JUNIPER NETWORKS

Junos® OS

WLAN Configuration and Administration Guide for SRX210, SRX240, and SRX650 Services Gateways

Release
12.1

Published: 2012-03-06

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos OS WLAN Configuration and Administration Guide
Release 12.1

Revision History
March 2012—R1 Junos OS 12.1

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

This preface provides the following guidelines for using the *Junos OS WLAN Configuration and Administration Guide*:

SRX Series Documentation and Release Notes

For a list of related SRX Series documentation, see http://www.juniper.net/techpubs/hardware/srx-series-main.html .

If the information in the latest release notes differs from the information in the documentation, follow the *Junos OS Release Notes*.

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at http://www.juniper.net/books .

Objectives

This guide provides an overview of the wireless LAN features of the Junos OS and describes how to configure these features on the SRX Series Services Gateway.

Audience

This manual is designed for anyone who installs, sets up, configures, monitors, or administers an SRX Series Services Gateway running Junos OS. The manual is intended for the following audiences:

- Customers with technical knowledge of and experience with networks and network security, the Internet, and Internet routing protocols
- Network administrators who install, configure, and manage Internet routers

Supported Routing Platforms

This manual describes features supported on SRX210, SRX240, and SRX650 Services Gateways running Junos OS.

Documentation Conventions

Table 1 on page viii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page viii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Italic text like this	• Introduces important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; interface names; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub** <**default-metric** *metric*>**;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** (***string1*** **|** ***string2*** **|** ***string3***)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/ .
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at http://www.juniper.net/support/requesting-support.html

PART 1

Overview

CHAPTER 1

Introduction

WLAN Overview

The wireless local area network (WLAN) system supported in this Junos OS Release consists of an SRX Series Services Gateway and one or more AX411 Series WLAN Access Points that are centrally managed by the SRX Series device. The access points are connected to the ports on the SRX Series device and can relay data between the wired and wireless network.

A WLAN allows wireless clients to communicate with each other and access the wired network. Wireless clients can be laptop or desktop computers, personal digital assistants (PDAs), or any other device equipped with a Wi-Fi adapter and supporting drivers. When a wireless client starts up, it searches for beacon frames that originate from access points to determine the service the access points provide. Upon completing predefined authentication with an access point, the client is connected or associated with the access point and can access the network. Depending upon the type of authentication configured, the access point might need to communicate with a RADIUS server to validate or authenticate the client.

The AX411 Access Point can only be managed from an SRX210, SRX240, or SRX650 Services Gateway with the appropriate access point licenses installed. Up to 32 access points can be connected to an SRX Series Services Gateway. Multiple access points can be connected to a single port on the SRX Series device through an external switch or hub.

NOTE: The SRX Series device can manage only the AX411 Access Point and not any other vendors' access points.

NOTE: On all branch SRX devices, managing AX411 WLAN Access Points through a Layer 3 Aggregated Ethernet (ae) interface is not supported.

The Juniper Networks WLAN provides security policies, AAA, and other security features for wireless access. Configuration and management of the AX411 Access Point is through either the Junos OS CLI or J-Web interface on the SRX Series Services Gateway. You can also use the Network and Security Manager (NSM) to configure and manage the access point through the SRX Series device. Access point logs are maintained on the SRX Series Services Gateway and upgrades of the access point software are performed from the SRX Series device.

Related Documentation

- AX411 Access Point Feature Overview on page 4
- Understanding Wireless Client Requirements on page 5
- Understanding Access Point Licensing on page 6
- *Network and Security Manager: Configuring J Series Services Routers and SRX Series Services Gateways Guide*

AX411 Access Point Feature Overview

Use the Junos OS CLI or J-Web interface on the SRX Series Services Gateway to configure the following features of the AX411 Access Point:

- IEEE 802.11 a/b/g/n wireless client stations—The AX411 Access Point supports dual radios, each of which can be configured independently. A radio can operate in any one of the radio modes specified by the IEEE wireless networking standards such as 802.11a, 802.11b/g, or 802.11n. The radio mode determines what type of wireless clients can connect to the access point. The radio on the access point can be configured to support just one type of client or a mixed mode, where different types of clients can connect to the radio.
- Wireless security for client authentication and encryption, including:
  - Wi-Fi Protected Access (WPA) Personal—A Wi-Fi Alliance standard that includes Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP) and Temporal Key Integrity Protocol (TKIP) with preshared key authentication. Both WPA and the newer WPA2 standards are supported.
  - WPA Enterprise—A Wi-Fi Aliance standard that includes AES-CCMP and TKIP with RADIUS server authentication.
  - 802.1x—An IEEE standard for dynamic key generation using a RADIUS server that supports Extensible Authentication Protocol (EAP). To work with Windows clients, the authentication server must support Protected EAP (PEAP) and version 2 of the Microsoft Challenge Handshake Authentication Protocol (MS-CHAPv2). This is also known as *dynamic WEP*.
  - Static Wired Equivalent Privacy (WEP) protocol—A data encryption protocol that uses shared keys.
  - MAC authentication—Wireless clients are allowed or denied network access based on their MAC address. The list of MAC addresses that are allowed or denied can be configured on a RADIUS server or on the SRX Series device.

The access point also supports no security, which allows any client to connect to the access point. Data transferred between the client and the access point is not encrypted.

- IEEE 802.1x supplicant mode—The access point can operate as an 802.1x supplicant to authenticate itself with the network using EAP-MD5 challenge authentication.
- Multiple virtual access points on a single access point—A virtual access point is a logical simulation of a physical access point and is identified by a configured service set identifier (SSID) and a unique basic service set identifier (BSSID). You can configure up to 16 virtual access points per radio.
- DHCP client—At its initial startup, the access point broadcasts requests for an IP address to an available DHCP server. If there is no DHCP server on the network, a static IP address and default gateway can be configured for the access point.
- Quality-of-service (QoS) configuration based on the Wi-Fi Alliance Wi-Fi Multimedia (WMM) specification—This feature allows you to tune throughput and performance for different types of wireless traffic such as voice over IP (VoIP), audio, video, streaming media, and other IP data.

Related Documentation

- *AX411 Access Point Hardware Guide*
- AX411 Access Point Configuration Overview on page 13

Understanding Wireless Client Requirements

The AX411 provides wireless access to any client with a properly configured Wi-Fi client adapter for the 802.11 radio mode in which the access point is running. The AX411 Access Point supports multiple client operating systems.

To connect to the AX411 Access Point, wireless clients need the following hardware and software:

- Wi-Fi client adapter—Portable or built-in Wi-Fi adapter that supports one or more of the IEEE 802.11 radio modes in which you plan to run the access point.
- Wireless client software—Client software, such as the Microsoft Windows Supplicant, configured to associate with the AX411 Access Point.
- Client security settings—If the security mode on the AX411 is set to anything other than “no security,” wireless clients need to be configured for the authentication mode used by the access point and provide a valid username and password, certificate, or similar proof of identity.

NOTE: Client users can allow the Windows Wireless Zero Configuration (WZC) service to automatically configure wireless settings on the client.

Related Documentation

- Understanding Client Security on page 42
- *AX411 Access Point Hardware Guide*

Understanding Access Point Licensing

You can configure and manage up to two AX411 Access Points from an SRX Series Services Gateway without installing a license on the SRX Series device. To configure and manage additional AX411 Access Points, you must install one or more licenses on the SRX Series device.

The following licenses are available for the SRX Series Services Gateway:

- 2–access point license—Two additional access points can be configured from the SRX Series Services Gateway.
- 4–access point license—Four additional access points can be configured from the SRX Series Services Gateway.
- 8–access point license—Eight additional access points can be configured from the SRX Series Services Gateway.
- 14–access point license—14 additional access points can be configured from the SRX Series Services Gateway.

Licenses can be added in any increment to increase the number of access points supported on an SRX Series device.

For information about how to purchase software licenses for your device, contact your Juniper Networks sales representative.

Related Documentation

- *Junos OS Initial Configuration Guide for Security Devices*
- Getting Started with the Default Access Point Configuration on page 9

PART 2

Configuration

CHAPTER 2

AX411 Access Point Configuration

Getting Started with the Default Access Point Configuration

This topic describes the basic workflow to enable wireless clients to connect to the WLAN using the default configuration for the AX411 Access Point.

If you have not configured a licensed access point before connecting it to the SRX Series device, the factory-default configuration is applied to the access point. You can later configure the access point; the new configuration is applied as well as the access point name you specified.

NOTE: **The following procedures describe the configuration of the SRX Series Services Gateway to enable operation of the AX411 Access Point with its default configuration. You do not need to configure the access point itself before powering it on; wireless clients using Wireless Zero Configuration (WZC) can automatically connect to the default SSID on the access point.**

To change the default configuration of an access point, you must first specify the MAC address of the access point to be configured. The MAC address links an access point to its configuration.

Before you begin:

- Read "Understanding Wireless Client Requirements" on page 5 and "Understanding Access Point Licensing" on page 6
- Refer to the *AX411 Access Point Getting Started Guide* and the *AX411 Access Point Hardware Guide* for details about hardware components.
- Read the release notes for your release. The release notes contain important release-related information about release-specific features, unsupported features, changed features, fixed issues, and known issues. The information in the release notes is more current than the information in this guide.

To enable wireless clients to connect to the WLAN with the default configuration for the AX411 Access Point:

1. Install the SRX Series Services Gateway, configure network settings, and connect the device to your network. See the installation guide for your SRX Series device.
2. Install access point licenses as needed in the SRX Series Services Gateway (see "Understanding Access Point Licensing" on page 6). You can install multiple licenses to increase the number of access points that can be configured and managed through the SRX Series device. See the *AX411 Access Point Getting Started Guide*.
3. We highly recommend that you connect the AX411 Access Point to a PoE port on the SRX Series device. We also recommend that the port on the SRX Series device be a Gigabit Ethernet port to accommodate the traffic flow from wireless clients.

   To enable the PoE-capable port on the SRX Series device:

   ```
   [edit]
   user@host# set poe interface ge-0/0/0
   ```

   To enable all PoE-capable ports on the SRX Series device:

   ```
   [edit]
   user@host# set poe interface all
   ```

   An external power supply for the access point can be used in conjunction with an SRX Series device that does not support PoE.
4. Configure the port on the SRX Series device to which the access point is connected as either a Layer 2 (see "Understanding Layer 2 Forwarding Operations" on page 18) or Layer 3 interface. The DHCP server on the SRX Series device should be configured to provide IP addresses to the access point and to wireless clients that connect to the WLAN.

   - To configure the port as a Layer 2 interface and configure a DHCP server and address pool on the SRX Series device:

     ```
     [edit]
     user@host# set interfaces vlan unit 0 family inet address 16.1.1.1/24
     user@host# set vlans v100 vlan-id 100
     user@host# set vlans v100 l3-interface vlan.0
     user@host# set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members
       v100
     user@host# set system services dhcp router 16.1.1.1
     user@host# set system services dhcp pool 16.1.1.1/24 address-range high 16.1.1.30
       low 16.1.1.10
     ```

     If the port is a trunk port, configure the native VLAN ID:

     ```
     [edit]
     user@host# set interfaces ge-0/0/0 unit 0 family ethernet-switching port-mode
       trunk native-vlan-id 100
     ```

   - To configure the port as a Layer 3 interface and configure a DHCP server and address pool on the SRX Series device:

     ```
     [edit]
     user@host# set interfaces ge-0/0/0 unit 0 family inet address 16.1.1.1/24
     user@host# set system services dhcp router 16.1.1.1
     ```

```
user@host# set system services dhcp pool 16.1.1.1/24 address-range high 16.1.1.30
    low 16.1.1.10
```

5. Add the interface to a security zone and configure a security policy to allow traffic to and from the zone. The **ge-0/0/0** interface is in the Trust security zone by default; other interfaces on the SRX Series device must be added to a security zone. The default security policy on the SRX Series device permits application traffic to and from the Trust zone. If you connect the access point to the **ge-0/0/0** port on the SRX Services Gateway with the default security policy, no further configuration is required on the SRX Series device.
6. Connect the access point to a PoE port on the SRX Series Services Gateway. The access point powers on and the DHCP client on the access point broadcasts requests for an IP address.

