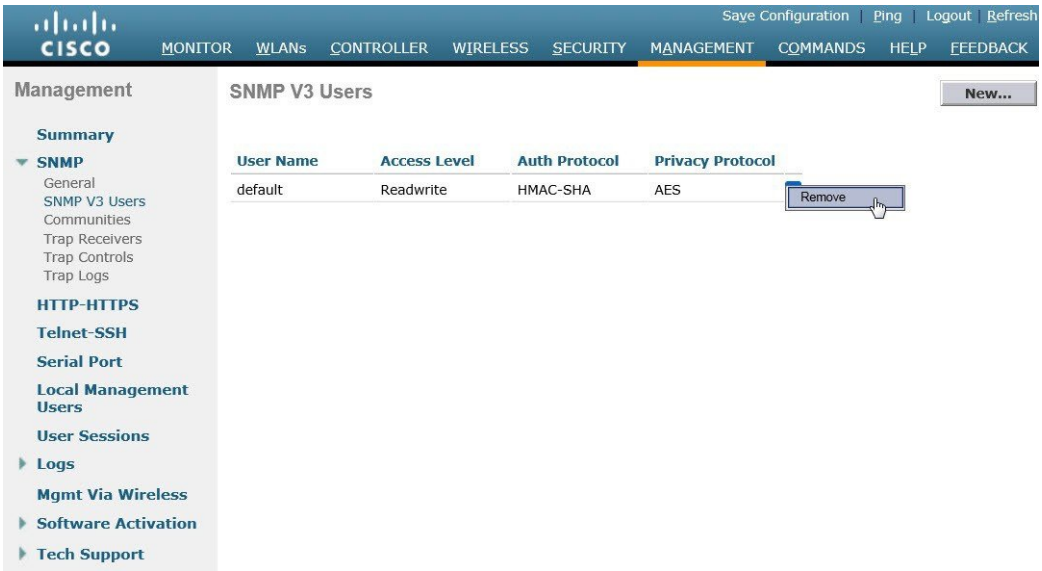
Step 16 Navigate to **Management** > **SNMP** > **General** and disable SNMP v3 Mode, and click **Apply**.

Figure 2:

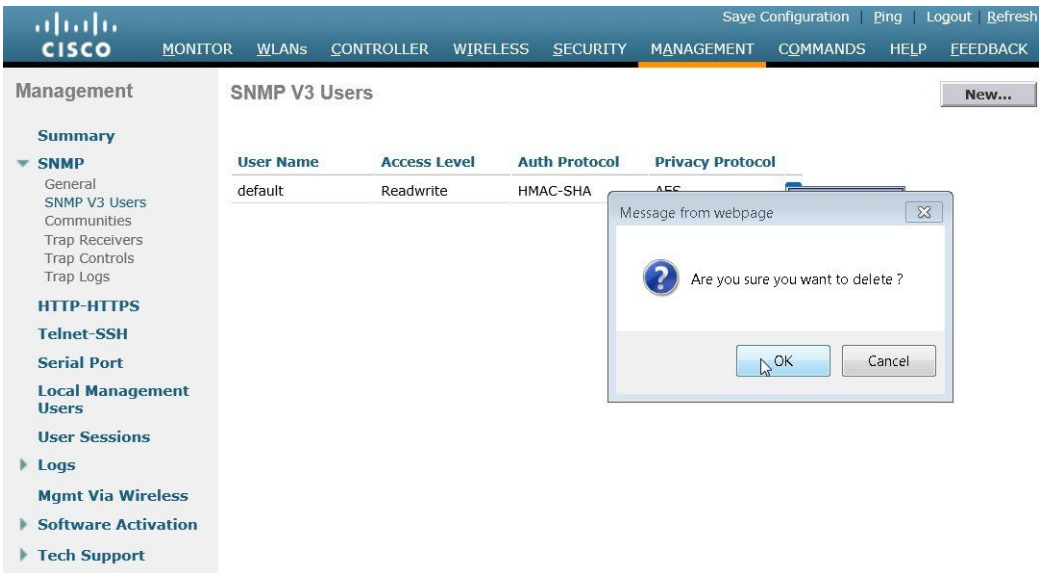


Step 17 Navigate to **Management** > **SNMP Communities** > **SNMP V3 Users**.

Step 18 On the right side of the default **User Name**, point and click the blue down arrow, and then click **Remove**.



Step 19 Press **OK** to confirm that you are sure you want to delete, then press **Save Configuration**.



Note Changes to the SNMP configuration may sometimes require that the WLC be rebooted.

Configuring Wireless User Authentication

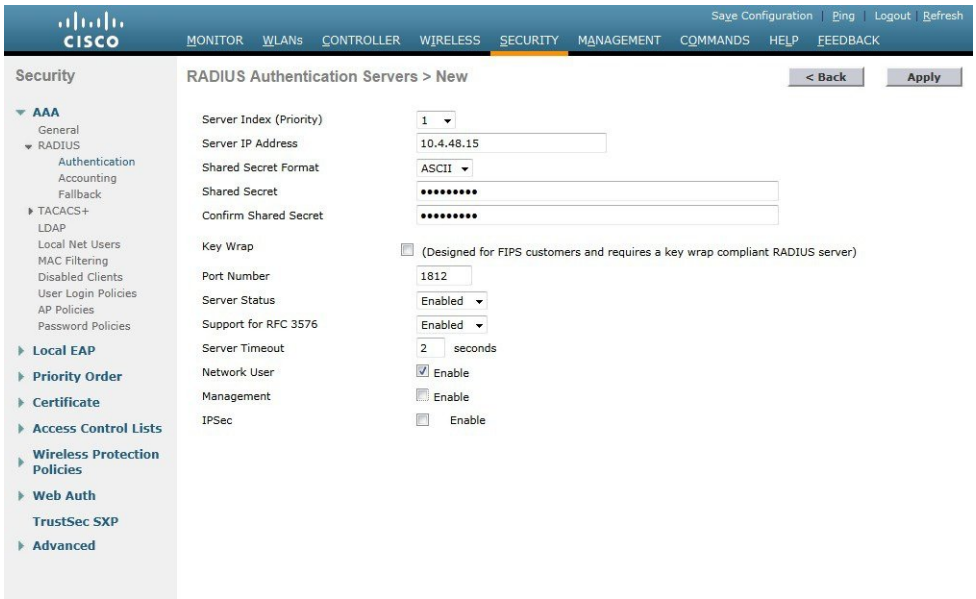
Procedure

Step 1 In **Security** > **AAA** > **Radius** > **Authentication**, click **New**.

Step 2 Enter the **Server IP Address**. (Example: 10.4.48.15)

Step 3 Enter and confirm the **Shared Secret**. (Example: SecretKey)

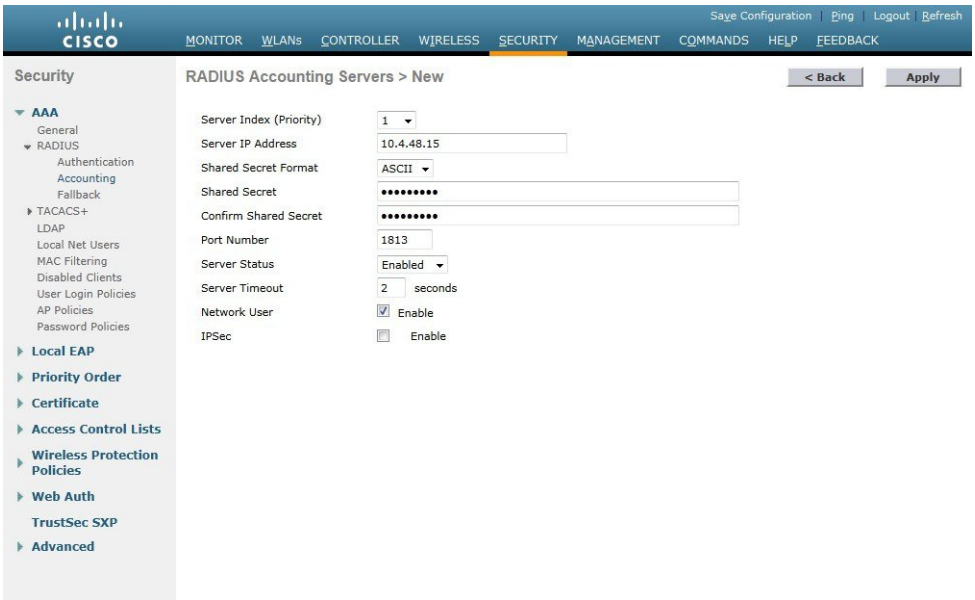
Step 4 To the right of **Management**, clear **Enable**, and then click **Apply**.



