



## **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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

#### Introduction 1

Technology Use Case 1

Use Case: Teleworker with Wireless Devices 1

---

### CHAPTER 2

#### Design Overview 3

Design Overview 3

Deployment Components 3

Cisco Wireless LAN Controllers 3

Cisco OfficeExtend Access Points 4

Corporate Firewall 4

Design Models 4

Cisco Aironet 1815T(Teleworker) Workflow 5

---

### CHAPTER 3

#### Understanding ports on Cisco Aironet 1815t 7

---

### CHAPTER 4

#### Software Features on Cisco Aironet AIR-AP1815T 9

---

### CHAPTER 5

#### Configuring WLC 11

Configure the WLC for NAT 11

Configuring the Time Zone 12

Configuring SNMP 13

Configuring Wireless User Authentication 17

---

### CHAPTER 6

#### Configuring Voice or Data WLAN Connectivity 19

Creating Wireless LAN Data Interface 19

Creating the Wireless LAN Voice Interface 21

Creating the Remote LAN Interface 22

Configuring the Data Wireless LAN 24

Configure Voice Wireless LAN 26

Configure the Remote LAN 29

---

**CHAPTER 7**

**Configuring AP Authentication 35**

Configuring AP Authentication in WLC 35

---

**CHAPTER 8**

**Configuring Cisco Aironet 1815T (Teleworker) Access Point 37**

---

**CHAPTER 9**

**Configuring Personal SSID on Cisco Aironet 1815 Teleworker Access Point 39**



# Introduction

---

- [Technology Use Case](#) , page 1

## 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 implement devices 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 mobility between 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





## Design Overview

---

- [Design Overview](#) , page 3
- [Design Models](#) , page 4
- [Cisco Aironet 1815T\(Teleworker\) Workflow](#) , page 5

## 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.

---

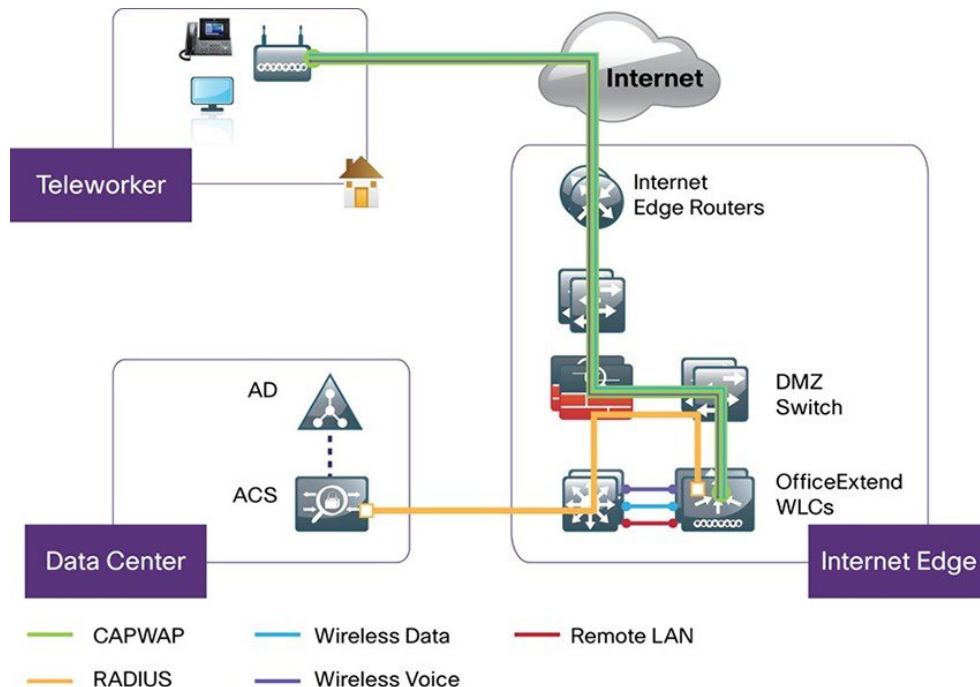
# Design Models

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





## Understanding ports on Cisco Aironet 1815t

### Interfaces

The Cisco AIR-AP1815T has the following interfaces:

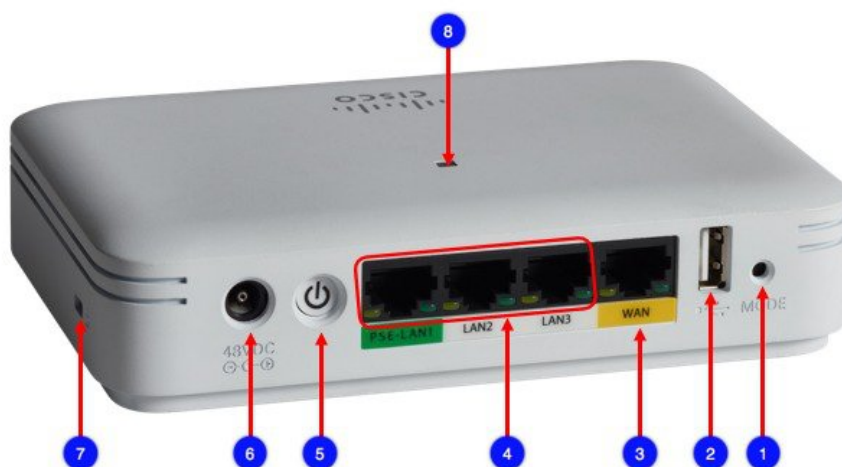
- One 10/100/1000 BASE-T (Ethernet) WAN Interface
- Three 10/100/1000 BASE-T (Ethernet) LAN Interfaces
  - Auto-MDIX (automatically support either straight through or crossover cables)
  - 802.3af PSE power on one LAN 1 Ethernet Interface
- Local Power DC Jack
- Recovery push button (enables partial 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.