   Upon obtaining an IP address, the access point begins broadcasting the default SSID **juniper-default**.
7. Connect your wireless clients to this default SSID using the following configuration:
   - WPA2 Personal security
   - Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP) encryption
   - Preshared key **juniper-wireless** for authentication

NOTE: Client users can allow Windows Wireless Zero Configuration (WZC) service to automatically configure wireless settings on the client.

Related Documentation

- Factory-Default Configuration on page 11
- AX411 Access Point Configuration Overview on page 13
- *Junos OS Security Configuration Guide*

Factory-Default Configuration

Table 3 on page 11 lists the default configuration of the AX411 Access Point provided by Juniper Networks.

Table 3: AX411 Access Point Factory-Default Configuration

Configurable Setting	Default Value
Access point name	(Automatically generated)
Network Settings	
IP address	Provided by DHCP server on the SRX Series device.
Management VLAN ID	1

Table 3: AX411 Access Point Factory-Default Configuration *(continued)*

Configurable Setting	Default Value
Untagged VLAN ID	1
Country Code/ Regulatory Domain Settings	
Country code	Based on product SKU
Broadcast of country code in access point beacons and probe responses (IEEE 802.11d world mode)	Enabled
Virtual Access Point Settings	
Virtual access point 0 on radio 1 and radio 2	SSID: juniper-default VLAN ID: 1 Security: WPA2-Personal Encapsulation: AES Key: juniper-wireless Broadcast SSID: yes MAC authentication type: none
Radio Settings	
Radio 1:	State: on IEEE 802.11 mode: 802.11a/n 802.11a/n channel: auto Channel bandwidth: 40 MHz
Radio 2:	State: on IEEE 802.11 mode: 802.11b/g/n 802.11b/g/n channel: auto Channel bandwidth: 20 MHz

Table 3: AX411 Access Point Factory-Default Configuration *(continued)*

Configurable Setting	Default Value
Radios 1 and 2:	Primary channel: lower Protection: auto Maximum number of clients: 200 Transmit power: 100 percent Supported IEEE rate sets: • 802.11a—54, 48, 36, 24, 18, 12, 9, 6 • 802.11b—11, 5.5, 2, 1 • 802.11g—54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 • 5 GHz 802.11n—54, 48, 36, 24, 18, 12, 9, 6 • 2.4 GHz 802.11g—54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 Basic IEEE rate sets: • 802.11a—24, 12,, 6 • 802.11b— 2, 1 • 802.11g—11, 5.5, 2, 1 • 5 GHz 802.11n—24, 12, 6 • 2.4 GHz 802.11g—11, 5.5, 2, 1 Broadcast/multicast rate limiting: disabled Fixed multicast rate: auto Beacon interval: 100 DTIM period: 2 Fragmentation threshold: 2346 RTS threshold: 2347
Quality of Service	
WMM	Enabled

AX411 Access Point Configuration Overview

You configure the AX411 Access Point using the Junos OS CLI or J-Web interface on the SRX Series device.

NOTE: Accessing the AX411 Access Point through its console port is not supported.

Accessing the AX411 Access Point through SSH is disabled by default. You can enable the SSH access using the **set wlan access-point < name > external system services enable-ssh** command.

While configuring the AX411 Access Point on your SRX Series devices, you must enter the WLAN admin password using the **set wlan admin-authentication password** command. This command prompts for the password and the password entered is stored in encrypted form.

NOTE:

- Without wlan config option enabled, the AX411 Access Points will be managed with the default password.
- Changing the **wlan admin-authentication** password when the **wlan subsystem** option is disabled might result in mismanagement of Access Points . You might have to power cycle the Access Points manually to avoid this issue.
- The SRX Series devices that are not using the AX411 Access Point can optionally delete the **wlan config** option.

To change the default configuration of an access point, you must first specify the MAC address of the access point being configured. The MAC address links an access point to its configuration on the SRX Series device.

You can determine the MAC address of an access point in one of the following ways:

- If you have physical access to the access point, view the MAC address printed on the bottom of the device.
- Use CLI operational command **show system services dhcp binding** to display the MAC address of the access point.
- From the J-Web user interface, select **Monitor>Wireless LAN** and click the **Select an access point** menu.

To specify the MAC address of an access point:

```
[edit]
user@host# set wlan access-point ap–1 mac-address 00:12:cf:c7:5d:c0
```

In this example, the access point with the MAC address 00:12:cf:c7:5d:c0 is configured with the name **ap-1**.

If you remove the configuration for an access point from the SRX Series Services Gateway, the access point is reset to its factory default.

NOTE: Changing some access point settings might cause the access point to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change access point settings when WLAN traffic is low.

Related Documentation

- System and Network Configuration Overview on page 17
- Radio Configuration Overview on page 27

- Virtual Access Point Configuration Overview on page 40
- Understanding Quality of Service on page 55

CHAPTER 3

System and Network Settings

System and Network Configuration Overview

Configure the following system and network settings for the access point:

- Interface on the SRX Series device to which the access point is connected.
- System settings, which include:
  - Network Time Protocol (NTP) server.
  - Console port baud rate.
  - Ethernet settings, including static IP address and default gateway, management and untagged VLAN IDs, and DNS server address.
- If your network uses IEEE 802.1x standard port-based network authentication control to allow devices to connect, the access point can be configured to provide a username and password for authentication.

Related Documentation

- Understanding How the Access Point Obtains an IP Address on page 18
- Understanding Layer 2 Forwarding Operations on page 18
- Understanding NTP Support on page 19
- Understanding 802.1x Authentication of the Access Point on page 19

Understanding How the Access Point Obtains an IP Address

This topic describes how the access point obtains an IP address.

By default, the DHCP client on the AX411 Access Point automatically broadcasts requests for an IP address and other network information when the access point is powered on. At its initial startup, the access point obtains its IP address from the DHCP server on the SRX Series device. After the access point has established a connection to the SRX Series device, you can configure static IP and default gateway addresses for the access point.

When the access point obtains an IP address from a DHCP server, you can run one of the following CLI operational mode commands to view the IP address of the access point:

- user@host> **show wlan access-points *name***
- user@host> **show wlan access-points *name* detail**

Related Documentation

- Understanding Layer 2 Forwarding Operations on page 18
- AX411 Access Point Configuration Overview on page 13

Understanding Layer 2 Forwarding Operations

In typical deployments, configure the PoE port of the SRX Series device as a Layer 2 port (**family ethernet-switching**) that is a VLAN trunk or access port. Configuring the port as a Layer 2 port enables spanning VLANs across access points.

All access points connected to a single SRX Series device and all the wired clients connected to the Layer 2 ports of the same SRX Series device form a single switching domain. This facilitates Layer 2 roaming of wireless clients between the access points connected to the same SRX Series device.

When clients connected to the same access point are on the same VLAN, the access point forwards traffic between the clients. A VLAN can span across access points and also between a wired LAN and a wireless LAN. When clients on the same VLAN are connected to different access points, the switching functions on the SRX Series device forwards traffic between the clients. When there are wireless clients connected to an access point and wired clients connected to a port on the SRX Series device on the same VLAN, the switching functions on the SRX Series device forward traffic between the clients.

Packets received from the access point on the Layer 2 port are regular Ethernet packets and are indistinguishable from Ethernet packets received on other Layer 2 ports connected to wired devices. The packets can be switched or routed through the VLAN Layer 3 interface. Firewall policies can be configured on VLAN Layer 3 interfaces to inspect traffic that is routed from wireless clients.

Related Documentation

- Understanding Management VLAN Support on page 19
- Understanding Untagged VLAN Designation on page 19

Understanding Management VLAN Support

The management VLAN is the VLAN associated with the IP address used to access the access point. Management traffic to and from the AX411 Access Point is sent on the management VLAN. The access point ignores any management traffic received from a different VLAN.

The management VLAN can be the same as one of the VLANs configured for a virtual access point or a different VLAN. The default management VLAN configured on the AX411 Access Point is VLAN 1. This VLAN is also the default untagged VLAN. If you already have a management VLAN configured on your network with a different VLAN ID, change the management VLAN ID on the access point by specifying a number from 2 to 4094.

Related Documentation

- Example: Configuring the Management VLAN on page 20

Understanding Untagged VLAN Designation

The access point allows one VLAN ID to be configured as the ID for “untagged” traffic. When untagged traffic is received on the Ethernet interface, the access point assigns this VLAN ID to the traffic. When the access point sends traffic destined to the untagged VLAN out of the Ethernet interface, the traffic is untagged. The default untagged VLAN is VLAN 1.

Related Documentation

- *Junos OS CLI Reference*

Understanding NTP Support

The access point supports a Network Time Protocol (NTP) client that can obtain and maintain its time from a server on the network. Using an NTP server provides the access point with the correct time for log messages and session information. The NTP client sends requests to a configured NTP server every 3600 seconds.

Related Documentation

- *Junos OS CLI Reference*

Understanding 802.1x Authentication of the Access Point

On networks that use IEEE 802.1x port-based network access control, an 802.1x authenticator must grant access to a supplicant. As an 802.1x supplicant, the AX411 Access Point can provide configured information to the authenticator to gain access to the network. If your network uses 802.1x, you must configure a Message Digest 5 (MD5) username and password that the access point can use for its authentication. Both the username and password can be 1 to 64 characters in length. ASCII printable characters are allowed, which includes upper- and lowercase alphabetic letters, digits, and special symbols such as @ and #.

Related Documentation

- Example: Configuring 802.1x Authentication on page 21

Example: Configuring the Management VLAN

This example shows how to configure the management VLAN ID for an access point.

Requirements

Before you begin, specify the MAC address of the access point being configured. See "AX411 Access Point Configuration Overview" on page 13.

Overview

In this example, you set the management VLAN ID to 123 for access point ap-1.

Configuration

GUI Step-by-Step Procedure

To configure the management VLAN:

1. Select **Configure>Wireless LAN>Settings**.
2. Under AP Name, select **ap-1**, then click **Edit**.
3. In the Edit - Access Point window, select the Management tab.
4. Next to Management VLAN ID, enter **123**.
5. Click **OK**.

Step-by-Step Procedure

To configure the management VLAN:

1. Specify the WLAN access point and the management VLAN ID.

```
[edit]
user@host# set wlan access-point ap-1 external system ports ethernet
  management-vlan 123
```

2. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show wlan access-point ap-1** command.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Management VLAN Support on page 19

Example: Configuring 802.1x Authentication

This example shows how to configure the access point to provide a username and password for 802.1x authentication.

Requirements

Before you begin, specify the MAC address of the access point being configured. See "AX411 Access Point Configuration Overview" on page 13.

Overview

In this example, you configure the username (Ap-496) and password (Tn734axc) that access point ap-1 uses to validate itself with an 802.1x authenticator.

Configuration

GUI Step-by-Step Procedure

To configure 802.1x authentication:

1. Select **Configure>Wireless LAN>Settings**.
2. Under AP Name, select **ap-1**, then click **Edit**.
3. In the Edit - Access Point window, select the Basic Settings tab.
4. Under Dot1x supplicant, enter the username **Ap-496** and the password **Tn734axc**.
5. Click **OK**.

