ZYXEL
Your Networking Ally

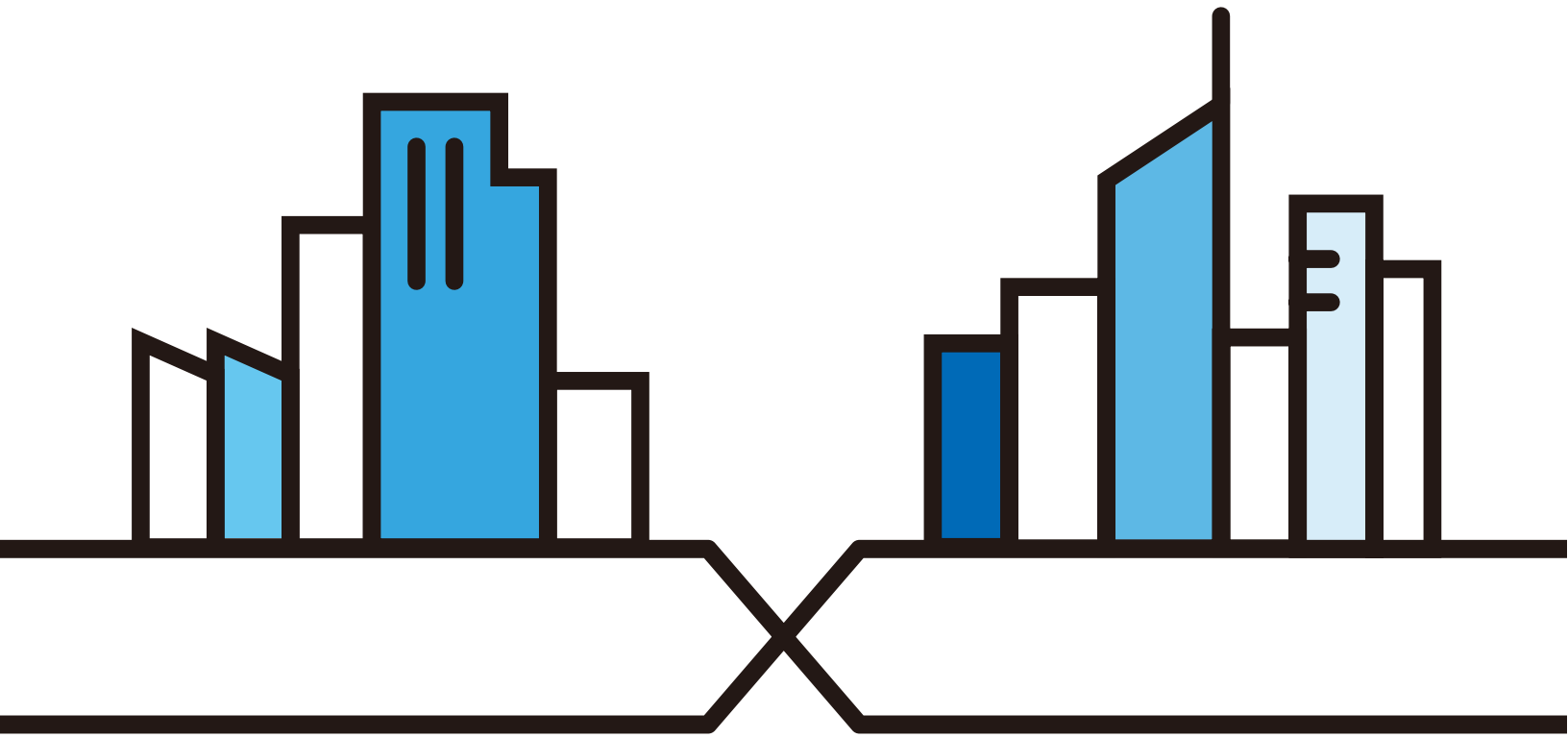
CLI Reference Guide

NWA/WAC Series

802.11 a/b/g/n/ac Access Point

Default Login Details	
LAN IP Address	http://192.168.1.2
User Name	admin
Password	1234

Version 5.30 Edition 1, 07/2018



IMPORTANT!
READ CAREFULLY BEFORE USE.
KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a Reference Guide for a series of products intended for people who want to configure the NWA/WAC via Command Line Interface (CLI).