## 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.





## Configuring WLC

---

- [Configure the WLC for NAT, page 11](#)
- [Configuring the Time Zone, page 12](#)
- [Configuring SNMP, page 13](#)
- [Configuring Wireless User Authentication, page 17](#)

### 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.

The screenshot shows the Cisco WLC configuration page for the 'management' interface. The page is titled 'Interfaces > Edit' and includes a navigation menu on the left with options like General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main configuration area is divided into several sections:

- General Information:** Interface Name: management, MAC Address: d0:d0:fd:1f:59:e0
- Configuration:** Quarantine: , Quarantine Vlan Id: 0
- NAT Address:** Enable NAT Address: , NAT IP Address: 172.16.130.20
- Interface Address:** VLAN Identifier: 0, IP Address: 192.168.19.20, Netmask: 255.255.255.0, Gateway: 192.168.19.1
- Physical Information:** Port Number: 1, Backup Port: 0, Active Port: 1, Enable Dynamic AP Management:
- DHCP Information:** Primary DHCP Server: 10.4.48.10, Secondary DHCP Server: 0.0.0.0
- Access Control List:** ACL Name: 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."

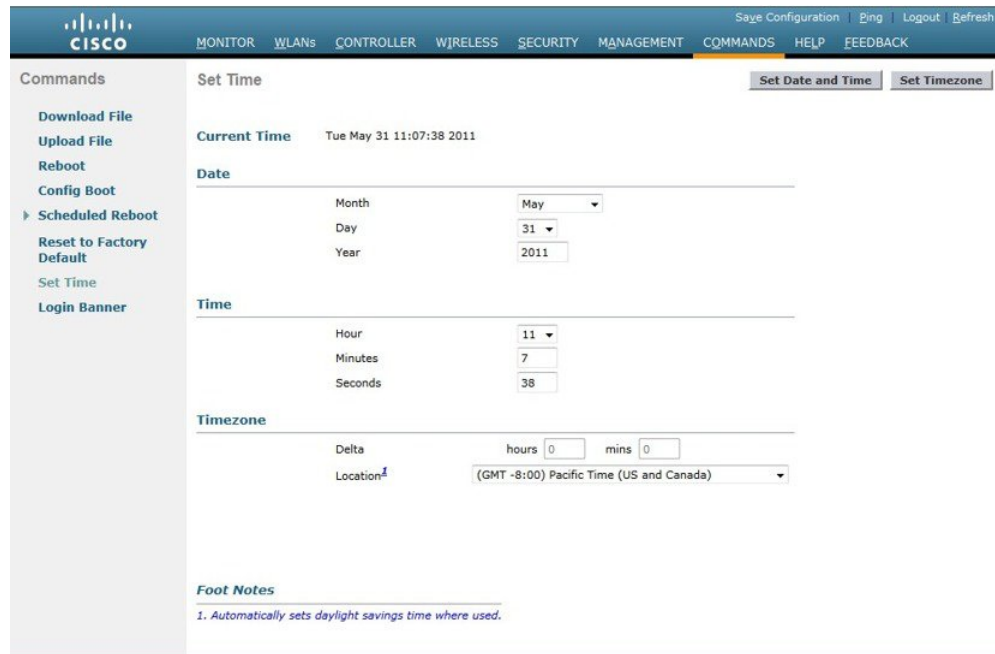
## Configuring the Time Zone

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 location of the WLC.
- Step 3** Click Set Timezone.





Commands

Download File  
Upload File  
Reboot  
Config Boot  
Scheduled Reboot  
Reset to Factory Default  
Set Time  
Login Banner

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Save Configuration | Ping | Logout | Refresh

Set Time Set Date and Time Set Timezone

Current Time Tue May 31 11:07:38 2011

Date

Month

Day

Year

Time

Hour

Minutes

Seconds

Timezone

Delta hours  mins

Location

Foot Notes

1. Automatically sets daylight savings time where used.

## 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**.

Management

SNMP v1 / v2c Community > New

Community Name:

IP Address:

IP Mask:

Access Mode:

Status:

Summary

- SNMP
  - General
  - SNMP V3 Users
  - Communities
  - Trap Receivers
  - Trap Controls
  - Trap Logs
- HTTP-HTTPS
- Telnet-SSH
- Serial Port
- Local Management Users
- User Sessions
- Logs
- Mgmt Via Wireless
- Software Activation
- Tech Support

Save Configuration | Ping | Logout | Refresh

< Back | 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**.

Management

SNMP v1 / v2c Community > New

Community Name:

IP Address:

IP Mask:

Access Mode:

Status:

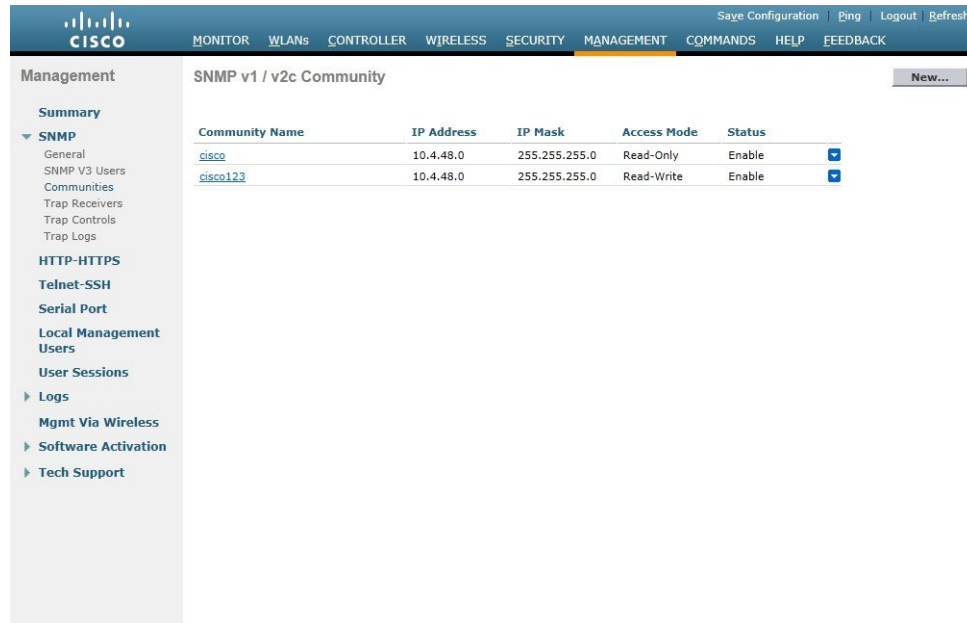
Summary

- SNMP
  - General
  - SNMP V3 Users
  - Communities
  - Trap Receivers
  - Trap Controls
  - Trap Logs
- HTTP-HTTPS
- Telnet-SSH
- Serial Port
- Local Management Users
- User Sessions
- Logs
- Mgmt Via Wireless
- Software Activation
- Tech Support

Save Configuration | Ping | Logout | Refresh

< Back | 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.



Management

SNMP v1 / v2c Community New...

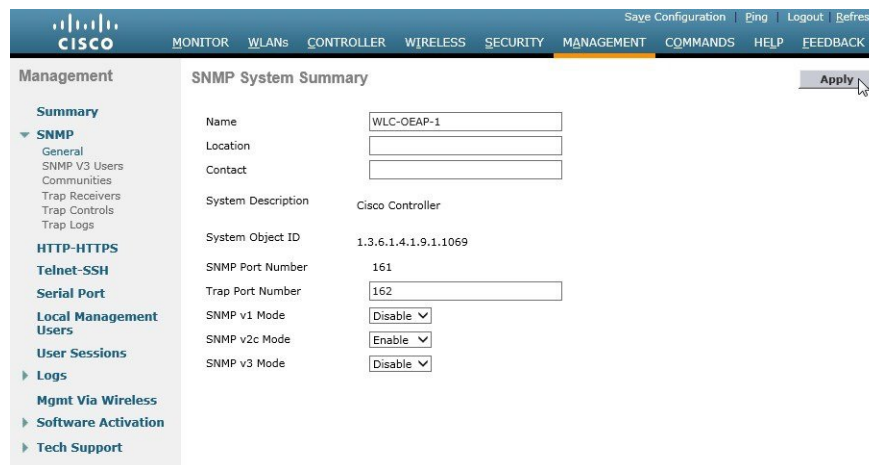
Community Name	IP Address	IP Mask	Access Mode	Status
<a href="#">cisco</a>	10.4.48.0	255.255.255.0	Read-Only	Enable <span>▼</span>
<a href="#">cisco123</a>	10.4.48.0	255.255.255.0	Read-Write	Enable <span>▼</span>

Summary

- SNMP
  - General
  - SNMP V3 Users
  - Communities
  - Trap Receivers
  - Trap Controls
  - Trap Logs
- HTTP-HTTPS
- Telnet-SSH
- Serial Port
- Local Management Users
- User Sessions
- Logs
- Mgmt Via Wireless
- Software Activation
- Tech Support

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

**Figure 2:**



Management

SNMP System Summary Apply

Name: WLC-OEAP-1

Location:

Contact:

System Description: Cisco Controller

System Object ID: 1.3.6.1.4.1.9.1.1069

SNMP Port Number: 161

Trap Port Number: 162

SNMP v1 Mode: Disable ▼

SNMP v2c Mode: Enable ▼

SNMP v3 Mode: Disable ▼

Summary

- SNMP
  - General
  - SNMP V3 Users
  - Communities
  - Trap Receivers
  - Trap Controls
  - Trap Logs
- HTTP-HTTPS
- Telnet-SSH
- Serial Port
- Local Management Users
- User Sessions
- Logs
- Mgmt Via Wireless
- Software Activation
- Tech Support

- 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**.

The screenshot shows the Cisco WLC Management interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'MANAGEMENT' tab is active. On the left, the 'Management' sidebar is expanded to 'SNMP'. The main content area is titled 'SNMP V3 Users' and contains a table with the following data:

User Name	Access Level	Auth Protocol	Privacy Protocol
default	Readwrite	HMAC-SHA	AES

A 'Remove' button is visible next to the 'default' user entry.

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

The screenshot shows the same Cisco WLC Management interface as above, but with a confirmation dialog box open. The dialog box is titled 'Message from webpage' and contains the text: 'Are you sure you want to delete?'. There are 'OK' and 'Cancel' buttons at the bottom of the dialog box.

**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**.

The screenshot shows the Cisco WLC configuration interface for RADIUS Authentication Servers. The page title is "RADIUS Authentication Servers > New". The configuration fields are as follows:

Field	Value
Server Index (Priority)	1
Server IP Address	10.4.48.15
Shared Secret Format	ASCII
Shared Secret	SecretKey
Confirm Shared Secret	SecretKey
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

- 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 | Bing | 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)

Server IP Address

Shared Secret Format

Shared Secret

Confirm Shared Secret

Port Number

Server Status

Server Timeout  seconds

Network User  Enable

IPSec  Enable



## 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 19](#)
- [Creating the Wireless LAN Voice Interface, page 21](#)
- [Creating the Remote LAN Interface, page 22](#)
- [Configuring the Data Wireless LAN, page 24](#)
- [Configure Voice Wireless LAN, page 26](#)
- [Configure the Remote LAN, page 29](#)