Step 5 To the right of Management, clear **Enable**, and then click **Apply**.

Step 6 Enter the **Server IP Address**. (Example: 10.4.48.15)

Step 7 Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security
RADIUS Accounting Servers > New
< Back
Apply
AAA
General
RADIUS
Authentication
Accounting
Fallback
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies
Local EAP
Priority Order
Certificate
Access Control Lists
Wireless Protection Policies
Web Auth
TrustSec SXP
Advanced
Server Index (Priority) 1
Server IP Address 10.4.48.15
Shared Secret Format ASCII
Shared Secret ••••••••••
Confirm Shared Secret ••••••••••
Port Number 1813
Server Status Enabled
Server Timeout 2 seconds
Network User Enable
IPSec Enable

CHAPTER 6

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

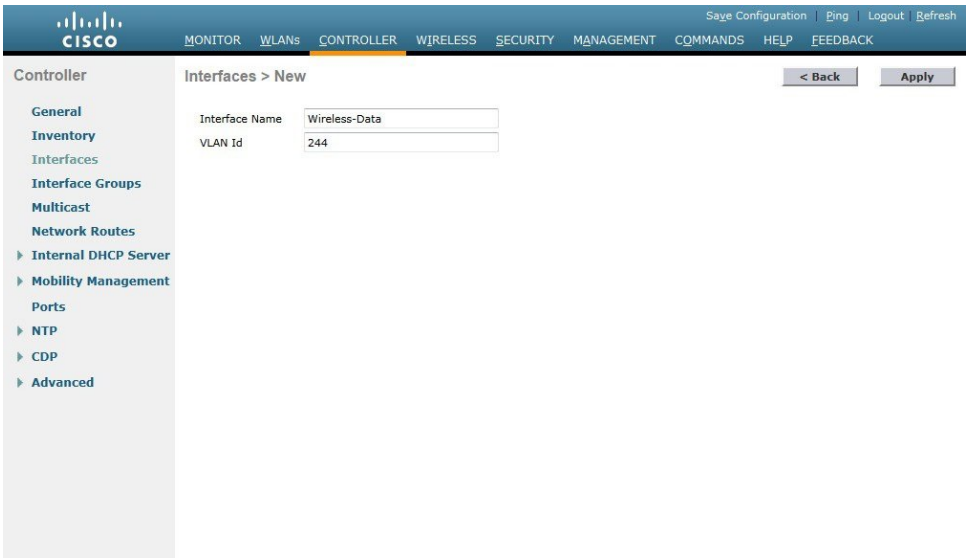
To create wireless LAN data interface, perform the following steps:

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)



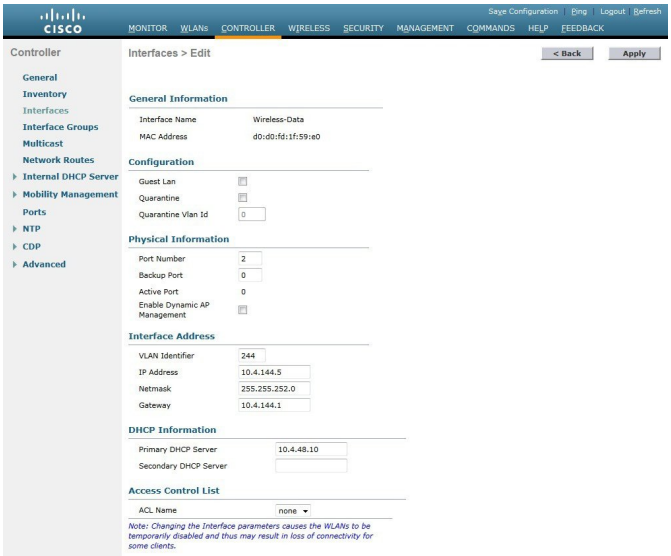
Step 4 In the **Port Number** box, enter the WLC interface that connects to the LAN distribution switch. (Example: 2)

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)



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.

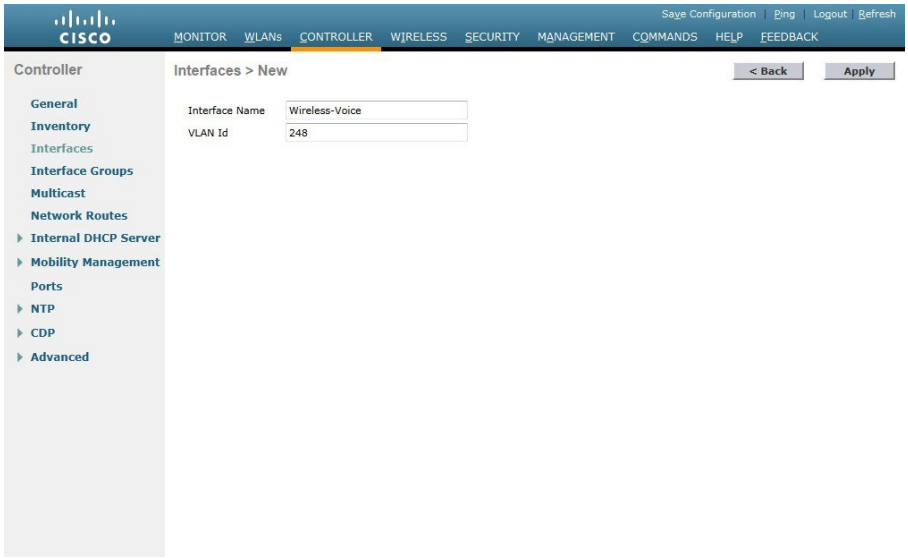
To create wireless LAN voice interface, perform the following steps:

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)



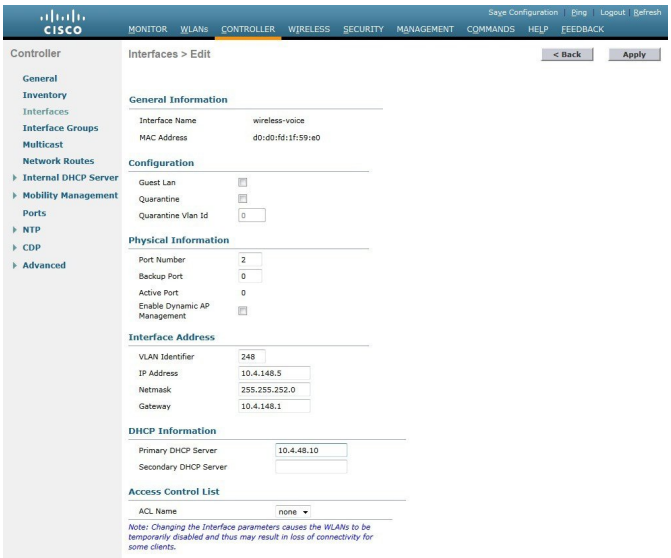
Step 4 In the **Port Number** box, enter the WLC interface that connects to the LAN distribution switch. (Example: 2)

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)



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.