Step-by-Step Procedure

To configure 802.1x authentication:

1. Configure the WLAN access point, username, and password.

```
[edit]
user@host# set wlan access-point ap-1 external dot1x-supplicant username Ap-496
  password Tn734axc
```

2. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show wlan access-point ap-1** command.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding 802.1x Authentication of the Access Point on page 19

CHAPTER 4

Country Code and Regulatory Domain

Understanding the Country Code

The country code affects the radio modes, list of channels, and radio transmission power that the AX411 Access Point can support. Wireless regulations vary from country to country. Make sure you select the correct code for the country in which the access point operates so that the access point complies with the regulations in that country.

Related Documentation

- Understanding Radio Modes on page 28
- Understanding Power and Channel Assignment on page 29

Understanding Regulatory Domains and IEEE 802.11d

The country code setting identifies the regulatory domain in which the access point operates.

The AX411 Access Point supports the IEEE 802.11d (world mode) standard by default. This standard causes the access point to broadcast the country it is operating in as part of its beacons and probe responses. This standard allows client stations to operate in any country without reconfiguration. For example, the wireless laptop belonging to a visitor from Europe can associate with an access point in the United States and automatically switch to the correct channel settings without the user reconfiguring the laptop settings.

You can disable the access point from broadcasting the country code in its beacons. However, this only applies to radios configured to operate in the **g** (2.4 GHz) band. For radios operating in the **a** (5 GHz) band, the access point software configures support for 802.11h. When 802.11h is supported, the country code information is broadcast in the beacons.

NOTE: On AX411 Access Points, the possible completions available for the configuring the country code displays the list of all the countries, and it is not based on the regulatory domain within which the access point is deployed.

Related Documentation

- Example: Disabling Country Broadcast on page 24

Example: Disabling Country Broadcast

This example shows how to disable the access point from broadcasting the country code in its beacons and probe responses.

Requirements

Before you begin, specify the MAC address of the access point being configured. See "AX411 Access Point Configuration Overview" on page 13.

Overview

In this example, you disable radio 1 on access point ap-1 from broadcasting the country in which it is operating in its beacons and probe responses.

Configuration

GUI Step-by-Step Procedure

To disable the access point from broadcasting the country in which it is operating:

1. Select **Configure>Wireless LAN>Settings**.
2. Under AP Name, select **ap-1**.
3. Under Radio ID, select **radio 1**, then click **Edit**.
4. In the Edit - Radio window, select the Radio Settings tab.
5. Under 802.11d Support, click **Disable**.
6. Click **OK**.

Step-by-Step Procedure

To disable the access point from broadcasting the country in which it is operating:

1. Specify the WLAN access point and radio options.

   ```
   [edit]
   user@host# set wlan access-point ap-1 radio 1 radio-options disable-dot11d
   ```

2. If you are done configuring the device, commit the configuration.

   ```
   [edit]
   ```

```
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show wlan access-point ap-1** command.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding the Country Code on page 23
- Understanding Regulatory Domains and IEEE 802.11d on page 23

CHAPTER 5

Radio Settings

Radio Configuration Overview

The AX411 Access Point supports dual radios, each of which can be configured independently. A radio can operate in any one of the radio modes specified by IEEE wireless networking standards such as 802.11a, 802.11b/g, or 802.11n. The radio mode determines what type of wireless clients can connect to the access point. The radio on the access point can be configured to support just one type of wireless client or a mixed mode where different types of clients can connect to the radio.

NOTE: **Applying changes to radio settings can cause the access point to stop and restart system processes. If this happens, wireless clients that are connected to the access point will temporarily lose connectivity. We recommend that you change radio settings when WLAN traffic is low.**

Related Documentation

- Understanding Turning a Radio Off on page 28
- Understanding Radio Modes on page 28
- Understanding Power and Channel Assignment on page 29
- Understanding Transmit Power Allocation on page 29
- Understanding IEEE 802.11n on page 31
- Understanding Maximum Client Associations on page 34

Understanding Turning a Radio Off

Radios on the access point are enabled by default. You can disable a radio in its configuration. Disabling an active radio causes the access point to broadcast a deauthentication message to connected wireless clients. This action triggers the clients to start authentication and association processes immediately with other available access points.

Any virtual access point configured for the radio is not visible to wireless clients until the radio is enabled again.

Related Documentation

- *Junos OS CLI Reference*
- Understanding Access Point Shutdown on page 75

Understanding Radio Modes

The radio mode defines the Physical Layer (PHY) standard that the radio uses. The radio mode determines the types of wireless clients that can connect to the access point.

NOTE: **The modes available on the AX411 Access Point depend on the country code setting.**

For each radio, select one of the following modes:

- IEEE 802.11a—Only 802.11a clients can connect to the access point.
- IEEE 802.11b/g—802.11b and 802.11g clients can connect to the access point.
- IEEE 802.11a/n—802.11a clients and 802.11n clients operating in the 2.4 GHz frequency can connect to the access point.
- IEEE 802.11b/g/n—802.11b, 802.11g, and 802.11n clients operating in the 2.4 GHz frequency can connect to the access point. This is the default mode.
- 5 GHz IEEE 802.11n—Only 802.11n clients operating in the 2.4 GHz frequency can connect to the access point.
- 2.4 GHz IEEE 802.11n—Only 802.11n clients operating in the 5 GHz frequency can connect to the access point.

Related Documentation
- Example: Configuring Radio Settings on page 36

Understanding Power and Channel Assignment

To achieve the desired network performance of the 802.11 radios, you can configure the access point with power and channel settings. The available power and channel settings depend on country code, regulatory domain requirements, and radio mode.

For 802.11a radios, if the regulatory domain requires radar detection on the channel, the dynamic frequency selection (DFS) and transmit power control (TPC) features of 802.11h are activated. DFS is a mechanism that requires wireless devices to share spectrum and avoid co-channel operation with radar systems in the 5-GHz band. DFS requirements vary based on the regulatory domain, which is determined by the country code setting of the access point. Each regulatory domain defines a standard, which specifies the types of waveforms that must be detected as well as the threshold and timing requirements. For example, the European Union Telecommunications Institute (ETSI) standard EN 301 893 V1.3.1 defines the DFS requirements for countries in the ETSI domain. The Federal Communications Commission (FCC) standard FCC 06-96 defines these requirements for FCC countries such as the USA. The AX411 Access Point supports the requirements defined in these standards and also allows the administrator to change the country code configuration from one regulatory domain to another.

Related Documentation
- Understanding Transmit Power Allocation on page 29
- Understanding Channel Assignment on page 30

Understanding Transmit Power Allocation

The AX411 Access Point allows for configuration of transmit power on a per radio basis. The typical transmit power of the 802.11a/b/g mode radio is approximately +17 dBm to +30 dBm. There is a direct relation between the power and cell coverage of the access point. The clients that are not in the cell range would lose connectivity. It is advisable to keep the cell coverage as small as possible to provide more capacity, as capacity and coverage are inversely proportional.

Transmit power assignment is done on a percentage basis. By default, the access point assigns 100 percent power assignment to each radio at startup to give maximum coverage and potentially reduce the number of access points required. The transmit power percentage can be configured on a per-radio basis.

To increase capacity of the network, place access points closer together and reduce the value of the transmit power. This helps reduce overlap and interference among access points. A lower transmit power setting can also keep your network more secure because weaker wireless signals are less likely to propagate outside of the physical location of your network.

Related Documentation
- Example: Configuring Radio Settings on page 36

Understanding Channel Assignment

The channel defines the portion of the radio spectrum the radio uses for transmitting and receiving. The range of available channels for the radio is determined by the radio mode and the country code setting. Each radio mode offers a number of channels, depending on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC) or the International Telecommunication Union (ITU-R).

You can configure a static channel on a per-radio basis. The valid 802.11b/g or 802.11a channel numbers vary depending on the country code. For example, valid 802.11b/g channels for the US are 1 to 11 and valid channels for most European countries are 1 to 13. The default static channel for 802.11b/g is 6. The default static channel for 802.11a is 36.

If the radio is configured to be in 802.11a mode and the country code is covered by a regulatory domain that requires radar detection, then the access point attempts to use the statically configured channel first. If radar is detected on that channel, the access point then uses the 802.11h protocol for selecting the channel. This means selecting a radar-free channel and performing a 60-second availability check before operating on that channel. Regulatory domain requirements specify that the access point must move out of the operating channel within the “channel leave time” (10 seconds) of when radar is detected. Additionally, the access point must perform a 60-second availability check to determine that the new channel is radar-free before operating on that channel. However, per 802.11h, when radar is detected on a channel, the access point sends a channel switch announcement and five beacons with the new channel number. Because the new channel cannot be confirmed within the channel leave time, the new channel number advertised in the channel announcement and beacon frames is the first non-radar channel, which may or may not be the new operating channel. Also, clients that roam to the newly announced channel might time out while waiting for the access point because it will take at least 60 seconds for the access point to actually start operating on its new channel.

If you select **auto** for the channel setting, the access point scans available channels and selects a channel where no traffic is detected. The channel is chosen from the list of valid channels for that country and radio band. In the 5-GHz band, if a radar sensitive channel is selected in regulatory domains that require radar detection, the access point performs a 60-second passive scan searching for radar before operating on that channel. If radar is not detected, the access point will operate on that channel; otherwise, the access point will select another channel from the list of valid channels.

Related Documentation

- Example: Configuring Radio Settings on page 36

Understanding IEEE 802.11n

The AX411 Access Point software provides support for IEEE standard 802.11n – Draft 2.0. This standard enables higher throughput, improved reliability, and improved range.

By default, the access point is configured to operate in a **b/g/n** mode which enables pre-**n** clients to associate with the access point. The **n** clients can also associate in this mode, where they can take advantage of the 802.11n enhancements. You can override the default mode of operation and tune various aspects of the 802.11n standard.

The following sections describe the various 802.11n-specific configurable options.

Radio Mode

The radio mode determines the type of wireless clients that can connect to the access point. The 802.11n access point supports 802.11b, 802.11g, 802.11a, and 802.11n clients. The radio can be configured to support only one type of client or to use a mixed mode in which different types of clients can connect to the radio.

The AX411 Access Point has two radios: radio 1 is set to operate at 5 GHz and radio 2 is set to operate at 2.4 GHz.

Radio 1 supports the following modes:

- 802.11a—Only 802.11a clients can connect to the access point.
- 802.11a/n—802.11a and 802.11n clients operating in 5-GHz frequency can connect to the access point. This is the default mode for this radio.
- 5 GHz 802.11n—Only 802.11n clients operating in 5-GHz frequency can connect to the access point.

Radio 2 supports the following modes:

- 802.11b/g—802.11b and 802.11g clients can connect to the access point.
- 802.11b/g/n—802.11b, 802.11g, and 802.11n clients operating in 2.4-GHz frequency can connect to the access point. This is the default mode for this radio.
- 2.4 GHz 802.11n—Only 802.11n clients operating in 2.4-GHz frequency can connect to the access point.

Channel Bandwidth

The 802.11n specification allows the use of a 40-MHz wide channel. This enables higher data rates to be achieved versus rates obtainable using the “legacy” channel bandwidth of 20 MHz. However, when using a wider channel bandwidth there are fewer channels available for use by other 2.4-GHz or 5-GHz devices. To restrict the use of the channel bandwidth to a 20-MHz channel, you can configure the channel bandwidth. This setting applies to either the 2.4-GHz or 5-GHz bands.

Some regulatory domains do not support the use of 40-MHz channel bandwidth. If the access point is operating in a regulatory domain that does not support a 40-MHz channel bandwidth, then this setting will not apply.

Primary Channel (40-MHz Channel Bandwidth Only)

A 40-MHz channel can be considered to consist of two 20-MHz channels that are contiguous in the frequency domain. These two 20-MHz channels are often referred to as the “primary” and “secondary” channels. The primary channel is used for **n** clients who only support 20-MHz channel bandwidth and legacy clients.

When the access point is configured to use 40-MHz channel bandwidth, you can specify the location of the primary channel—either the upper half or lower half of the 40-MHz channel. When the user selects a 40-MHz channel, the channel choice will always refer to the primary channel.

For example, if the 40-MHz channel is in the 5-GHz band and you have selected channel 36 and specified the primary channel as “upper,” then the primary channel would exist at channel 40, the secondary channel would exist at channel 36, and the center frequency of the 40-MHz channel would exist at channel 38.

Transmission Rates

The 802.11n specification defines a new set of transmission rates to enhance throughput for 802.11n wireless clients. These rates are defined as modulation and coding scheme (MCS) indexes. MCS indexes have different meanings depending on the size of the channel bandwidth in use. The access point software and hardware supports MCS indexes 0-15, and 32 which allows for a maximum transmission rate as high as 270 Mbps. Transmission rates are not configurable.

The access point software and hardware is capable of transmission rates as high as 54 Mbps for legacy devices. When the access point is configured to operate in a “mixed” radio mode (for example, 802.11b/g/n mode), the access point sends and receives frames based on the type of client. By default, the access point always selects the optimum rate for communicating with the client based on wireless network conditions. Note that in a mixed radio mode, you are still allowed to select supported and basic rates. The 802.11n clients are backward compatible with legacy transmission rates (a rate defined in an 802.11 standard prior to 802.11n) and can communicate using these legacy rates.

Default selected values for legacy basic rates are as follows:

- g radio mode—1, 2, 5.5, and 11 Mbps

- a radio mode—6, 12, and 24 Mbps

Default selected values for legacy supported rates are as follows:

- g radio mode—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps
- a radio mode—6, 9, 12, 18, 24, 36, 48, and 54 Mbps

Protection

The 802.11n specification provides protection rules to guarantee that 802.11n transmissions do not cause interference with legacy stations or access points. By default, these protection mechanisms are enabled. However, you can turn off these protection mechanisms.

With protection enabled, protection mechanisms are invoked if legacy devices are within range of the access point. This causes more overhead on every transmission, which has an impact on performance. There is no impact on performance if there are no legacy devices within range of the access point.

NOTE: **Care should be taken when turning protection off because legacy clients or access points within range can be affected by 802.11n transmissions. This setting does not affect a client's ability to associate with the access point.**

There are also protection mechanisms for 802.11g transmissions to provide similar, interference-free operation of legacy 802.11b clients and access points. When you configure the protection setting, both the 802.11n and 802.11g protection mechanisms are affected.

Guard Interval

An additional technique used to improve throughput in 802.11n transmissions is to shorten the guard interval. The guard interval is a time interval inserted between orthogonal frequency division multiplexing (OFDM) symbols in which no valid data is transmitted.

The purpose of this guard interval is to reduce intersymbol and intercarrier interference (ISI and ICI). The 802.11n specification allows for a reduction in this guard interval from 800 nanoseconds (defined in the 802.11a and 802.11g specifications) to 400 nanoseconds. This can yield a 10 percent improvement in data throughput. When you shorten the guard interval, the access point will transmit using a 400 nanoscond guard interval when communicating with clients that also support the short guard interval. This setting is only configurable when one of the 802.11n modes is selected.

Related Documentation

- Example: Configuring Radio Settings on page 36

Understanding Maximum Client Associations

You can configure the maximum number of clients that are allowed to associate with the access point at the same time. Specify a value from 0 to 200. Once this limit is reached, all new client association attempts will be denied.

If you change this setting, all currently associated clients will be forced to reassociate with the access point. If the new maximum is less than the previous number of associated clients, some of the previously associated clients might not be allowed to associate with the access point. For example, if there are 50 clients associated with the access point when you set the new maximum to 30, only the first 30 successfully authenticated clients will be allowed to reassociate with the access point. Any other clients that attempt to reassociate will be denied.

Related Documentation

- Example: Configuring Radio Settings on page 36

Understanding Beacon Intervals

The access point transmits beacon frames at regular intervals to announce the existence of the wireless network. By default, the access point transmits a beacon frame once every 100 milliseconds (10 beacon frames per second). You can specify a different interval from 20 to 2000 milliseconds.

Related Documentation

- *Junos OS CLI Reference*

Understanding DTIM Period

The delivery traffic indication message (DTIM) is an element included in some beacon frames. It indicates the client stations that are currently in low-power mode that have data buffered on the access point awaiting pickup. The DTIM period indicates how often clients serviced by the access point should check for buffered data awaiting pickup on the access point.

You specify the DTIM period in number of beacons. For example, if you set this value to 1, clients check for buffered data on the access point at every beacon. If you set this value to 10, clients check the access point on every tenth beacon. The default is two beacons. You can specify a value from 1 to 255 beacons.

Related Documentation

- *Junos OS CLI Reference*

Understanding Fragmentation Threshold

The fragmentation threshold is a way of limiting the size of packets transmitted over the network. If a packet exceeds the fragmentation threshold, the packet is sent as multiple 802.11 frames.

Fragmentation involves more overhead because of the extra work of dividing and reassembling frames and because it increases message traffic on the network. However, fragmentation can help improve network performance and reliability if properly configured. For example, setting a smaller threshold can help with radio interference problems.

The default fragmentation threshold is the maximum 2346 bytes, which effectively disables packet fragmentation. We recommend that you do not set a lower threshold unless you suspect radio interference. The additional headers applied to each fragment increases overhead on the network and can greatly reduce throughput.

Related Documentation

- *Junos OS CLI Reference*

Understanding RTS Threshold

The request to send (RTS) threshold specifies the packet size of an RTS transmission. This parameter can help control traffic flow through the access point, especially when there are many clients connected.

A low threshold means that RTS packets are sent more frequently, consuming more bandwidth and reducing the throughput of the packet. However, sending more RTS packets can help the network recover from interference or collisions that might occur on a busy network or on a network experiencing electromagnetic interference.

Related Documentation

- *Junos OS CLI Reference*

Understanding Fixed Multicast Rate

You can configure a fixed multicast rate for the transmission of broadcast and multicast packets on a per-radio basis. This parameter can be useful in an environment where multicast video streaming is occurring in the wireless medium, provided the wireless clients are capable of handling the configured rate. Setting this parameter to **auto** means that the best rate is automatically determined. The range of valid values for this parameter are determined by the current setting of the radio mode. The default value is **auto**.

Related Documentation

- *Junos OS CLI Reference*

Understanding Broadcast and Multicast Rate Limiting

Limiting the rate of multicast and broadcast traffic can improve overall network performance by limiting the number of packets transmitted into the wireless network. In some protocols, this limits the number of redundant packets transmitted across the network. The default and maximum rate limit is 50 packets per second.

The burst rate limit allows intermittent bursts of traffic above the rate limit on the network. Setting the burst rate limit determines how much traffic bursts there can be before all traffic exceeds the rate limit. The default and maximum burst rate limit is 75 packets per second.

The maximum rate and maximum rate burst can be configured on a per-radio basis.

Frames exceeding the configured threshold are dropped.

Related Documentation

- *Junos OS CLI Reference*

Understanding Fixed Rate Speeds

You can configure a radio for actual supported rates and advertised rates in megabits per second. You can assign multiple rates to the supported rates. Based on the interference and received strength signal indicator (RSSI), the actual rate is finalized from the list of supported rates.

Supported Rates

Supported rates are the rates that the access point supports. You can specify multiple rates; the access point automatically chooses the most efficient rate based on factors such as error rates and the distance of clients from the access point.

Basic Rates

Basic rates are the rates that the access point advertises to the network. This allows communications to be set up with other access points and clients on the network. It is more efficient for an access point to advertise a subset of its supported rates.

Related Documentation

- *Junos OS CLI Reference*

Example: Configuring Radio Settings

This example shows how to configure radio settings on an access point.

Requirements

Before you begin, specify the MAC address of the access point being configured. See "AX411 Access Point Configuration Overview" on page 13.

Overview

In this example, you configure radio 2 on access point ap-1 and specify the radio mode as bgn, the channel number as 6, and the bandwidth as 40 MHz. You then set the maximum stations as 100 and the transmit power as 75 percent.

Configuration

GUI Step-by-Step Procedure

To configure radio settings:

1. Select **Configure>Wireless LAN>Settings**.
2. Under AP Name, select **ap-1**.
3. Under Radio ID, select **radio 2**, then click **Edit**.
4. In the Edit - Radio window, select the Radio Settings tab.
5. For Radio mode, select **bgn**.
6. Next to Channel, enter **6**.
7. For Channel bandwidth, select **40**.
8. Click **More**.
9. Next to Max stations, enter **100**.
10. Next to Transmit power, enter **75**.
11. Click **OK** to return to the Radio Settings tab.
12. Click **OK**.

Step-by-Step Procedure

To configure radio settings:

1. Specify the WLAN access point, radio options, channel number, and bandwidth.