### 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 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'CONTROLLER' tab is active. 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 is the same as in the previous screenshot. The 'CONTROLLER' tab is active. The main content area is titled 'Interfaces > Edit'. It is divided into several sections: 'General Information' (Interface Name: Wireless-Data, MAC Address: do:do:fd:1f:59:e0), 'Configuration' (Guest Lan, Quarantine, and Quarantine Vlan Id checkboxes and a dropdown), 'Physical Information' (Port Number: 2, Backup Port: 0, Active Port: 0, Enable Dynamic AP Management checkbox), 'Interface Address' (VLAN Identifier: 244, IP Address: 10.4.144.5, Netmask: 255.255.252.0, Gateway: 10.4.144.1), 'DHCP Information' (Primary DHCP Server: 10.4.48.10, Secondary DHCP Server: empty), and 'Access Control List' (ACL Name: 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.' At the top right of the main area are '< Back' and 'Apply' buttons.



# 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 menu shows 'Controller' as the active section, 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."

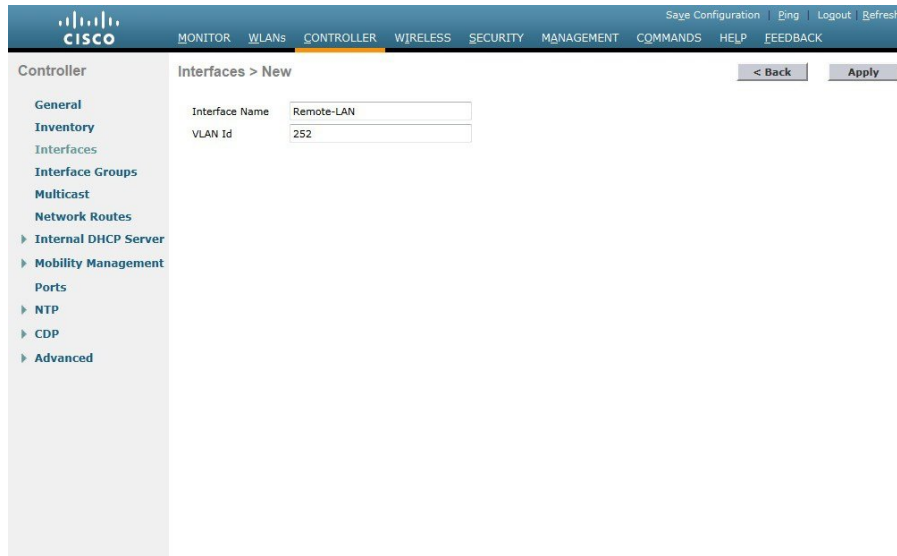
## Creating the Remote LAN Interface

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

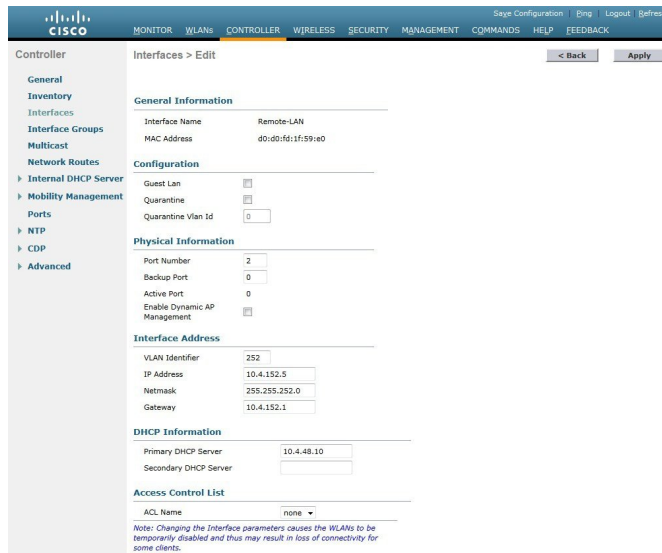
To create remote LAN interface, perform the following steps:

### 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

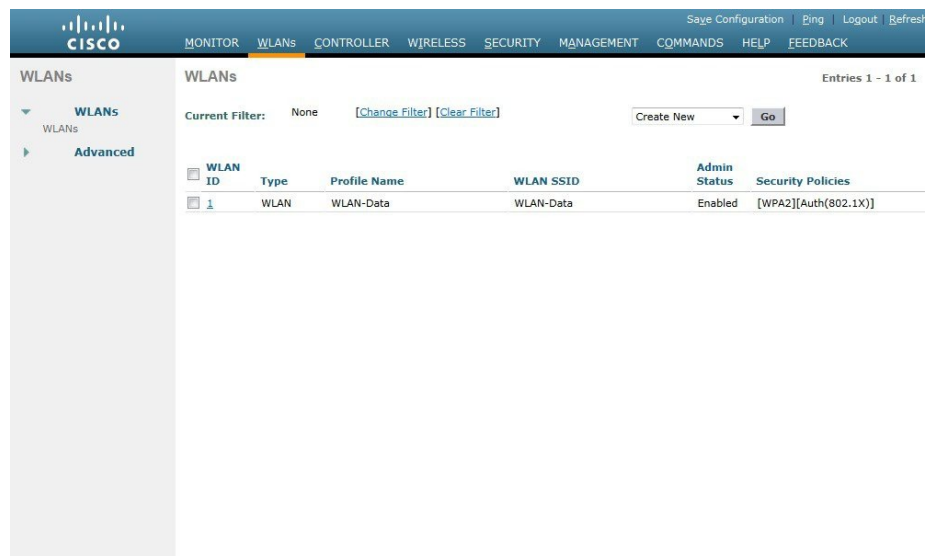
Wireless data traffic is different from voice traffic in that it can more efficiently handle delay and jitter as well as greater packet loss. For the data wireless LAN, keep the default QoS settings and segment the data traffic onto the data wired VLAN.

