Preface

Audience

This guide is for the networking professional who installs and manages Cisco Aironet Access Points in Autonomous mode. To use this guide, you should have experience working with the Cisco IOS software and be familiar with the concepts and terminology of wireless local area networks.

Note This guide does not cover lightweight access points. Configuration for these devices can be found in the appropriate installation and configuration guides on Cisco.com.

Purpose

This guide provides the information you need to install and configure your access point. This guide provides procedures for using the Cisco IOS software commands that have been created or changed for use with the access point. It does not provide detailed information about these commands. For detailed information about these commands, refer to the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release. For information about the standard Cisco IOS software commands, refer to the Cisco IOS software documentation set available from the Cisco.com home page at **Support > Documentation**.

This guide also includes an overview of the access point web-based interface (APWI), which contains all the functionality of the command-line interface (CLI). This guide does not provide field-level descriptions of the APWI windows nor does it provide the procedures for configuring the access point from the APWI. For all APWI window descriptions and procedures, refer to the access point online help, which is available from the Help buttons on the APWI pages.

Configuration Procedures and Examples

The procedures and examples given in this guide have been documented as seen on the Cisco Aironet 3600 Series Access Points.

To view the latest configuration examples, visit Cisco Tech Zone(https://techzone.cisco.com). In the Tech Zone **Navigator**, browse to **Wireless LAN > Autonomous APs (IOS)** - Knowledge base for Autonomous (IOS) Wireless Deployments.

Note You need to have an account on Cisco.com to access Cisco Tech Zone. If you do not have an account, you can create one by clicking **Register Now** on the Log In page.

Organization

This guide is organized into these chapters:

Chapter 1, "Overview of Access Point Features," lists the software and hardware features of the access point and describes the access point role in your network.

Chapter 2, "Using the Web-Browser Interface," describes how to use the web-browser interface to configure the access point.

Chapter 3, "Using the Command-Line Interface," describes how to use the command-line interface (CLI) to configure the access point.

Chapter 4, "Configuring the Access Point for the First Time,"describes how to configure basic settings on a new access point.

Chapter 5, "Administrating the Access Point," describes how to perform one-time operations to administer your access point, such as preventing unauthorized access to the access point, setting the system date and time, and setting the system name and prompt.

Chapter 6, "Configuring Radio Settings," describes how to configure settings for the access point radio such as the role in the radio network, transmit power, channel settings, and others.

Chapter 7, "Configuring Multiple SSIDs," describes how to configure and manage multiple Service Set Identifiers (SSIDs) and multiple basic SSIDs (BSSIDs) on your access point. You can configure up to 16 SSIDs and up to eight BSSIDs on your access point.

Chapter 8, "Configuring Spanning Tree Protocol,"describes how to configure Spanning Tree Protocol (STP) on your access point, bridge, or access point operating in a bridge mode. STP prevents bridge loops from occurring in your network.

Chapter 9, "Configuring an Access Point as a Local Authenticator," describes how to configure the access point to act as a local RADIUS server for your wireless LAN. If the WAN connection to your main RADIUS server fails, the access point acts as a backup server to authenticate wireless devices.

Chapter 10, "Configuring WLAN Authentication and Encryption," describes how to configure the cipher suites required to use authenticated key management, Wired Equivalent Privacy (WEP), and WEP features including MIC, CMIC, TKIP, CKIP, and broadcast key rotation.

Chapter 11, "Configuring Authentication Types," describes how to configure authentication types on the access point. Client devices use these authentication methods to join your network.

Chapter 12, "Configuring Other Services," describes how to configure the access point to participate in WDS, to allow fast reassociation of roaming client services, and to participate in radio management.

Chapter 13, "Configuring RADIUS and TACACS+ Servers," describes how to enable and configure the RADIUS and Terminal Access Controller Access Control System Plus (TACACS+), which provide detailed accounting information and flexible administrative control over authentication and authorization processes.

Chapter 14, "Configuring VLANs," describes how to configure your access point to interoperate with the VLANs set up on your wired LAN.

Chapter 15, "Configuring QoS," describes how to configure and manage MAC address, IP, and EtherType filters on the access point using the web-browser interface.

Chapter 16, "Configuring Filters," describes how to configure and manage MAC address, IP, and EtherType filters on the access point using the web-browser interface.

Chapter 17, "Configuring CDP," describes how to configure Cisco Discovery Protocol (CDP) on your access point. CDP is a device-discovery protocol that runs on all Cisco network equipment.

Chapter 18, "Configuring SNMP," describes how to configure the Simple Network Management Protocol (SNMP) on your access point.

Chapter 19, "Configuring Repeater and Standby Access Points and Workgroup Bridge Mode," describes how to configure your access point as a hot standby unit or as a repeater unit.

Chapter 20, "Managing Firmware and Configurations," describes how to manipulate the Flash file system, how to copy configuration files, and how to archive (upload and download) software images.

Chapter 22, "Configuring LLDP," describes how to configure the Link Layer Discovery Protocol (LLDP), used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network.

Chapter 23, "Configuring L2TPv3 Over UDP/IP," describes how to configure the Layer 2 Tunneling Protocol (L2TPv3), which is a tunneling protocol that enables tunneling of Layer 2 packets over IP core networks.

Chapter 24, "Configuring Ethernet over GRE," describes Ethernet over GRE (EoGRE), which is a tunneling protocol that enables tunneling of Layer 2 packets encapsulated in GRE header over IP core networks.

Chapter 25, "Configuring System Message Logging," describes how to configure system message logging on your access point.

Chapter 27, "Miscellaneous AP-Specific Configurations," contains miscellaneous configurations that are specific to certain access points.

Appendix A, "Protocol Filters," lists some of the protocols that you can filter on the access point.

Appendix B, "Supported MIBs," lists the Simple Network Management Protocol (SNMP) Management Information Bases (MIBs) that the access point supports for this software release.

Appendix C, "Error and Event Messages," lists the CLI error and event messages and provides an explanation and recommended action for each message.

Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface text**.
- Arguments for which you supply values are in *italic*.
- Square brackets ([ ]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes, cautions, and timesavers use these conventions and symbols:

Note Means reader take note. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means reader be careful. In this situation, you might do something that could result equipment damage or loss of data.

Tip Means the following will help you solve a problem. The tips information might not be troubleshooting or even an action, but could be useful information.

Related Documentation

Release notes for autonomous mode APs are at:

http://www.cisco.com/c/en/us/support/wireless/aironet-3700-series/products-release-notes-list.html

Release notes for lightweight APs, and wireless controllers, are at:

http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-release-notes-list.html

Configuration guides for lightweight APs are included in those for wireless controllers, at:

http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-installation-and-configuration-guides-list.html