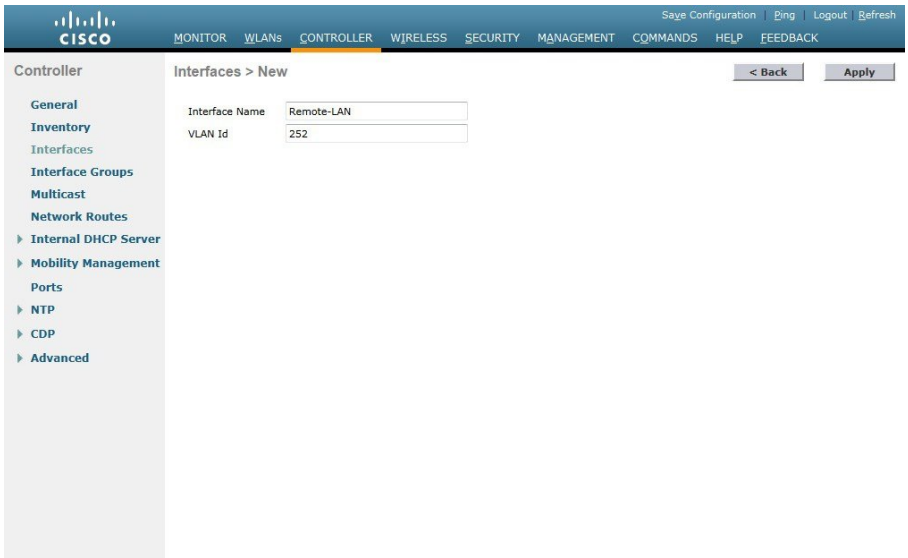
To create remote LAN interface, perform the following steps:

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)



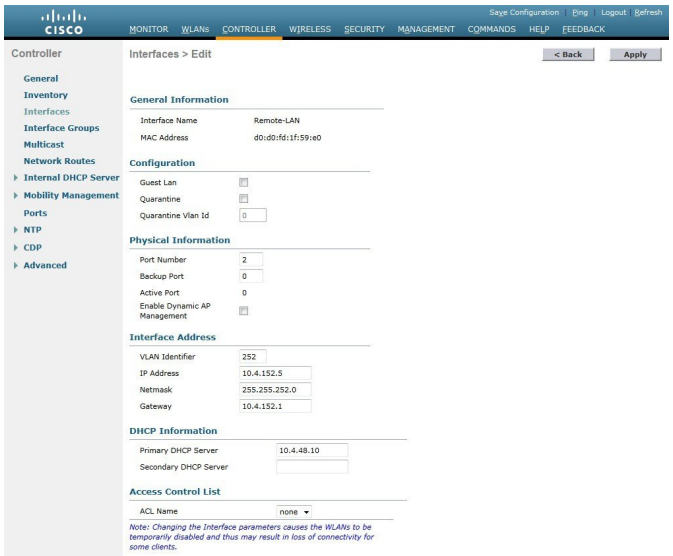
Step 4 In the **Port Number** box, enter the WLC interface that connects to the LAN distribution switch. (Example: 2)

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

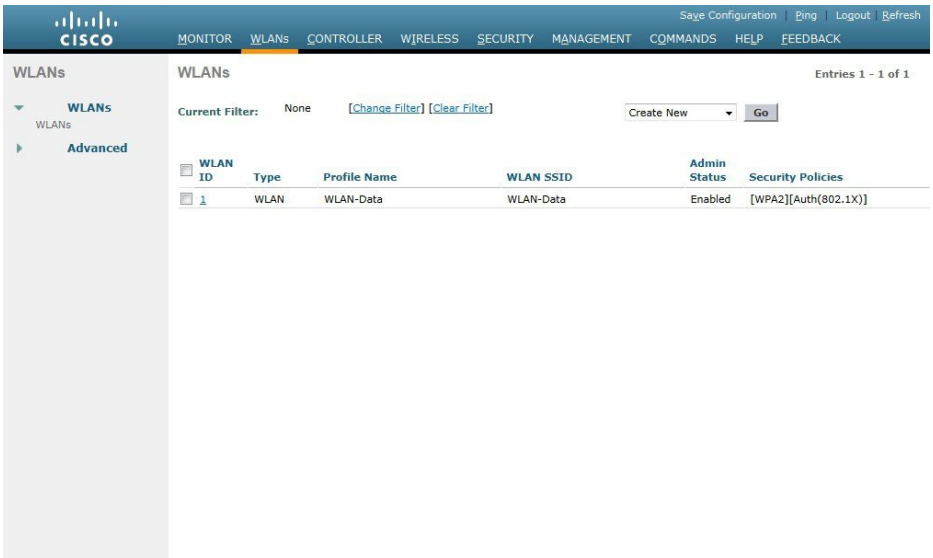
Wireless data traffic is different from voice traffic in that it can more efficiently handle delay and jitter as well as greater packet loss. For the data wireless LAN, keep the default QoS settings and segment the data traffic onto the data wired VLAN.

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

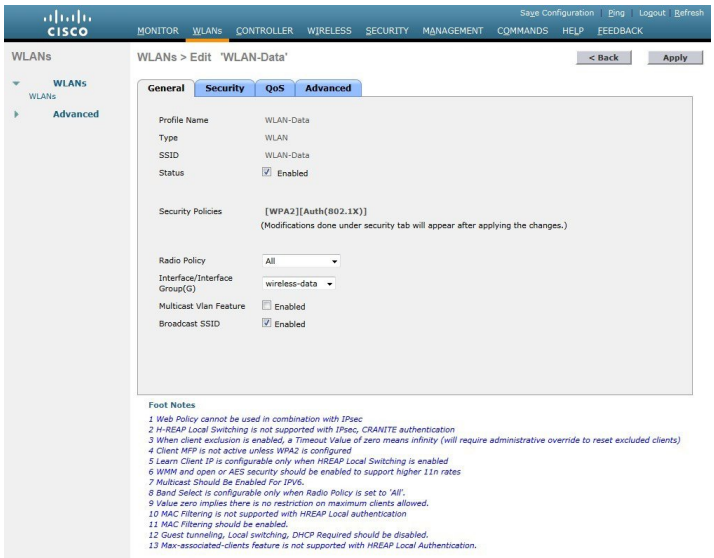
Procedure

Step 1 Navigate to **WLANs**.

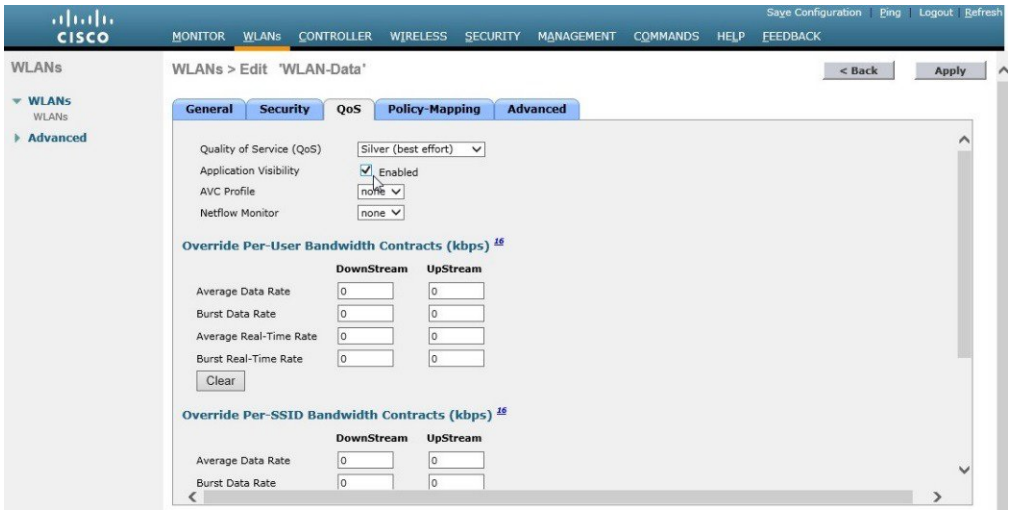
Step 2 Click the **WLAN ID** of the SSID created during platform setup.