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

## Procedure

**Step 1** Navigate to **WLANs**.

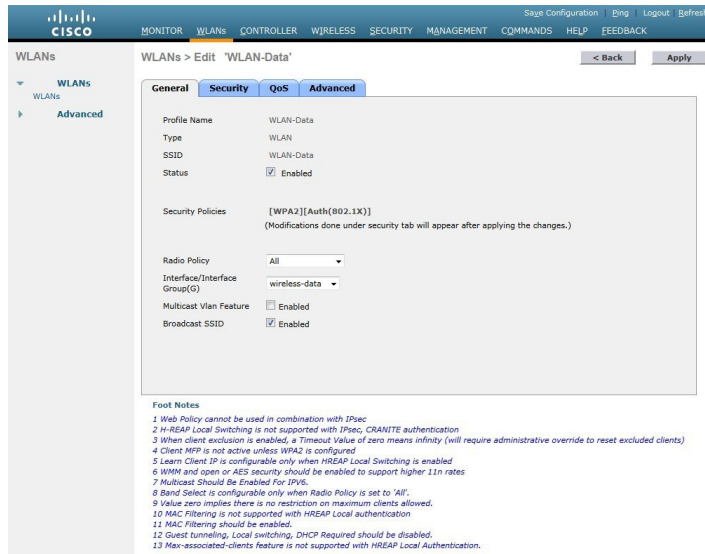
**Step 2** Click the **WLAN ID** of the SSID created during platform setup.



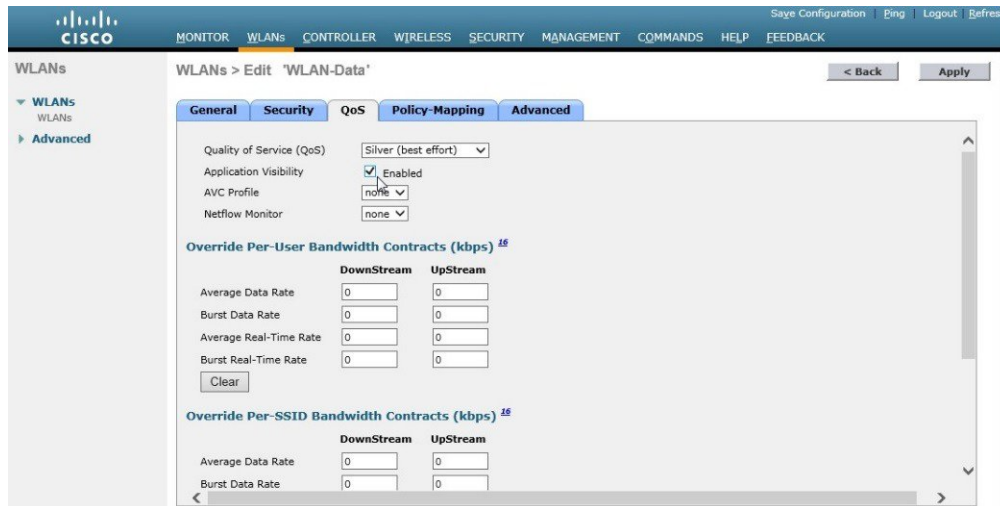
The screenshot shows the Cisco configuration interface for WLANs. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WLANs' section is active, showing a table with one entry. The table has columns for 'WLAN 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**.

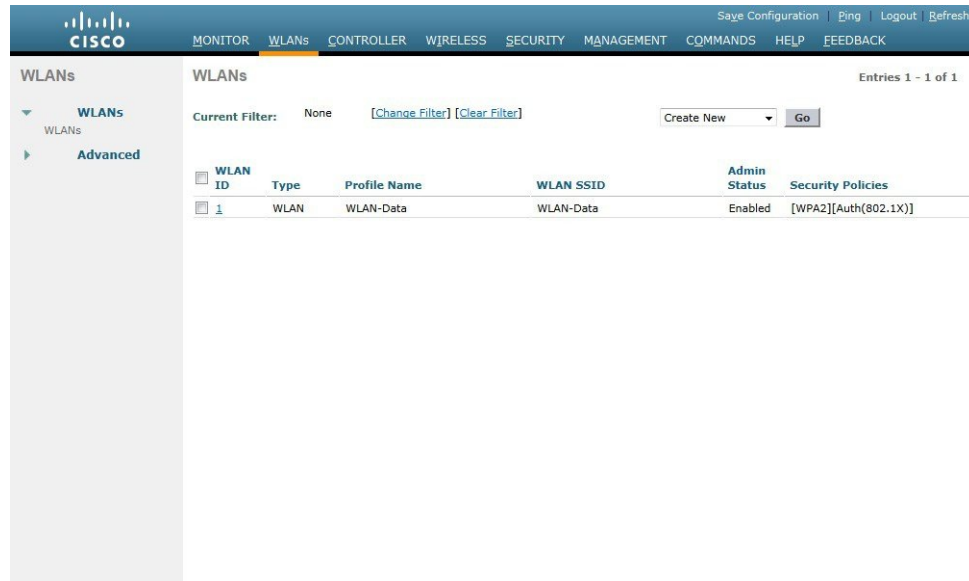
## Configure Voice Wireless LAN

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:

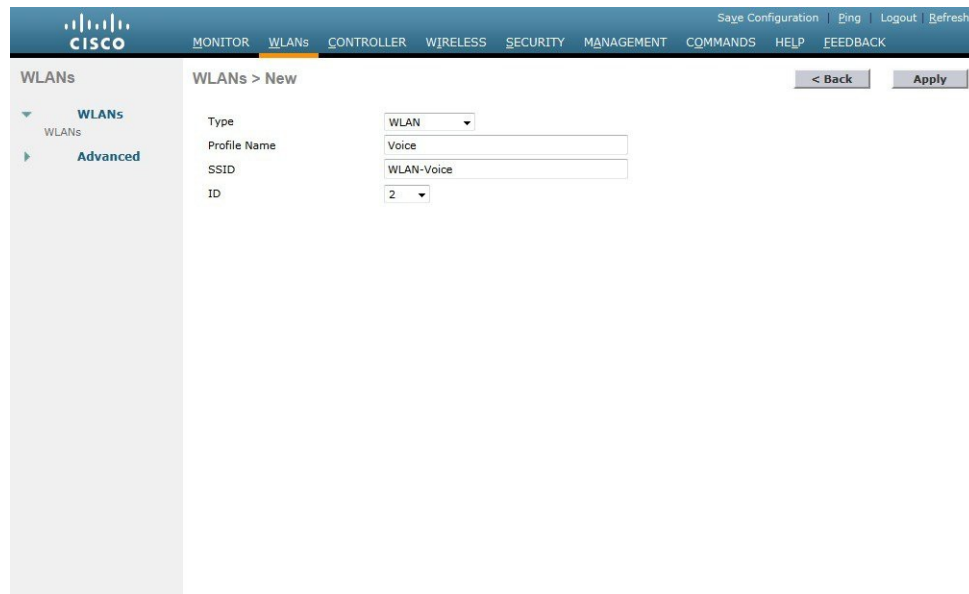
### Procedure

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



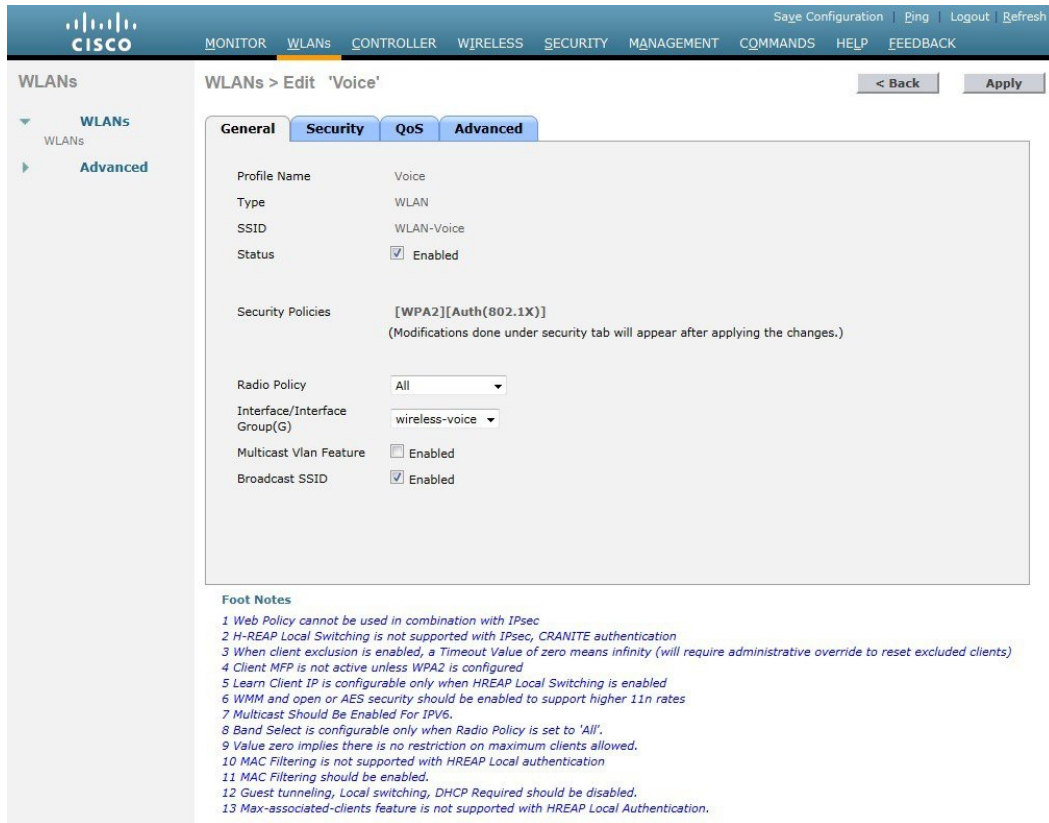
**Step 3** Enter the **Profile Name**. (Example: Voice)