```
[edit]
user@host# set wlan access-point ap-1 radio 2 radio-options mode bgn channel
  number 6 bandwidth 40
```

2. Set the maximum stations and transmit power.

```
[edit]
user@host# set wlan access-point ap-1 radio 2 radio-options mode bgn
  maximum-stations 100 transmit-power 75
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show wlan access-point ap-1** command.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Transmit Power Allocation on page 29
- Understanding Channel Assignment on page 30
- Understanding IEEE 802.11n on page 31

- Understanding Maximum Client Associations on page 34

CHAPTER 6

Virtual Access Points

Understanding Virtual Access Points

A virtual access point simulates a physical access point. A virtual access point is configured on a per-radio basis. Each radio can have up to 16 viritual access points, with virtual access point IDs from 0 to 15. By default, only one virtual access point (VAP 0) is enabled.

Virtual access points allow the wireless LAN to be segmented into multiple broadcast domains that are the wireless equivalent of Ethernet VLANs. Virtual access points allow different security mechanisms for different clients on the same access point. Virtual access points also provide better control over broadcast and multicast traffic, which can help avoid a negative performance impact on a wireless network.

Each virtual access point is identified by a configured service set identifier (SSID) and a unique basic service set identifier (BSSID). The default SSID for virtual access points 1–15 is **Virtual Access Point *x*,** where ***x*** is the virtual access point ID.

Each virtual access point can be independently enabled or disabled with the exception of VAP 0 on each radio. VAP 0 is the physical radio interface and is always enabled. To disable operation of VAP 0, the radio itself must be disabled. VAP 0 is assigned to the BSSID of the physical radio interface.

Each virtual access point supports all security mechanisms. By default, no security is in place on the access point, so any wireless client can associate with it and access your LAN. You configure secure wireless client access for each virtual access point on an access point.

NOTE: To prevent unauthorized access to the access point and to your network, we recommend that you select and configure a security option other than None for each virtual access point that you enable.

Related Documentation

- Virtual Access Point Configuration Overview on page 40
- Understanding Client Security on page 42

Virtual Access Point Configuration Overview

Configure the following options for each virtual access point:

- SSID—Name for the wireless network. The SSID is broadcast by the access point by default.
- VLAN ID—VLAN ID that the access point adds to wireless client traffic. You can configure each virtual access point to use a different VLAN or you can configure multiple virtual access points to use the same VLAN. If clients authenticate with a RADIUS server, the server can return the VLAN ID for the client traffic.
- Client security options—For each virtual access point, you can configure the client security to control wireless client access.
- (Optional) No broadcasting of the SSID—Disable virtual access point responses to probes broadcast by wireless clients.
- (Optional) HTTP redirect—Redirect the user's first HTTP access to a specified webpage.

NOTE: Applying changes to the virtual access point configuration might cause the access point to stop and restart system processes. If this happens, wireless clients that are connected to the access point will temporarily lose connectivity. We recommend that you change the virtual access point configuration when WLAN traffic is low.