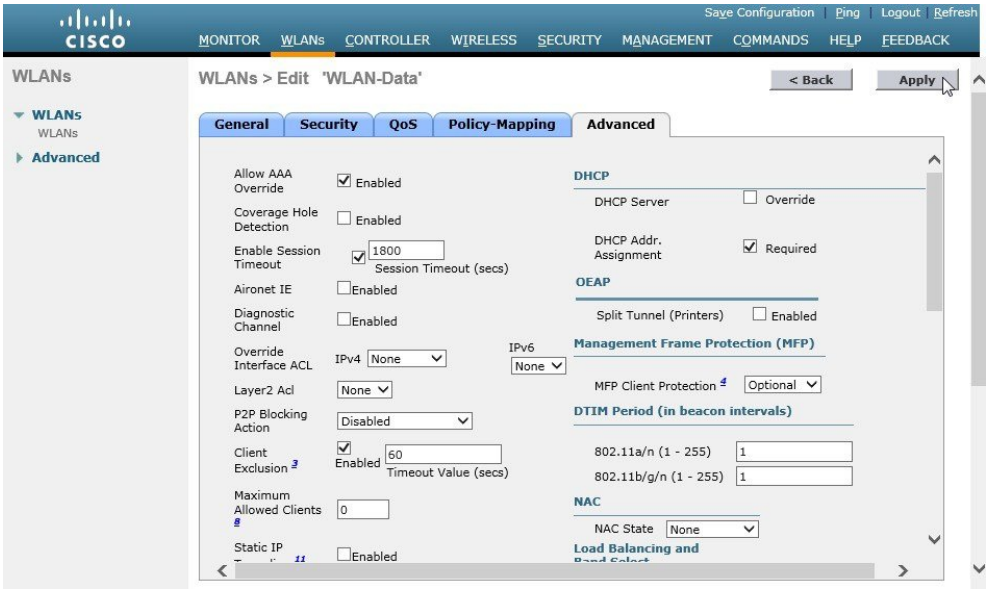
Step 3 On the General tab, in the Interface list, choose the interface created in Procedure 1.(Example: Wireless-Data) Next, enable Application Visibility and Control (AVC).



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**.



Configure Voice Wireless LAN

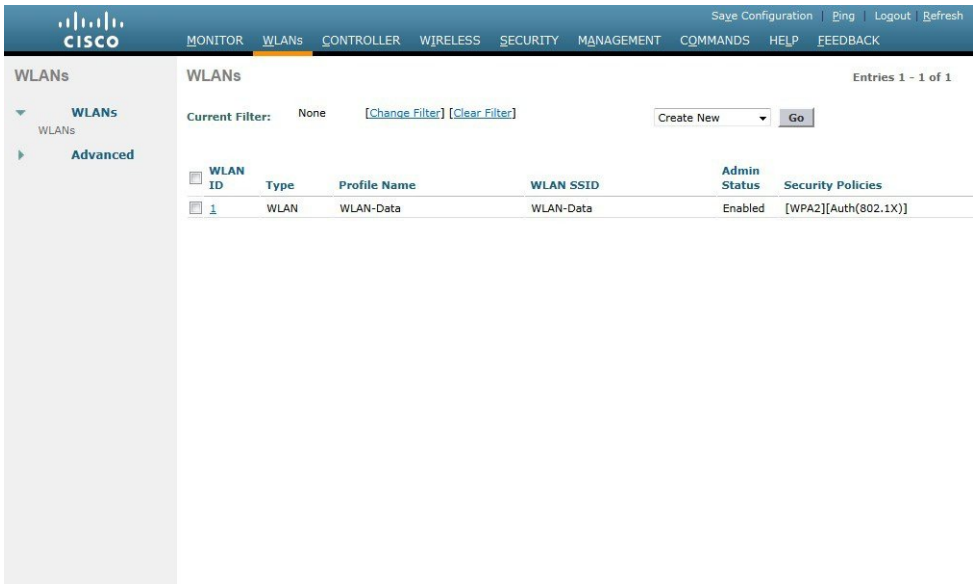
Wireless voice traffic is different from data traffic in that it cannot effectively handle delay and jitter as well as packet loss. To configure the voice wireless LAN, change the default QoS settings to Platinum and segment the voice traffic onto the voice wired VLAN.

To configures voice wireless LAN, perform the follwoing steps:

Procedure

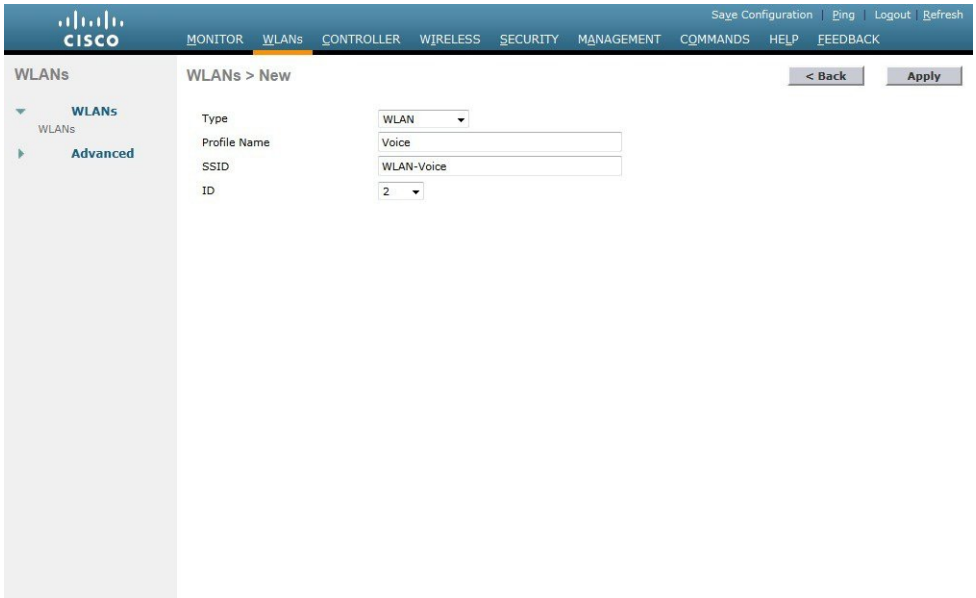
Step 1 Navigate to WLANs.

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



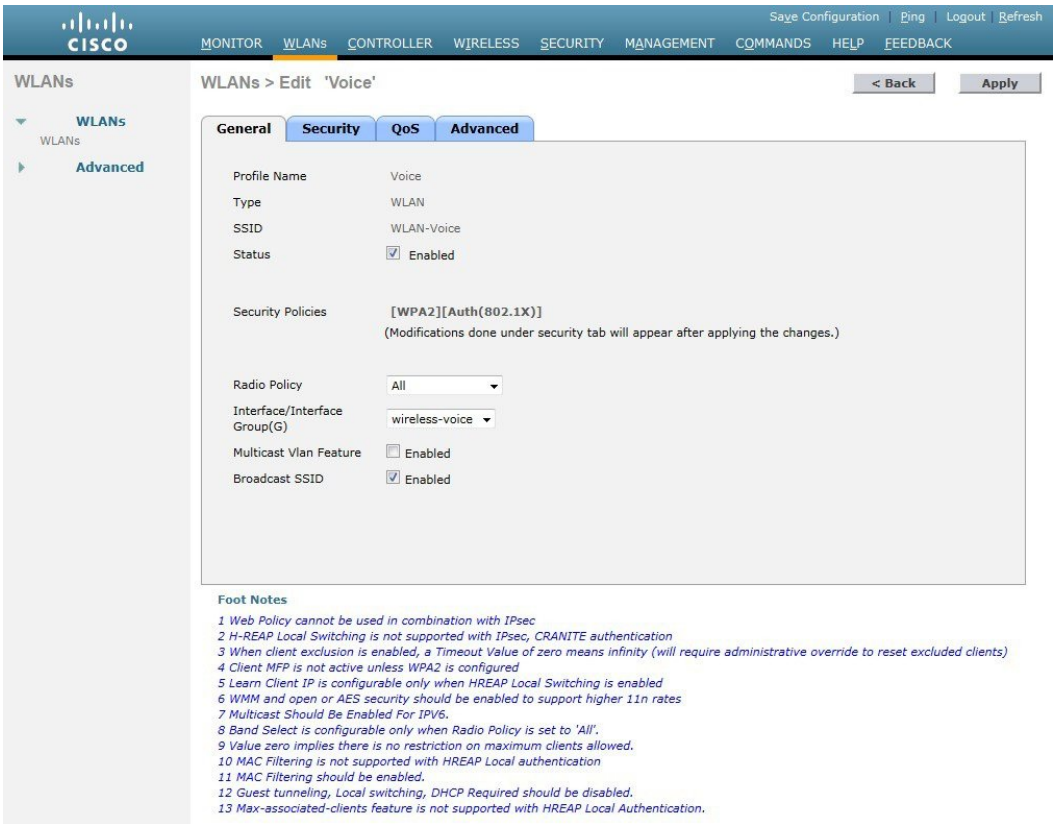
Step 3 Enter the **Profile Name**. (Example: Voice)