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

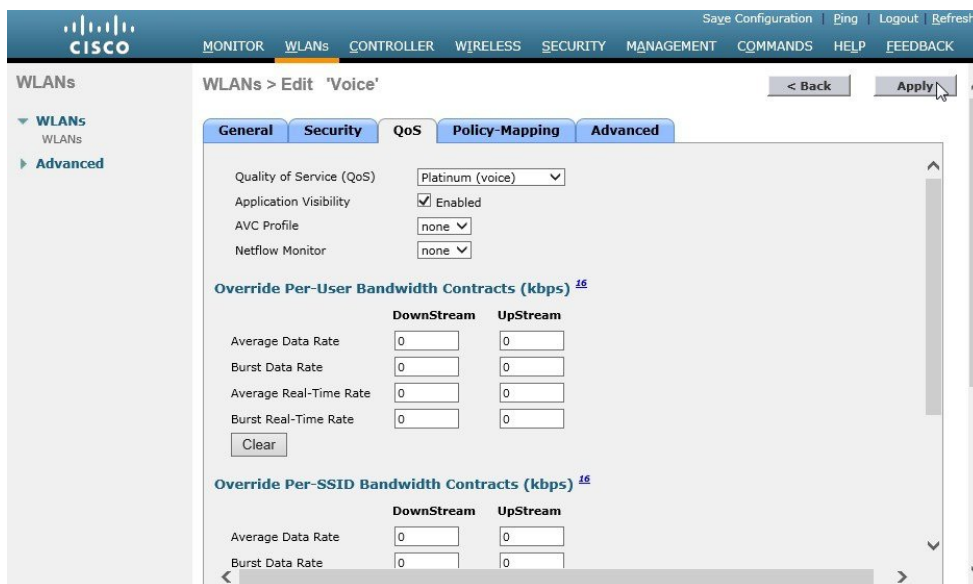


**Step 5** On the **General** tab, to the right of Status, select **Enabled**.

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



**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**.

The screenshot shows the Cisco Aironet 1815T WebUI configuration page for a WLAN named 'Voice'. The 'Advanced' tab is selected, and the following settings are visible:

- 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:** 0
- Static IP:**  Enabled
- DHCP:**
  - DHCP Server:**  Override
  - DHCP Addr. Assignment:**  Required
- OEAP:**
  - Split Tunnel (Printers):**  Enabled
- Management Frame Protection (MFP):**
  - MFP Client Protection:** Optional
- DTIM Period (in beacon intervals):**
  - 802.11a/n (1 - 255): 1
  - 802.11b/g/n (1 - 255): 1
- NAC:**
  - NAC State:** None

## 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 'General' 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' with the 'Security' tab selected. The 'Layer 2' sub-tab is active, and the following settings 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, and the 'RADIUS Servers' section is expanded. The configuration includes:

- Authentication Servers:** Server 1 is enabled with IP:172.20.229.11, Port:1812. Servers 2-6 are set to 'None'.
- Accounting Servers:** Server 1 is enabled with IP:172.20.229.11, Port:1813. Servers 2-6 are set to 'None'.
- EAP Parameters:** The 'Enable' checkbox is unchecked.
- RADIUS Server Accounting:** 'Interim Update' is checked, and 'Interim Interval' is set to 0.
- LDAP Servers:** Server 1 is set to '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.

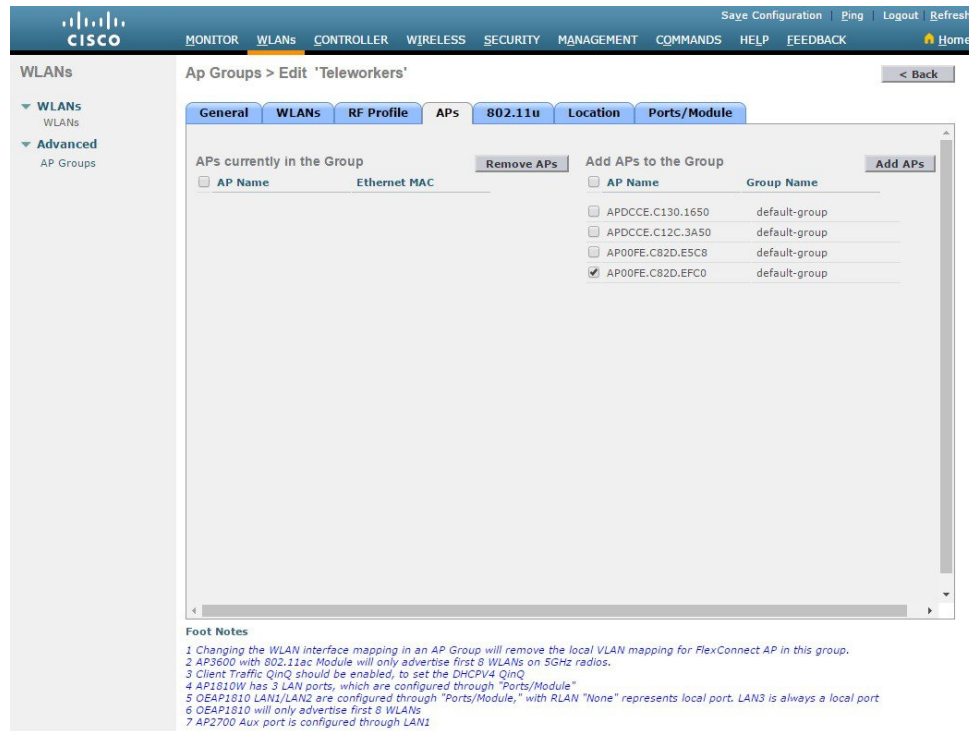
The screenshot shows the Cisco AP Groups configuration interface. The 'Add New AP Group' form is displayed with the following details:

- AP Group Name:** Teleworkers
- Description:** AP Group for Teleworkers

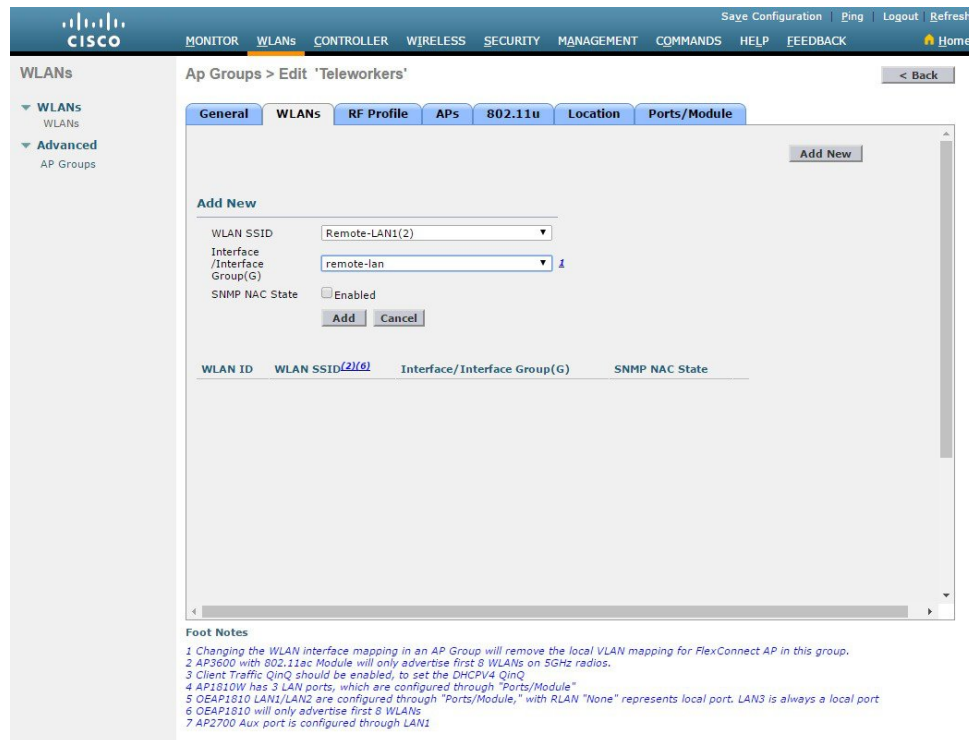
Below the form, a table lists the existing AP Group:

AP Group Name	AP Group Description
<a href="#">default-group</a>	

**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:

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



## 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 authentication 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-list or AAA**, and then click **Apply**.

The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'SECURITY' tab is active. On the left, the 'Security' menu is expanded to 'AAA', and 'AP Policies' is selected. The main content area shows the 'AP Policies' configuration page. The 'Policy Configuration' section has the following settings:

Policy Configuration	Value
Accept Self Signed Certificate (SSC)	<input type="checkbox"/>
Accept Manufactured Installed Certificate (MIC)	<input checked="" type="checkbox"/>
Accept Local Significant Certificate (LSC)	<input type="checkbox"/>
Authorize MIC APs against auth-list or AAA	<input checked="" type="checkbox"/>
Authorize LSC APs against auth-list	<input type="checkbox"/>

Below the policy configuration is the 'AP Authorization List' section, which shows 'Entries 1 - 1 of 1'. It includes a search bar and a table with the following entry:

MAC Address	Certificate Type	SHA1 Key Hash
00:50:56:a2:5d:96	SSC	b62741ab695f6ef95e5a3fc7b84496ee8972cd8f







# 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 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.

The screenshot shows the Cisco Aironet 1815T (Teleworker) configuration interface. The top navigation bar includes HOME, CONFIGURATION, EVENT\_LOG, NETWORK DIAGNOSTICS, and HELP. The left sidebar shows AP Info, SSID, and Client. The main content area is titled "Home: Summary" and contains the following sections:

**General Information**

AP Name	rtayal
AP IP Address	10.0.0.113
AP Mode	FlexConnect
AP MAC Address	00:fe:c8:2d:eb:80
AP Uptime	0 days, 0 hours, 9 minutes, 50 seconds
AP Software Version	8.3.90.5
WLC Info	[Cisco_7d:88:00] .35.131]
CAPWAP Status	Run
WAN Gateway Status	Good

**AP Statistics**

Radio	Admin Status	Chan/BW	Tx Power	Pkts In/Out
2.4 GHz	Enabled	1/20MHz	20dBm	63884/63887
5 GHz	Enabled	36/80MHz	20dBm	3803/3905

**LAN Port**

Port No	Admin Status	Port Type	Link Status	Pkts In/Out
1	Enabled	Corporate	Down	0/0
2	Enabled	Local	Down	0/0
3	Enabled	Local	Down	0/0

©2010 - 2016 Cisco Systems Inc. All rights reserved.

**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 screenshot shows the Cisco Aironet 1815T (Teleworker) configuration interface. The top navigation bar includes HOME, CONFIGURATION, EVENT\_LOG, NETWORK DIAGNOSTICS, and HELP. The left sidebar shows System, SSID, DHCP, WAN, Firewall, and Backup/Restore. The main content area is titled "Configuration" and contains the following sections:

**Controller**

IP Address:

**Uplink IP Configuration**

Static IP:

IP Address:

Subnet Mask:

Default Gateway:

Domain Name:

**DNS Configuration**

Primary DNS Server:

Secondary DNS Server:

©2010 - 2016 Cisco Systems Inc. All rights reserved.

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.



# 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.

The screenshot shows the configuration page for a Cisco Aironet 1815T Teleworker Access Point. The page is titled "Configuration" and has a navigation menu with "HOME", "CONFIGURATION", "EVENT\_LOG", "NETWORK DIAGNOSTICS", and "HELP". There are also "Refresh" and "Logout" buttons in the top right corner. The left sidebar contains a menu with "System", "SSID", "DHCP", "WAN", "Firewall", and "Backup/Restore". The main content area is divided into sections: "Personal Network" and "Security".

**Personal Network**

- Radio Interface: 5 GHz
- Enabled:
- Broadcast:
- SSID: PersonalSSID

**MAC Filter**

- Enabled:
- Allowed MAC Addresses: e.g. 00:10:10:34:E2:1F

MAC Address	Description	MAC Address	Description

**Security**

- WPA-PSK: Disabled
- WPA2-PSK: Enabled
- WPA Encryption: AES
- WPA passphrase: ..... [Click here to display](#)

**Foot Notes:**

1. WPA passphrase is the network password you will use to connect wirelessly.
2. The passphrase must be between 8 to 32 case-sensitive ASCII characters.

©2010 - 2016 Cisco Systems Inc. All rights reserved.

- 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.