Related Documentation

- Understanding SSIDs on page 41
- Understanding Virtual Access Points and VLANs on page 41
- Understanding Client Security on page 42
- Understanding Key Refresh on page 45
- Understanding MAC Authentication on page 46
- Understanding HTTP Redirect on page 45

Understanding SSIDs

The SSID is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the *network name*. By default, the SSID is broadcast by the access point and can appear in the list of available networks on wireless clients.

Multiple virtual access points can have the same SSID. You can also assign each virtual access point a unique SSID. Multiple SSIDs make a single access point appear as multiple access points to other systems on the network.

You have the option of disabling the broadcast of the SSID on each virtual access point. When the SSID broadcast is disabled, the SSID is not displayed in the list of available networks on a wireless client; the client must have the exact name configured to associate with the access point. Disabling the SSID broadcast also causes the virtual access point to suppress responses to client broadcast probes to all SSIDs.

Disabling the SSID broadcast prevents clients from accidentally connecting to your network, but it does not prevent a hacker from connecting or monitoring unencrypted traffic. Disabling the SSID broadcast offers a minimal level of protection on an exposed network such as a guest network, where the goal is to make it easy for clients to connect and where sensitive information is not accessible.

Related Documentation

- Example: Configuring a Virtual Access Point for No Security and HTTP Redirect on page 48
- Example: Configuring a Virtual Access Point for WPA Enterprise and MAC Filtering on page 50

Understanding Virtual Access Points and VLANs

When a wireless client connects to the access point, the access point tags traffic from the client with a VLAN ID. The VLAN ID can be one of the following:

- Untagged VLAN ID (the default is VLAN 1)
- Default VLAN ID configured for the virtual access point (the default is VLAN 1)
- VLAN ID returned by a RADIUS server when the client is authenticated by the server

An access point can support multiple VLANs. These VLANs can be distributed across virtual access points and radios.

The same VLAN can be configured for multiple virtual access points.

The VLANs can be assigned to wireless clients by the RADIUS server when the clients associate and authenticate. RADIUS-assigned VLANs are created and deleted dynamically as clients associate and disassociate. The first client assigned to a particular VLAN causes the access point to create the VLAN. When the last client using that VLAN disassociates, the VLAN is deleted from the access point. The maximum number of dynamic VLANs is equal to the maximum number of configurable clients on the access point.

The RADIUS server attributes for configuring a VLAN (defined in RFC 3580, *IEEE 802.1x Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*) are as follows:

RADIUS Server Attribute	Value	Description
Tunnel-Type	13	For VLAN tunnels
Tunnel-Medium-Type	6	802 medium
Tunnel-Private-Group-ID	*vlan-id*	VLAN ID assigned to the client (in the range 1–4094)

Frames sent from wireless into wired media are assigned to a VLAN returned by the RADIUS server or the default VLAN for the virtual access point. For unicast frames received from the wired network, the access point looks up destination MAC and VLAN and sends the frame to the appropriate virtual access point(s). For multicast frames a different multicast encryption key is used for each VLAN in the same virtual access point to avoid data leakage between VLANs.

Related Documentation

- Example: Configuring a Virtual Access Point for No Security and HTTP Redirect on page 48
- Example: Configuring a Virtual Access Point for WPA Enterprise and MAC Filtering on page 50

Understanding Client Security

The access point supports several types of authentication methods that are used by clients to connect to the access point. Each of these methods and their associated parameters is configurable on a per virtual access point basis. By default, no security is in place on the access point, so any wireless client can associate with it and access your LAN. You configure secure wireless client access for each virtual access point on an access point.

The following sections describe the security you can configure for wireless clients.

No Security

No security (also referred to as *plain text security*) means that data transferred between clients and the access point is not encrypted. This method allows clients to associate with the access point without any authentication. This is generally not recommended but can be used in conjunction with a guest VLAN and a Web-based authentication server, or for debugging network problems.

Static WEP

Wired Equivalent Privacy (WEP) protocol is a data encryption standard for 802.11 wireless networks. You configure a static 64- or 128-bit preshared key for a virtual access point and its potential clients. Because of its well-documented vulnerabilities, static WEP is generally not recommended in networks that require high security. However, in Wi-Fi Protected Access (WPA) and other networks where clients do not support stronger security methods, static WEP is preferred over None.

Static WEP mode supports key lengths of 64 and 128 bits. The access point also supports the weak initialization vector avoidance to reduce the security constraints related to WEP.

For static WEP, you can also select open system and/or shared key authentication:

- Open system allows any client to associate with the access point. This method is also used with plain text, 802.1X and WPA modes. However, clients must have the correct WEP key configured to successfully decrypt data from the access point and transmit properly encrypted data to the access point.
- Shared key authentication requires the client to have the correct WEP key configured to associate with the access point.

Enabling both open system and shared key supports clients configured for either authentication mode. Clients configured to use WEP with open system are allowed to associate with the access point, but must have the correct key configured to pass traffic. Clients configured to use WEP with shared key must have the proper key configured to associate with the access point.

When using static WEP, follow these guidelines:

- All clients must have their WLAN security set to use WEP; clients must specify one of the WEP keys configured on the access point to decode data transmissions from the access point.
- The access point must be configured with all WEP keys used by clients to decode data transmissions from the clients.
- A specific WEP key must use the same index on both the access point and clients. For example, if the access point is configured with **abc123** for WEP key 3, then the clients must use the same string for WEP key 3.
- Clients can use different keys to transmit data to the access point. Certain wireless client software allows you to configure multiple WEP keys and use a transfer key index to cause the client to encrypt transmitted data using different keys. This ensures that neighboring access points cannot decode each other's transmissions.
- You cannot mix 64- and 128-bit WEP keys between the access point and clients.

Dynamic WEP

Dynamic WEP improves security over static WEP by utilizing 802.1X to distribute dynamically generated keys from the access point to its clients. A RADIUS server provides a WEP key for each client session and regenerates keys at each reauthentication interval.

This method requires a RADIUS server that uses the Extensible Authentication Protocol (EAP), such as the Microsoft Internet Authentication Server. To work with Windows clients, the RADIUS server must support Protected EAP (PEAP) and Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2).

You can use any variety of authentication methods supported by IEEE 802.1x, including certificates, Kerberos, and public key authentication. Clients must be configured to use the same authentication method that the access point uses.

WPA Personal

Wi-Fi Protected Access (WPA) Personal is a Wi-Fi Alliance standard that uses preshared key authentication with Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP) and Temporal Key Integrity Protocol (TKIP) cipher suits. Both WPA and the newer WPA2 standards are supported. If you have both clients that support WPA2 and clients that only support WPA, you can configure the virtual access point to allow both types of clients to associate and authenticate.

WPA Enterprise

Wi-Fi Protected Access (WPA) Enterprise is a Wi-Fi Alliance standard that uses RADIUS server authentication with Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP) and Temporal Key Integrity Protocol (TKIP) cipher suits. This mode allows for use of high security encryption along with centrally managed used authentication. Both WPA and the newer WPA2 standards are supported. If you have both clients that support WPA t2 and clients that only support WPA, you can configure the virtual access point to allow both types of clients to associate and authenticate.

If WPA2 is selected, preauthentication can also be enabled. When a client preauthenticates to an access point, the following RADIUS attributes are stored in the access point's preauthentication cache. These values are applied to the client's session when the client roams to that access point:

- VLAN attributes:
  - Tunnel-type
  - Tunnel-medium-type
  - Tunnel-private-group-id
- Client QoS attributes:

- Vendor-specific (26), WISPr-bandwidth-max-dn
- Vendor-specific (26), WISPr-bandwidth-max-up
- Vendor-specific (26), LVL7-wireless-client-ACL-dn
- Vendor-specific (26), LVL7-wireless-client-ACL-up
- Vendor-specific (26), LVL7-wireless-client-policy-dn
- Vendor-specific (26), LVL7-wireless-client-policy-up

- Session timeout:
  - Session timeout

The session timeout and the system up time (sysUpTime) at the time the preauthentication was performed are stored to calculate and set the remaining session time correctly.

Related Documentation

- Example: Configuring a Virtual Access Point for No Security and HTTP Redirect on page 48
- Example: Configuring a Virtual Access Point for WPA Enterprise and MAC Filtering on page 50

Understanding Key Refresh

You can enable broadcast and session key rotation intervals on a per virtual access point basis. These parameters only apply to security modes that involve key rotation (dynamic WEP and WPA Enterprise).

The broadcast key refresh rate sets the interval at which the broadcast (group) key is refreshed for clients associated to a particular virtual access point. The session key refresh rate specifies the interval at which the access point refreshes session (unicast) keys for each client associated to a particular virtual access point. Each of these rotations can be disabled by setting the interval to zero. The broadcast key refresh timer is started when the access point is configured. This timer expires after every key refresh interval. A client that associates during this interval will get its first broadcast key refresh the next time this timer expires. From the client's perspective, this first refresh will most likely occur before the full refresh rate interval.

Related Documentation

- *Junos OS CLI Reference*

Understanding HTTP Redirect

You can enable the redirection of a wireless user's first Web access to a custom webpage located on an external server. For example, the user might be redirected to a webpage that shows a company logo and network usage policy. The redirection affects only the user's first HTTP access after the wireless client associates with the access point and the user opens a Web browser on the client to access the Internet.

The user might easily miss the webpage by hitting a refresh button on the browser or quickly selecting a different link, or simply accessing the Web through HTTPS. Despite the limitation of the HTTP redirect, this function is commonly deployed by Wi-Fi hotspots.

The HTTP redirect feature is enabled on a per virtual access point basis. When you enable HTTP redirect, you specify the URL to which wireless users are directed.

When HTTP redirect is enabled, HTTP packets are intercepted before any Layer 2 forwarding is performed.

Related Documentation

- Example: Configuring a Virtual Access Point for No Security and HTTP Redirect on page 48

Understanding MAC Authentication

Each wireless network interface card (NIC) used by a wireless client has a unique media access control (MAC) address. A client's MAC address can be used to control access to the access point. MAC authentication can be done either locally or with a RADIUS server. MAC authentication can be the only method of client authentication or it can be performed in addition to other authentication methods. When used in conjunction with other authentication methods, MAC authentication is performed after other authentication.

MAC authentication is configured on a per virtual access point basis and can be set to one of the following options:

- Disabled—No MAC authentication is performed for the virtual access point.
- Local—The client's MAC address is checked against a global list of client MAC addresses that are allowed or denied access to the network. You configure the list with the **station-mac-filter** statement in the [**edit wlan access-point access-point options**] hierarchy. This function is similar to configuring a MAC filter. MAC authentication of a client fails if either an **allow-list** is specified and the client's MAC is not in the list, or a **deny-list** is specified and the client's MAC is in the list. In either case the client is denied association. The global list is applicable to every virtual access point, but the usage of this list is determined by the MAC authentication mode for each virtual access point.
- RADIUS—The client's MAC address is checked against a RADIUS server and the globally configured allow or deny action is used. The password **NOPASSWORD** is used to allow the access point to authenticate the MAC address with the RADIUS server. (This password is global, not per MAC address.) When MAC authentication on the RADIUS server is set to deny mode, the presence of a specified MAC address on the RADIUS server is used to deny network access to that MAC address. If an entry for the client's MAC address is not found on the RADIUS server, the opposite action of the globally configured action is used.

  MAC entries are configured on the RADIUS server as follows:

RADIUS Server Attribute	Description	Range	Usage
User-Name	Ethernet address of the client station	Valid Ethernet MAC address	Required

RADIUS Server Attribute	Description	Range	Usage
User-Password	A fixed password used to look up a client MAC entry	**NOPASSWORD**	Required

Related Documentation

- Example: Configuring a MAC Filter List on page 47

Example: Configuring a MAC Filter List

This example shows how to configure a MAC filter list to control access to an access point.