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

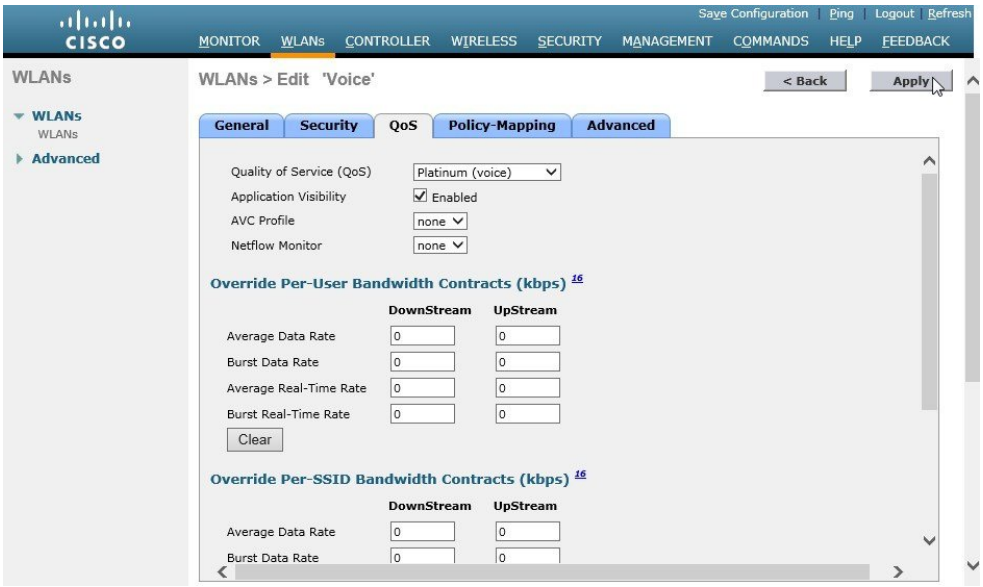


Step 5 On the **General** tab, to the right of Status, select **Enabled**.

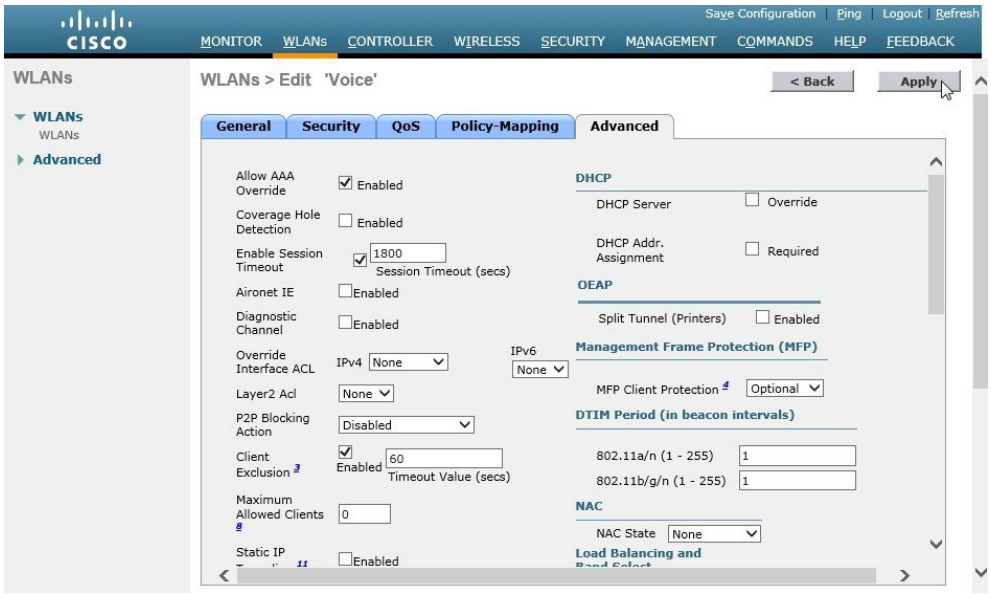
Step 6 In the **Interface** list, choose the interface created in Procedure 2. (Example: Wireless-Voice)



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



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



Configure the Remote LAN

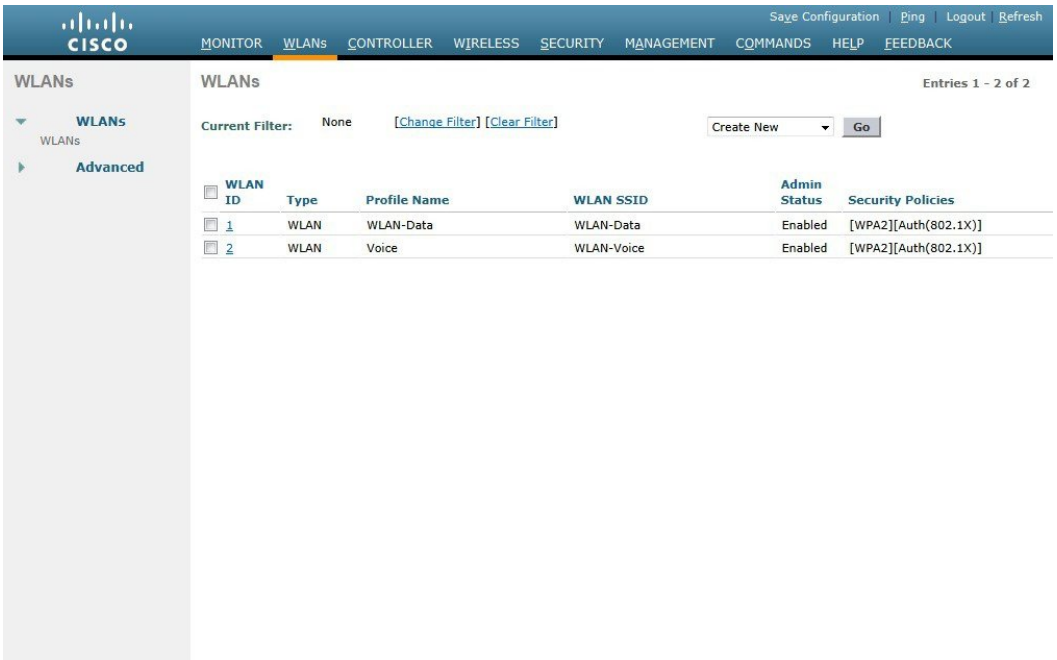
A remote LAN is similar to a WLAN except it is mapped to one of the Ethernet ports on the back of the Cisco Aironet 1815 Teleworker Access Point.

To configure the remote LAN, perform the following steps:

Procedure

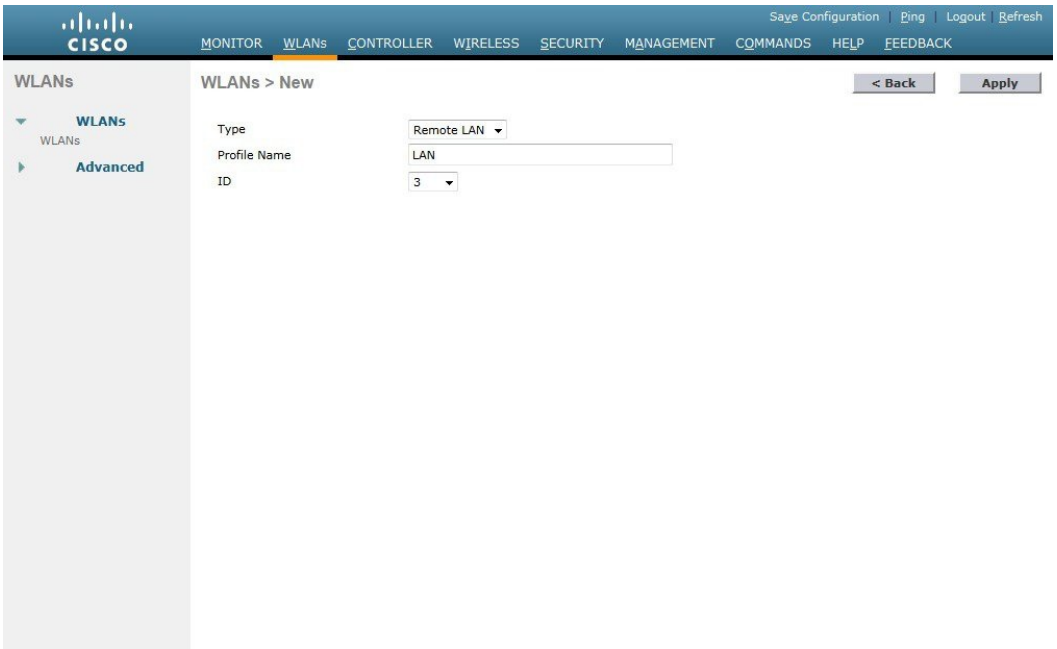
Step 1 Navigate to WLANs.

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



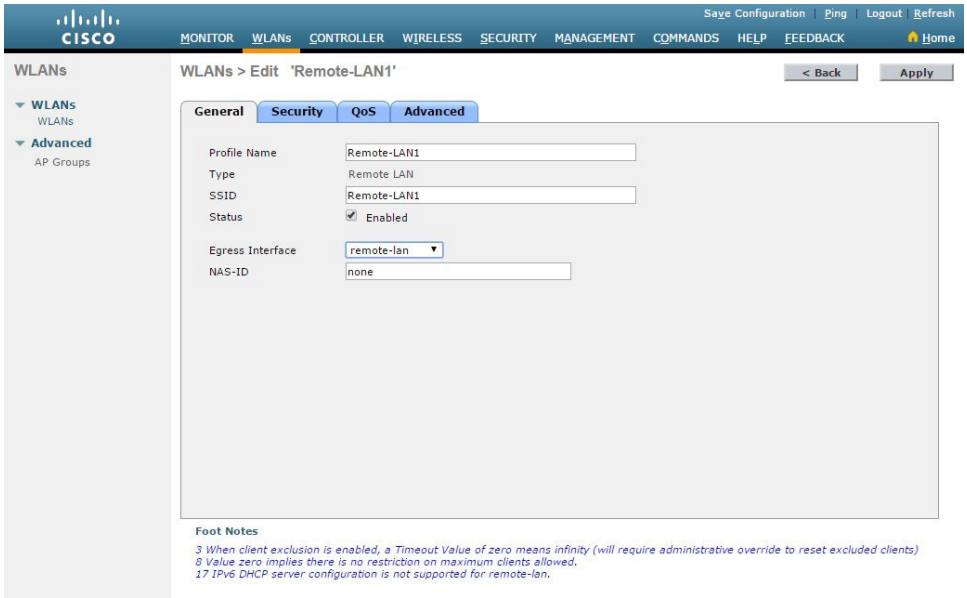
Step 3 In the **Type** list, choose **Remote LAN**.

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



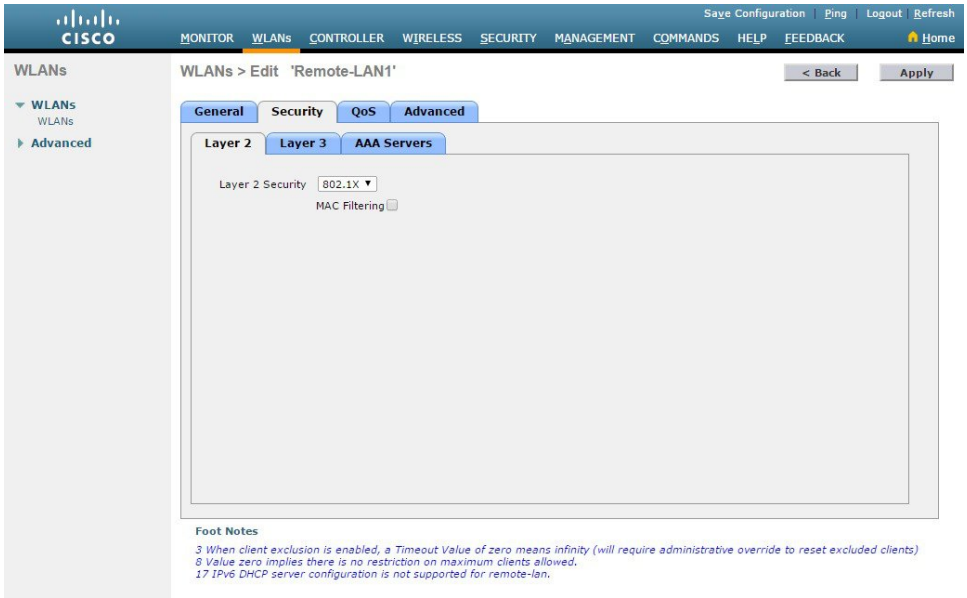
Step 5 On the **General** tab, to the right of **Status**, select **Enabled**.

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

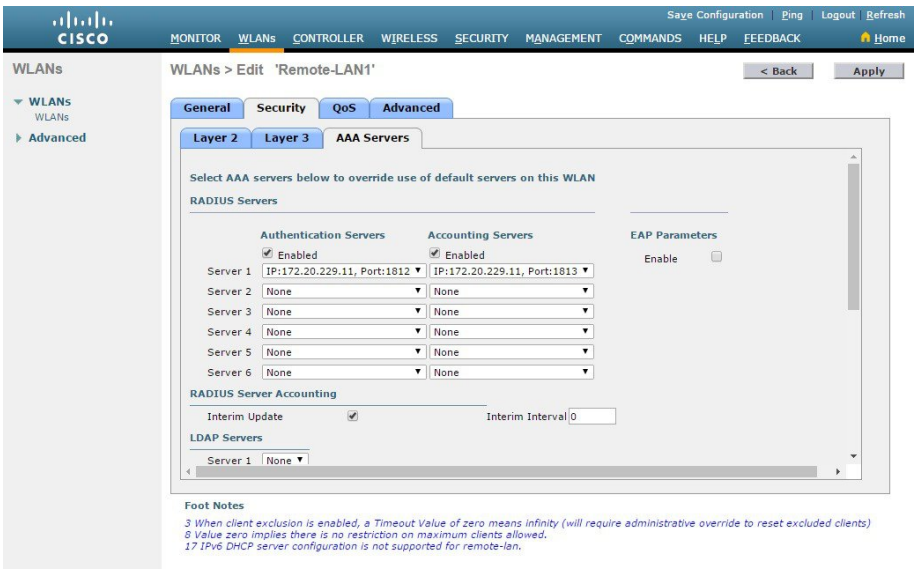


Step 7 Click the **Security** tab.

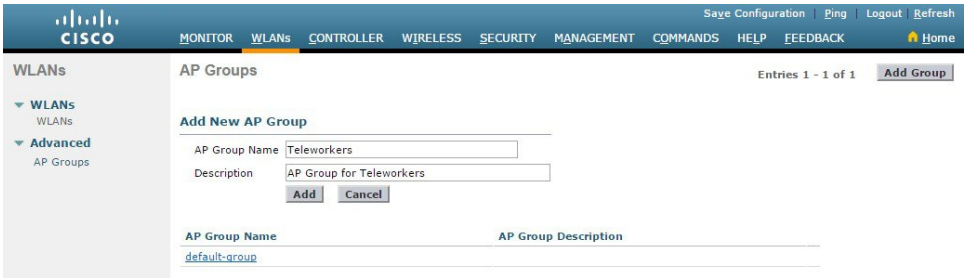
Step 8 On the Layer 2 tab, clear **MAC Filtering** and select **802.1x**.