Requirements

Before you begin, specify the MAC address of the access point being configured. See "AX411 Access Point Configuration Overview" on page 13.

Overview

MAC authentication allows you to control access to an access point based on client MAC addresses. Based on how you set the filter, you can either allow only clients whose MAC addresses are on a filter list or deny clients that are on the list.

In this example, you configure a MAC filter list for access point ap-1. You deny the client MAC addresses (00:08:C7:1B:8C:02 and 00:23:45:67:89:ab) from accessing the wireless network.

Configuration

GUI Step-by-Step Procedure

To configure a MAC filter list:

1. Select **Configure>Wireless LAN>Settings**.
2. Under AP Name, select **ap-1**.
3. In the Edit - Access Point window, select the MAC Filtering tab.
4. Click **Add**.
5. In the Add MAC Filter window, enter **00:08:C7:1B:8C:02**, and click **OK**.
6. Click **Add**
7. In the Add MAC Filter window, enter **00:23:45:67:89:ab**, and click **OK**.
8. For Action, select deny.
9. Click **OK**.

Step-by-Step Procedure

To configure a MAC filter list:

1. Configure the WLAN access point and specify the client MAC address.

   ```
   [edit]
   user@host# set wlan access-point ap-1 access-point-options station-mac-filter
     deny-list mac-address [00:08:C7:1B:8C:02 00:23:45:67:89:ab]
   ```

2. If you are done configuring the device, commit the configuration.

   ```
   [edit]
   user@host# commit
   ```

Verification

To verify the configuration is working properly, enter the **show wlan access-point ap-1** command.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding MAC Authentication on page 46

Example: Configuring a Virtual Access Point for No Security and HTTP Redirect

This example shows how to configure a virtual access point for no security and HTTP redirect.

Requirements

Before you begin, specify the MAC address of the access point being configured. See "AX411 Access Point Configuration Overview" on page 13.

Overview

In this example, you configure virtual-access-point 1 on radio 1 for access point ap-1. You configure WLAN by setting the SSID to open-hotspot, VLAN ID to 2, and security to none. Finally, you configure the WLAN access point so that HTTP redirects to http://www.juniper.net/usage_agreement.html.

Configuration

GUI Step-by-Step Procedure

To configure a virtual access point for no security and HTTP redirect:

1. Select **Configure>Wireless LAN>Settings**.
2. Under AP Name, select **ap-1**.
3. Under Radio ID, select **radio 1**, then click **Edit**.

4. In the Edit - Radio window, select the Radio tab.
5. Next to Virtual Access Points, click **Add**.
6. In the Add - Virtual Access Point window, select the Basic Settings tab.
7. Next to VAP ID, select **1**.
8. Next to SSID, enter **open-hotspot**.
9. Next to VLAN ID, enter **2**.
10. Select **HTTP Redirect**.
11. Next to Redirect URL, enter http://www.juniper.net/usage_agreement.html.
12. Select the Security tab.
13. Next to Security, select **None**.
14. Click **OK**.

Step-by-Step Procedure

To configure a virtual access point for no security and HTTP redirect:

1. Configure WLAN for SSID, VLAN ID, and security.

```
[edit]
user@host# set wlan access-point ap-1 radio 1 virtual-access-point 1 ssid
  open-hotspot vlan 2 security none
```

2. Configure the WLAN access point.

```
[edit]
user@host# set wlan access-point ap-1 radio 1 virtual-access-point 1 http-redirect
  redirect-url http://www.juniper.net/usage_agreement.html
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show wlan access-point ap-1** command.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Client Security on page 42
- Understanding Virtual Access Points and VLANs on page 41
- Understanding SSIDs on page 41
- Understanding HTTP Redirect on page 45

Example: Configuring a Virtual Access Point for WPA Enterprise and MAC Filtering

This example shows how to configure a virtual access point for WPA enterprise and MAC filtering.

Requirements

Before you begin, specify the MAC address of the access point being configured. See "AX411 Access Point Configuration Overview" on page 13.

Overview

In this example, you configure virtual-access-point 2 on radio 1 for access point ap-1. You specify SSID as employee-only and VLAN ID as 217. You then define security as wpa-enterprise , WPA version as v2, chiper suites as both (TKIP and CCMP), RADIUS server IP address as 192.211.1.254, and RADIUS shared secret as sandia#978. You specify MAC authentication type as local. Finally, you specify MAC filtering for denied MAC addresses 00:08:C7:1B:8C:02 and 00:23:45:67:89:ab.

Configuration

CLI Quick Configuration

To quickly configure a virtual access point for WAP enterprise and MAC filtering, copy the following commands and paste them into the CLI:

```
[edit]
set wlan access-point ap-1 radio 1 virtual-access-point 2 ssid employee-only vlan 217
    security wpa-enterprise wpa-version v2
set wlan access-point ap-1 radio 1 virtual-access-point 2 security wpa-enterprise
    cipher-suites both
set wlan access-point ap-1 radio 1 virtual-access-point 2 security wpa-enterprise
    pre-authenticate radius-server 192.211.1.254 radius-key sandia#978
set wlan access-point ap-1 radio 1 virtual-access-point 2 security mac-authentication-type
    local
set wlan access-point ap-1 access-point-options station-mac-filter deny-list mac-address
    [00:08:C7:1B:8C:02 00:23:45:67:89:ab]
```

GUI Step-by-Step Procedure

To configure a virtual access point for WPA enterprise and MAC filtering:

1. Select **Configure>Wireless LAN>Settings**.
2. Under AP Name, select **ap-1**.
3. Under Radio ID, select **radio 1**, then click **Edit**.
4. In the Edit - Radio window, select the Radio tab.
5. Next to Virtual Access Points, click **Add**.
6. In the Add - Virtual Access Point window, select the Basic Settings tab.

7. Next to VAP ID, select **2**.
8. Next to SSID, enter **employee-only**.
9. Next to VLAN ID, enter **217**.
10. Clear **HTTP Redirect**.
11. Select the Security tab.
12. Next to MAC authentication type, select **Local**.
13. Next to Security, select **WPA Enterprise**.
14. Next to WPA Version, select **v2**.
15. Next to Cipher suites, select **both**.
16. Select **Pre authenticate**.
17. Next to Radius server, enter **192.211.1.254**.
18. Next to Radius key, enter **sandia#978**.
19. Click **OK** to return to the Edit - Radio window.
20. Click **OK** to return to the Wlan Settings page.
21. Under AP Name, select **ap-1**.
22. In the Edit - Access Point window, select the MAC Filtering tab.
23. Click **Add**.
24. In the Add MAC Filter window, enter **00:08:C7:1B:8C:02**, and click **OK**.
25. Click **Add**.
26. In the Add MAC Filter window, enter **00:23:45:67:89:ab**, and click **OK**.
27. For Action, select **deny**.
28. Click **OK**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the *Junos OS CLI User Guide*.

To configure a virtual access point for WPA enterprise and MAC filtering:

1. Configure the WLAN access point.

   ```
   [edit]
   user@host# edit wlan access-point ap-1
   ```

2. Configure a virtual access point.

   ```
   [edit wlan access-point ap-1]
   user@host# edit radio 1 virtual-access-point 2
   ```

3. Specify SSID and VLAN ID.

   ```
   [edit wlan access-point ap-1 radio 1 virtual-access-point 2]
   ```

```
user@host# set ssid employee-only vlan 217
```

4. Configure security.

```
[edit wlan access-point ap-1 radio 1 virtual-access-point 2]
user@host# edit security wpa-enterprise
```

5. Define WPA version, cipher suites, pre authentication, radius server IP address, and RADIUS shared secret key.

```
[edit wlan access-point ap-1 radio 1 virtual-access-point 2 security wpa-enterprise]
user@host# set wpa-version v2
user@host# set cipher-suites both
user@host# set pre-authenticate radius-server 192.211.1.254 radius-key sandia#978
```

6. Specify MAC authentication type.

```
[edit wlan access-point ap-1 radio 1 virtual-access-point 2]
user@host# set security mac-authentication-type local
```

7. Set MAC filtering for denied MAC addresses.

```
[edit wlan access-point ap-1]
user@host# set access-point-options station-mac-filter deny-list mac-address
  [00:08:C7:1B:8C:02 00:23:45:67:89:ab]
```

Results From configuration mode, confirm your configuration by entering the **show wlan access-point ap-1** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show wlan access-point ap-1
access-point-options {
  station-mac-filter {
  deny-list {
  mac-address [ 00:08:C7:1B:8C:02 00:23:45:67:89:ab ];
    }
  }
  }
  radio 1 {
    virtual-access-point 2 {
    ssid employee-only;
    vlan 217;
    security {
      mac-authentication-type local;
    wpa-enterprise {
    wpa-version {
      v2;
    }
    cipher-suites {
      both;
    }
    pre-authenticate;
      radius-server 192.211.1.254;
      radius-key "$9$JzDqfTQnp0IjHz69CB1hSylLxs24oGD"; ## SECRET-DATA
      }
    }
  }
```

```
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- Verifying Virtual Access Point for WPA Enterprise and MAC Filtering on page 53

Verifying Virtual Access Point for WPA Enterprise and MAC Filtering

Purpose Verify that the virtual access point for WPA enterprise and MAC filtering is configured properly.

Action From configuration mode, enter the **show wlan access-point ap-1** command.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Virtual Access Point Configuration Overview on page 40
- Understanding SSIDs on page 41
- Understanding Virtual Access Points and VLANs on page 41
- Understanding Client Security on page 42

CHAPTER 7

Quality of Service

Understanding Quality of Service

Quality of service (QoS) configuration allows you to tune throughput and performance for different types of wireless traffic such as voice over IP (VoIP), audio, video, streaming media, or traditional IP data. You can specify minimum and maximum transmission wait times for traffic queues from the access point to the client and/or from the client to the access point.

The default values configured for traffic queues are those suggested by the Wi-Fi Alliance in the Wi-Fi Multimedia (WMM) specification. These values should not need to be changed in normal use.

NOTE: QoS settings apply to either radio 1 and radio 2 in the AX411 Access Point and traffic for each radio is queued independently.

NOTE: Changing QoS settings might cause the access point to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change access point settings when WLAN traffic is low.

Related Documentation

- Understanding Wi-Fi Multimedia on page 56
- Understanding Traffic Prioritization on page 57
- Understanding WMM Power Save on page 61
- Understanding No Acknowledgment on page 61

Understanding Wi-Fi Multimedia

The Wi-Fi Multimedia (WMM) specification provides prioritization of packets for four types of traffic:

- Voice—High priority queue with minimum delay. Time-sensitive data such as VoIP and streaming mode are automatically sent to this queue.
- Video—High priority queue with minimum delay. Time-sensitive video data is automatically sent to this queue.
- Best effort—Medium priority queue with medium throughput and delay. Most traditional IP data is sent to this queue.
- Background—Lowest priority queue with high throughput. Bulk data that requires maximum throughput but is not time-sensitive (for example, FTP data) is sent to the queue.

Priority is based on the 802.11 Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. When multiple devices try to access the wireless medium at the same time, packet collisions can occur. To minimize the chances of packet collision, a client must wait for a randomly selected time and then check to see if any other device is communicating on the medium before it starts to transmit.

The wait time consists of a fixed period called the arbitration interframe spacing (AIFS) followed by a random period called the contention window. You can specify the minimum and maximum contention window values.

The WMM specification suggests different wait times for each of the traffic queues so that applications that are sensitive to packet delays have less time to wait and therefore have a better chance of transmitting on the network. To allow consistent QoS across both wireless and wired networks, the queues defined in the WMM specification map to IEEE 802.1d prioritization tags (see Table 4 on page 56).

Table 4: WMM Queues to IEEE 802.1d Tag Mapping

WMM Queue	IEEE 802.1d Tag
Voice	7, 6
Video	5, 4
Best Effort	0, 3
Background	2, 1

Related Documentation

- *Junos OS CLI Reference*

Understanding Traffic Prioritization

The access point automatically prioritizes all data traffic that it forwards. The access point uses the WMM indicator, the 802.1p priority tag, and DiffServ code point (DSCP) to prioritize traffic. The access point also supports the SpectraLink Voice Priority (SVP) traffic classification.

WMM voice frames are not subject to 802.11n frame aggregation. This allows for low latency of each voice frame in a WMM voice traffic stream. Depending on the traffic on the network, this could give the appearance that aggregated WMM traffic—such as video—is being given higher priority than voice because the aggregated throughput of video traffic could be higher than the voice traffic. However, each unaggregated voice data frame is actually being assigned to a higher priority WMM queue.

The following sections define the rules for prioritizing frames.

- Frames Received on Wireless Medium on page 57
- Frames Received on Wired Medium on page 59
- DiffServ Marking Effects on Frame Priority on page 60

Frames Received on Wireless Medium

For packets received on the wireless medium the access point checks whether the frame contains WMM markings in the header. If the markings are present, the access point maps the WMM user priority (802.11e) to 802.1p priority as shown in Table 5 on page 57.

Table 5: 802.11e to 802.1p Priority Mapping

802.11e Priority	Access Category	802.1p Priority
1	Background	1
2	Background	2
0	Best Effort	0
3	Best Effort	3
4	Video	4
5	Video	5
6	Video	6
7	Video	7

Note that 802.1p priority 0 is given higher priority by the network than 802.1p priority 1 and 2.

If the incoming frame does not contain WMM markings, the access point checks whether the frame contains SpectraLink Voice Priority (SVP) protocol packets. Only IPv4 frames are checked for the SVP protocol packets. Any frame using the SVP protocol is assigned 802.1p priority 6.

If the frame does not contain SVP protocol packets, the access point examines the DSCP field. Only IPv4 frames are classified using the DSCP field. Table 6 on page 58 maps DSCP values to the assigned 802.1p priorities.

Table 6: DSCP to 802.1p Priority Mapping for Wireless Medium

DSCP Value	Code Point Designation	802.1p Priority
56	CS7	7
48	CS6	6
46	EF	6
40	CS5	5
38, 36, 34	AF4x	4
32	CS4	4
30, 28, 26	AF3x	4
24	CS3	3
22, 20,18	AF2x	3
16	CS2	2
14, 12, 10	AF1x	3
8	CS1	1
0	CS0	0

Frames that do not fall into any of the categories in Table 6 on page 58 are assigned 802.1p priority 0.

The access point has only one queue on the Ethernet port for packets to be transmitted to the wired side. This is based on the assumption that the Ethernet medium can handle more traffic than the access point can receive from the wireless side. Thus, an 802.11n access point must be connected to a Gigabit Ethernet port.

If the access point transmits the frame back into the wireless medium, then it uses the priority to select the appropriate egress queue in the same way as for traffic received from the wired network. The access point supports eight queues per radio for the packets to be transmitted to the wireless side.

Frames Received on Wired Medium

The access point can receive tagged and untagged frames on the wired medium. The access point prioritizes ingress traffic on the Ethernet port based on the 802.1p tag and the DSCP value. The Ethernet port prioritization is always enabled, even when WMM is disabled.

The frames destined to wireless clients are not tagged. The priority is only used for internal processing. If the frame uses the SVP protocol, then the 802.1p priority is set to 6. For other IPv4 frames the priority is assigned as shown in Table 7 on page 59.

Table 7: DSCP to 802.1p Priority Mapping for Wired Medium

DSCP Value	Code Point Designation	802.1p Priority
56	CS7	7
48	CS6	6
46	EF	6
40	CS5	5
38, 36, 34	AF4x	4
32	CS4	4
30, 28, 26	AF3x	4
24	CS3	3
22, 20,18	AF2x	3
16	CS2	2
14, 12, 10	AF1x	3
8	CS1	1
0	CS0	0

Untagged IPv4 frames use Table 7 on page 59 to assign 802.1p priority. Untagged non-IPv4 frames are prefixed with a tag containing 802.1p priority equal to 0. Tagged frames that are not using the SVP protocol use the priority in the tag to direct the packet to the correct wireless egress queue.

The next step is to map the 802.1p priority to the appropriate egress queue. The mapping works differently depending on whether WMM is enabled on the access point. If WMM is not enabled, then non-SVP traffic is mapped to the same hardware egress queue. SVP

traffic is mapped to a high priority hardware queue, which is configured using the following egress attributes:

- Arbitration interframe space (AIFS)=1
- Minimum contention window (cwMin)=0
- Maximum contention window (cwMax)=0
- Number of milliseconds of the longest burst (maxBurst)=1.5

When WMM is disabled, the transmitted 802.11 frames do not contain WMM markers.

When WMM is enabled, the SVP traffic is queued to the “voice” hardware queue. The other traffic is mapped to hardware queues based on the 802.1p priorities as shown in Table 8 on page 60.

Table 8: 802.11p to 802.1e Priority Mapping

802.11p Priority	Access Category	802.1e Priority
1	Background	1
2	Background	2
0	Best effort	0
3	Best effort	3
4	Video	4
5	Video	5
6	Video	6
7	Video	7

When WMM is supported by both the client and the access point, the frames contain WMM markers. If only the access point supports WMM then the frame is sent using the appropriate queue, but does not contain the WMM markers.

DiffServ Marking Effects on Frame Priority

The access point supports DiffServ as part of its client QoS feature, which allows for a frame to be marked as part of a configurable policy attribute action. A marking action can alter the 802.1p priority or the IP DSCP/precedence field of a frame to any of the values defined in the preceding tables.

Whenever DiffServ marks the 802.1p field of a frame, it also sets the internal frame priority to the same value. Whenever DiffServ marks the IP DSCP or IP Precedence field of a frame, it sets the internal frame priority to the same value as indicated in the 802.1p column in Table 7 on page 59, although it does not actually change the contents of the 802.1p field in the frame itself. Note that an IP Precedence marking is interpreted according

to its compatibility selector (CSx) code point value for purposes of referencing the DSCP mapping table. The updated internal frame priority is then used in the usual manner to determine the WMM queue mapping for frames traveling in the wired-to-wireless direction, or for frames received from the wireless medium that are forwarded to another wireless station within the same Basic Service Set (BSS).

Related Documentation

- *Junos OS CLI Reference*

Understanding WMM Power Save

The 802.11e standard provides for a power save mechanism called Automatic Power Save Delivery (APSD). The Wi-Fi Alliance's Wi-Fi Multimedia (WMM) specification power save is based on a form of APSD called Unscheduled APSD (U-APSD). The use of U-APSD increases throughput, and it also provides a mechanism for retrieving data on a per access class basis.

Wireless clients set up WMM power save when they associate with the access point. The client selects the access classes (voice, video, best effort, background) that use WMM power save.

WMM power save is enabled by default on the AX411 Access Point; you can disable U-APSD as part of the QoS features. The access point can support both U-APSD clients and legacy power-save clients simultaneously.

NOTE: Disabling or enabling WMM power save has no effect if WMM is disabled.

Related Documentation

- Understanding Wi-Fi Multimedia on page 56
- *Junos OS CLI Reference*

Understanding No Acknowledgment

The 802.11e standard also specifies an option referred to as "no acknowledgment". When this option is used, the MAC does not send an ack when it has correctly received a frame. This means that reliability of "no ack" traffic is reduced, but it improves the overall MAC efficiency for time-sensitive traffic, such as VoIP, where the data has a certain, very strict, lifetime. The "no ack" option also introduces more stringent real-time constraints because if an ack is not expected, then the next frame for transmission has to be ready within a short interframe space (SIFS) period from the end of the last transmission. Also, note that block acks override the WMM "no ack" option. In other words, block acks will be sent when doing frame aggregation even if the "no ack" option is enabled.

NOTE: Configuring no acknowledgment has no effect if WMM is disabled.

Related Documentation

- Understanding Wi-Fi Multimedia on page 56
- *Junos OS CLI Reference*

PART 3

Administration

CHAPTER 8

Packet Capture on the AX411 Access Point

Understanding Packet Capture on the AX411 Access Point

This topic includes the following sections:

Packet Capture on the AX411 Access Point

The AX411 Access Point software supports packet capture functionality. The packet capture tool helps you to analyze network traffic and troubleshoot network problems. The packet capture tool captures real-time data packets traveling over the network, for monitoring and logging. Packets are captured as binary data, without modification.

The access point can capture the following types of packets:

- 802.11 packets received and transmitted on the radio interfaces. The packets captured on radio interfaces include the 802.11 header.
- 802.3 packets received and transmitted on the Ethernet interface.
- 802.3 packets received and transmitted on the internal logical interfaces such as virtual access point interfaces.

The AX411 Access Point wireless packet capture tool operates in capture file mode.

Understanding Capture File Mode on the AX411 Access Point

In capture file mode, captured packets are stored in a file on the access point. The access point can transfer the file to a server through HTTPS.

During the capture you can monitor the capture status, elapsed capture time and current capture file size. The information is updated every 10 seconds while the capture is in progress.

You can specify the following parameters while configuring packet capture on the access point:

- Time—Time duration for the capture. You can specify a duration of 10 to 3600 seconds.
- Maximum file size—The maximum file size of the capture buffer. You can set the file size from 64 to 4096 KB.
- Interface—Interface on which to capture the packets. The interface is selected by specifying an interface name, such as **Radio1** or **Radio1VAP1**.

Table 9 on page 66 provides information on the AX411 Access Point configuration parameters for packet capture on the radio interfaces.

Table 9: Access Point Configuration Parameters for Packet Capture

Parameter	Description
Capture Beacons	• When this parameter is enabled, the access point captures 802.11 beacons detected or transmitted by the radio. • Disabling beacon capture significantly reduces the number of packets captured by the radio in mostly idle networks.
Promiscuous Capture	• When this parameter is enabled, the radio is placed in promiscuous mode (if packet capture is active) and the access point captures all traffic on the channel including traffic that is not destined for this access point. • As soon as the capture is done, the radio reverts to nonpromiscuous mode.
MAC filter	When this parameter is enabled, the access point captures only packets that are transmitted to or received from a client with the specified MAC address. The MAC filter is active only when capture is performed on an 802.11 interface.

NOTE: When you activate the packet capture, the capture proceeds until the capture time reaches the configured duration, the capture file reaches its maximum size, or you stop the capture.

Related Documentation

- AX411 Access Point Configuration Overview on page 13
- Understanding 802.1x Authentication of the Access Point on page 19
- Configuring Packet Capture on the AX411 Access Point (CLI Procedure) on page 66

Configuring Packet Capture on the AX411 Access Point (CLI Procedure)

Before you begin:

- Refer to the *AX411 Access Point Getting Started Guide* and the *AX411 Access Point Hardware Guide* for details about hardware components.

- Configure the AX411 Access Point on the SRX Series device. See "Getting Started with the Default Access Point Configuration" on page 9.

You can configure the packet capture feature on an access point using the following CLI commands:

- To enable packet capture feature for the access point:
  - To enable the packet capture to a file with all options:

    ```
    [edit]
    user@host# request wlan access-point packet-capture start access-point name
      interface interface-name duration capture-duration capture-file capture-file
      file-size-max file-size-max promiscuous capture-beacons filter-mac filter-mac
    ```

    For example:

    ```
    [edit]
    user@host# request wlan access-point packet-capture start mav-ap interface
      Radio1VAP0 + duration 300 capture-file tmp/mav_ap_capture.pcap file-size-max
      2096 + promiscuous disable-beacons filter-mac 00:11:22:33:44:55
    ```

  - To enable the packet capture to a file with mandatory options:

    ```
    [edit]
    user@host# request wlan access-point packet-capture start name interface
      interface-name
    ```

    For example:

    ```
    [edit]
    user@host# request wlan access-point packet-capture start mav-ap interface
      Radio1VAP0
    ```

- To halt the packet capture:

  ```
  [edit]
  user@host# request wlan access-point packet-capture stop ap-name
  ```

  For example:

  ```
  [edit]
  user@host# request wlan access-point packet-capture stop mav-ap
  ```

- To show detailed status of a single access point:

  ```
  [edit]
  user@host# show wlan access-point name detail
  ```

  For example:

  ```
  [edit]
  user@host# user@host# show wlan access-points wap-3 detail
  ```

Related Documentation

- Understanding Packet Capture on the AX411 Access Point on page 65
- AX411 Access Point Configuration Overview on page 13
- Understanding 802.1x Authentication of the Access Point on page 19

CHAPTER 9

System Log Messages on the AX411 Access Point

Understanding System Log Messages on the AX411 Access Point

Junos OS supports configuring and monitoring of system log messages (also called syslog messages). You can configure files to log system messages and also assign attributes, such as severity levels.

The System log messages provide following types of information:

- Client association messages such as
  - Request associations
  - Successful associations
  - Unsuccessful attempt for associations
- Radar detection on a channel
- Configuration change logs
- Logs for user login to system

Related Documentation

- Understanding Packet Capture on the AX411 Access Point on page 65
- AX411 Access Point Configuration Overview on page 13
- Configuring System Log Messages on the AX411 Access Point on page 70

Configuring System Log Messages on the AX411 Access Point

This topic includes the following sections:

Configuring System Log Messages on the AX411 Access Point (CLI Procedure)

To configure system log messages on the AX411 Access Point:

1. Navigate to the top of the configuration hierarchy in the CLI configuration editor and enter

   ```
   [edit]
   user@host# set wlan syslog-options
   ```

2. Enter the following options:

   - **log-size** — Maximum size of each system log file that can be stored on an access point. Range: 4 to 1024 kilobytes.
   - **period** — Specifies the interval, in seconds, between retrieving and storing syslog messages on the SRX Series device. Range: 60 to 86,400 seconds.

   For example:

   ```
   [edit]
   user@host# set wlan syslog-options log-size 64 period 360
   ```

3. If you are finished configuring the system log options, commit the configuration.

   ```
   [edit]
   user@host# commit
   ```

Configuring System Log Messages on Individual Access Points (CLI Procedure)

Table 10 on page 70 provides information on the AX411 Access Point supported configuration parameters that are required for configuring system log messages.

Table 10: Access Point Configuration Parameters for System Log Messages

Parameters	Description
log-level	Defines the severity levels of system messages. This parameter provides 8 levels of severity numbered 0–7. A higher number indicates a higher level of severity.
enable-persistent	Specifies that an access point stores all persistent log events to internal flash memory and the remote server or services gateway periodically fetches these system log messages files from all Access Points.

Table 10: Access Point Configuration Parameters for System Log Messages *(continued)*

Parameters	Description
enable-remote	Specifies that system log message files are not stored on internal flash and will be sent to the remote log server directly.
log-server-address	Specifies the IP address of the remote log server.
log-server-port	Specifies the port of the remote log server.

To configure system log messages on individual access points:

1. Navigate to the top of the configuration hierarchy in the CLI configuration editor and enter

   ```
   [edit]
   user@host# set wlan access-point access-point name logging-options
   ```

2. Enter the options as given in Table 10 on page 70.

   For example, to configure persistent logging:

   ```
   [edit]
   user@host# set wlan access-point ap1 logging-options log-level 7 enable-persistent
   ```

   For example, to configure remote logging:

   ```
   [edit]
   user@host# set wlan access-point ap1 logging-options log-level 7 enable-remote
     log-server-address 10.100.37.178 log-server-port 514
   ```

3. If you are finished configuring the system log options, commit the configuration.

   ```
   [edit]
   user@host# commit
   ```

CHAPTER 10

Access Point Operations

Understanding Access Point Software Upgrades

The AX411 Access Point is shipped with software preinstalled. As new features and software fixes become available, you must upgrade the software on the access point to use them.

The AX411 Access Point retains two software images in its storage. The image that is uploaded most recently to the access point is used as the active image and is loaded into the access point's memory when it is booted. The older software image provides an automatic backup mechanism if the newly loaded software fails to operate or the new image becomes corrupted during the upload process. In either case, the access point will automatically boot up using the backup image.

To download software upgrades, you must have a Juniper Networks Web account and a valid support contract. To obtain an account, complete the registration form at the Juniper Networks website: https://www.juniper.net/registration/Register.jsp .

You can use the Junos OS CLI or J-Web interface to upgrade the software on an access point.

Whenever new software is loaded onto the access point, the existing configuration on the access point is retained and applied.

Related Documentation

- *Junos OS CLI Reference*

Firmware Upgrade on the AX411 Access Point (CLI Procedure)

You can use the CLI configuration editor to upgrade software on an access point.

To upgrade access point software:

1. Navigate to the top of the configuration hierarchy in the CLI configuration editor.
2. Request the firmware upgrade on an access point:

   ```
   [edit]
   user@host# run request wlan access-point firmware upgrade [ name | all ] file [ image ]
   ```

   For example, on a single access point, enter

   ```
   [edit]
   user@host# run request wlan access-point firmware upgrade wap-1 file /var/tmp/upgrade_10_1_0_1.tar
   ```

   On all access points, enter

   ```
   [edit]
   user@host# run request wlan access-point firmware upgrade all file /var/tmp/upgrade_10_1_0_1.tar
   ```

3. Verify the successful completion of the firmware upgrade by checking the firmware version:

   ```
   user@host> show wlan access-points access-points name detail
   ```

CAUTION: Do not power down the access point while an upgrade is in progress.

NOTE: The firmware image has to be provided in a .tar format. Whenever the new image is loaded onto the access point, the configuration on the access point is reset to factory defaults.

Firmware Upgrade on the AX411 Access Point (J-Web)

You can use J-Web Configure to upgrade software on an access point.

In this procedure, the software to be loaded onto the access point is a tar file on a Windows PC. The file is first transferred from the PC to the SRX Series device, and then loaded onto the access point from the SRX Series device.

To upgrade access point software:

1. Copy the tar file that contains the access point software onto the Windows PC that is running the J-Web user interface.
2. In the J-Web user interface, select **Configure>Wireless LAN>Firmware upgrade**.

   The Firmware Upgrade page displays a list of access points configured on the SRX Series Services Gateway.

3. Click **Upgrade**.

4. Select the access point to be upgraded.
5. Enter the name of the tar file to be uploaded to the access point or click **Browse** to navigate to the file.
6. Click **Upgrade**.

Switching to Alternate Firmware on the AX411 Access Point (CLI Procedure)

You can switch to backup firmware using the CLI configuration editor.

To switch to the alternate image:

1. Navigate to the top of the configuration hierarchy in the CLI configuration editor and enter the **run request wlan access-point firmware switch-image** ***name*** command, for example:

   ```
   [edit]
   user@host# run request wlan access-point firmware switch-image mav-ap
   ```

2. Check the version of the alternate image using the **show wlan access-points** ***access-point name*** **detail** command.

   The output displays the firmware and alternate firmware versions.

Understanding Access Point Restart

An access point can be restarted with a CLI command if necessary. When an access point is restarted, any wireless clients that are associated with the access point lose connectivity to the network.

NOTE: You should only restart an access point when directed to do so by your Juniper Networks support representative.

Related Documentation

- *Junos OS CLI Reference*

Understanding Access Point Shutdown

Unplugging an access point from its power source shuts down access point functions. The access point broadcasts a deauthentication message to connected wireless clients. This action triggers the clients to start authentication and association processes immediately with other available access points.

When an access point is unplugged, it is no longer manageable from the SRX Series device. There is no CLI command to shut down an access point.

Related Documentation

- Understanding Turning a Radio Off on page 28

CHAPTER 11

Access Point Monitoring

Monitoring Access Points

Purpose Use the monitoring functionality to view the Access Points page.

Action To monitor access points, select **Monitor>Wireless LAN** in the J-Web interface.

Meaning Table 11 on page 77 summarizes key output fields in the Access Points page.

Table 11: Access Points Monitoring Page

Field	Value	Additional Information
Access Point Details		

Table 11: Access Points Monitoring Page *(continued)*

Field	Value	Additional Information
Name	Displays the following names: • **Access Point**—Name of the access point. • **Type**—Type of access point (internal or external). • **Location**—Location of the access point. • **Serial Number**—Serial number of the access point. • **Firmware Version**—Firmware version for the access point. • **Alternate Version**—Backup firmware for the access point. • **Regulatory Domain**—Regulatory domain of the access point, such as FCC (Federal Communications Commission), ETSI (European Union Telecommunications Institute), TELEC, or WORLD. • **Country**— Country name. • **Access Interface**—Port where the access point is connected. • **Packet Capture**—ON or OFF. The default is OFF. • **MAC Address**— MAC address of the external access point. • **IPv4 Address**—IPv4 address of the access point. • **Status**— ON or OFF. • **MAC Address**— MAC address of radio 1. • **Mode**—Mode of radio 1. The mode can be a, an, or 5GHz 802.11n. The default is 802.11 a/n. • **Channel**—Frequency at which radio 1 operates. • **Status**—ON or OFF. • **MAC Address**—MAC address of radio 2 • **Mode**—Mode of radio 2. The mode can be bg, bgn, or 2.4GHz 802.11n. The default is 802.11 b/g/n • **Channel**—Frequency at which radio 2 operates	
Value	Displays the values for the respective names	
Client Associations		

Table 11: Access Points Monitoring Page *(continued)*

Field	Value	Additional Information
VAP	Virtual access point with which the client is associated. For example, **wlan0vap2** means the client is associated with VAP 2 on radio 1. **wlan0** means the client is associated with VAP 0 on radio 1. **wlan1** means the client is associated with VAP 0 on radio 2.	
Client MAC Address	MAC address of the associated wireless client.	
Authentication	Underlying IEEE 802.11 authentication status, if the virtual access point security mode is set to none or static WEP. This status does not show IEEE 802.1x authentication or association status. If the virtual access point security mode is set to 802.1x or WPA, it is possible for a client association to be shown as being authenticated when it has actually not been authenticated through the second layer of security.	
Packets Rx/Tx	The number of packets received from the wireless clients and transmitted from the access point to the wireless client.	
Bytes Rx/Tx	The number of bytes received from the wireless clients and transmitted from the access point to the wireless client.	
Neighboring Access Points		
MAC Address	MAC address of the neighbor access point.	
Privacy	Security on the neighbor access point: • Off—Security mode is set to none (no security). • On—There is some security in place.	
WPA	WPA security is on or off on the neighbor access point.	

Table 11: Access Points Monitoring Page *(continued)*

Field	Value	Additional Information
Band	IEEE 802.11 mode being used on the neighbor access point: • 2.4—IEEE 802.11b, 802.11g, or 802.11n mode, or a combination of these modes.. • 5—IEEE 802.11a or 802.11n mode, or both modes.	
Channel	Channel on which the neighbor access point is currently broadcasting.	
SSID	Service set identifier that identifies the WLAN that the neighbor access point is broadcasting.	

Related Documentation

- AX411 Access Point Feature Overview on page 4
- AX411 Access Point Configuration Overview on page 13

PART 4

Index

Index

W