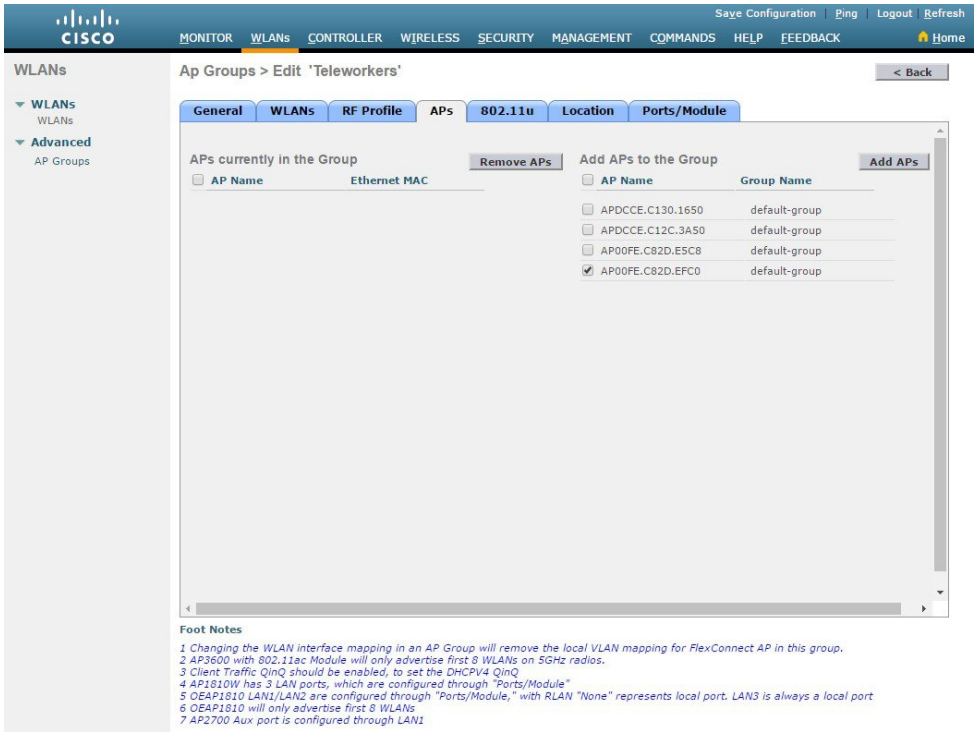
Step 9 On the **AAA Servers** tab, select RADIUS servers and the click **Apply**.



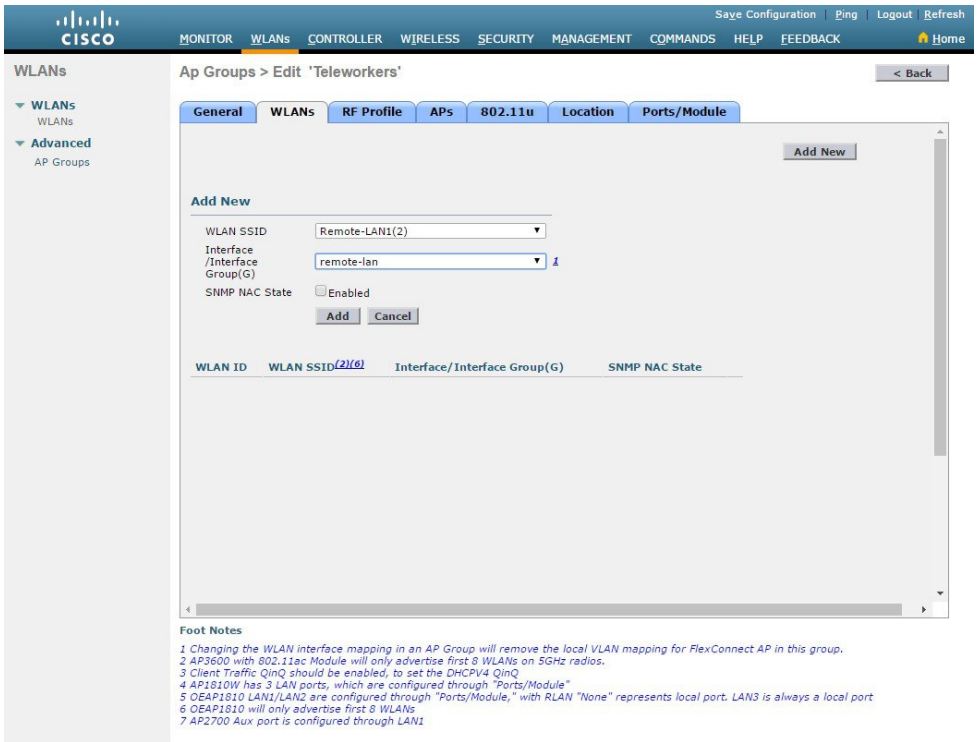
Step 10 Create an AP Group for the Teleworkers.



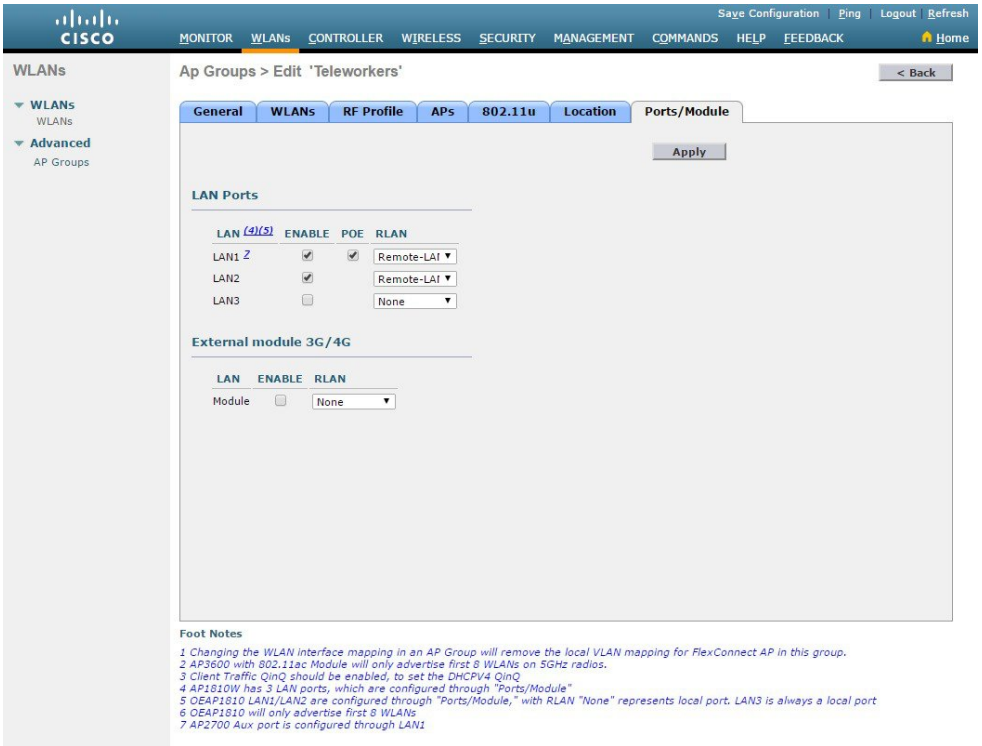
Step 11 Add the Cisco Aironet 1815T(Teleworker) Access Point to the AP Group.



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



Step 13 Assign RLANs to Wired LAN ports. One can Enable/Disable Wired LAN ports along with PoE onPSE LAN1 port .



CHAPTER 7

Configuring AP Authentication

Access point authentication ensures only authorized access points can connect to the controller.

If you want to control which access points can connect to the corporate Wireless LAN Controller, follow this process.

If you want to allow any access point to connect to the Wireless LAN Controller, skip to the next process.

- Configuring AP Authentication in WLC, page 35

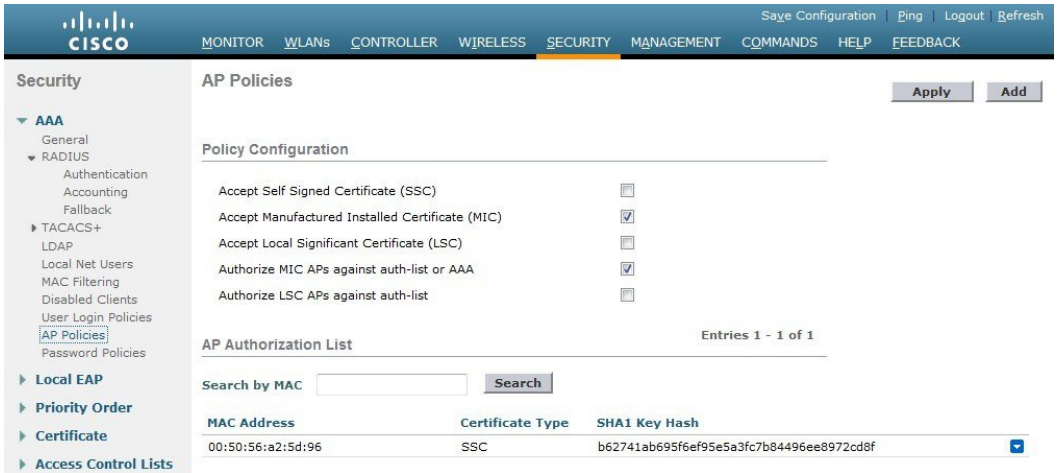
Configuring AP Authentication in WLC

To configure the AP authetication in WLC, perform the following steps:

Procedure

Step 1 Navigate to **Security** > **AAA** > **AP Policies**.

Step 2 Under **Policy Configuration**, select Authorize MIC APs against auth-listor AAA, and then click **Apply**.



CHAPTER 8

Configuring Cisco Aironet 1815T (Teleworker) Access Point

The Cisco Aironet 1815T(Teleworker) requires minimal configuration by the end user. For environments where zero-touch end user deployments are required, the corporate IT department or network-integration partner should pre–configure the Cisco Aironet 1815T with the address of the corporate Wireless LAN controller, as described in this procedure.

Note LAN 3 is a dedicated local port on Cisco Aironet 1815T. Connect your laptop to this device to access the local Cisco Aironet 1815t configuration.

Procedure

Step 1 Connect the WAN port on the back of the Cisco Aironet 1815T Teleworker Access Point to your home router/gateway. The Cisco Aironet 1815T Teleworker Access Point Point gets an IP address from the home router/ gateway.

Note The Cisco Aironet 1815T (Teleworker) Access Point is not designed to replace the functionality of a home router, and it should not be connected directly to the service provider gateway.

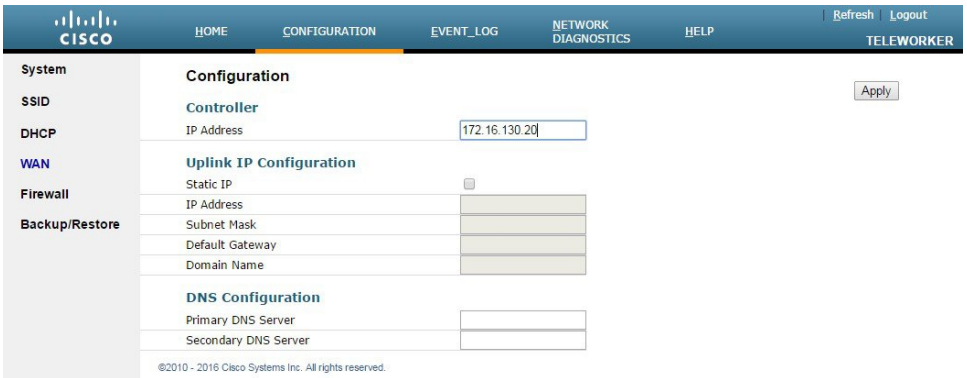
Step 2 After the Cisco Aironet 1815T (Teleworker)Access Point has booted up, connect a computer to the port labeled as LAN3. The computer gets an IP address from the default DHCP address pool of 10.0.0.0/24.

Step 3 Navigate to the Cisco Aironet® 1815T (Teleworker) Access Point by using its default IP address: http://10.0.0.1/

Step 4 Log in to the Administration page by using the default credentials admin/admin. The summary page appears.

Step 5 Navigate to **Configuration** > **WAN**.

Step 6 In the Controller IP Address box, enter the outside IP address of the primary WLC, and then click **Apply**. (Example: 172.16.130.20)



The Cisco Aironet® 1815T (Teleworker) Access Point connects to the controller and downloads the current software image. Allow 15–20 minutes for the device to download and reboot with the new code and configuration.

Note While the access point attempts to make a connection to the WLC, LED in front of the cradle flashes red, amber, and green. Once connected, the status LED flashed yellow until the AireOS download is complete. When the download is complete, the access point restarts. After the access point connects to the controller again, the status LED is displayed as solid green.

CHAPTER 9

Configuring Personal SSID on Cisco Aironet 1815 Teleworker Access Point

The Cisco Aironet 1815T (Teleworker) Access Point also supports Personal SSID. This enables local home client to use the same Cisco Aironet 1815 Teleworker Access Point to connect for local networking and internet connectivity. Please note that local client traffic is not tunneled back to the corporate Wireless LAN Controller.

To configure Personal SSID on Cisco Aironet 1815T (Teleworker) Access Point, perform the following steps:

Procedure

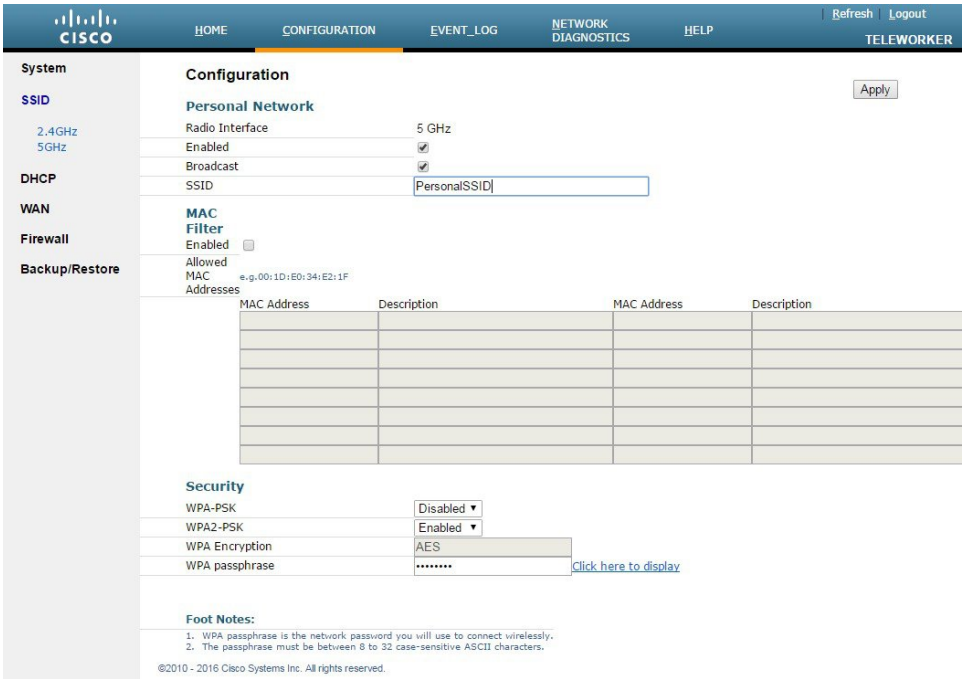
Step 1 Connect the WAN port on the back of the Cisco Aironet 1815T (Teleworker) Access Point to your home router or gateway. The Cisco Aironet 1815 Teleworker Access Point gets an IP address from the home router or gateway.

Step 2 After the Cisco Aironet 1815T (Teleworker) Access Point has started, connect a computer to the port labeled as LAN3 shown as 1 in Figure 2. The computer gets an IP address from the defaultDHCP address pool of 10.0.0.0/24.

Step 3 Navigate to the Cisco OfficeExtend Access Point by using its default IP address: http://10.0.0.1/

Step 4 Log in to the Administration page by using the default credentials admin/admin.

Step 5 Navigate to **Configuration** > **SSID** and configure Personal SSID for 2.4GHz or 5GHz.



Step 6 Enable the Radio and enter the SSID. For SSID broadcast, enable the Broadcast checkbox

Step 7 For security, select **WPA-PSK** or **WPA2-PSK** and enter Paraphrase for corresponding security type.

Step 8 Click **Apply** for settings to take effect.