Note: Some commands or command options in this guide may not be available in your product. See your product's User's Guide for a list of supported features. Every effort has been made to ensure that the information in this guide is accurate.

Note: The version number on the cover page refers to the latest firmware version supported by the NWA/WAC. This guide applies to versions 4.20, 4.21, 4.22, 4.30, 5.00, 5.10, 5.20, 5.25 and 5.30 at the time of writing.

How To Use This Guide

1 Read Chapter 2 on page 17 for how to access and use the CLI (Command Line Interface).

2 Read Chapter 3 on page 28 to learn about the CLI user and privilege modes.

Do not use commands not documented in this guide.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the NWA/WAC and access the Web Configurator.

- User's Guide

  The User's Guide explains how to use the Web Configurator to configure the NWA/WAC.

Note: It is recommended you use the Web Configurator to configure the NWA/WAC.

Icons Used in Figures

Figures in this guide may use the following generic icons. The NWA/WAC icon is not an exact representation of your device.

NWA/WAC	AP Controller	Router	Switch	Internet
				

Contents Overview

Table of Contents

PART I
Introduction

CHAPTER 1
Getting to Know your NWA/WAC

1.1 Overview

Your NWA/WAC is a wireless AP (Access Point). It extends the range of your existing wired network without additional wiring, providing easy network access to mobile users.

You can set the NWA/WAC to operate in either standalone AP or managed AP mode. When the NWA/WAC is in standalone AP mode, it can serve as a normal AP, as an RF monitor to search for rouge APs to help eliminate network threats (if it supports monitor mode and rogue APs detection/containment), or even as a root AP or a wireless repeater to establish wireless links with other APs in a WDS (Wireless Distribution System). A WDS is a wireless connection between two or more APs.

Your NWA/WAC's business-class reliability, SMB features, and centralized wireless management make it ideally suited for advanced service delivery in mission-critical networks. It uses Multiple BSSID and VLAN to provide simultaneous independent virtual APs. Additionally, innovations in roaming technology and QoS features eliminate voice call disruptions.

The NWA/WAC controls network access with Media Access Control (MAC) address filtering, and rogue Access Point (AP) detection. It also provides a high level of network traffic security, supporting IEEE 802.1x, Wi-Fi Protected Access 2 and Wired Equivalent Privacy (WEP) data encryption.

1.1.1 Product Features

The following tables list model specific features.

Table 1 NWA1123 Series Comparison Table

FEATURES	NWA1123-ACv2	NWA1123-AC PRO	NWA1123-AC HD	NWA1302-AC
Supported Wireless Standards	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac
Supported Frequency Bands	2.4 GHz 5 GHz	2.4 GHz 5 GHz	2.4 GHz 5 GHz	2.4 GHz 5 GHz
Available Security Modes	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX
Number of SSID Profiles	64	64	64	64
Number of Wireless Radios	2	2	2	2

Table 1 NWA1123 Series Comparison Table

FEATURES	NWA1123-ACv2	NWA1123-AC PRO	NWA1123-AC HD	NWA1302-AC
Monitor Mode & Rogue APs Containment	No	No	No	No
Rogue APs Detection	Yes	Yes	Yes	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes	Yes	No	No
Tunnel Forwarding Mode	No	No	No	No
Layer-2 Isolation	Yes	Yes	Yes	Yes
Power Detection	No	No	Yes	Yes
External Antennas	No	No	No	No
Internal Antennas	Yes	Yes	Yes	Yes
Antenna Switch	No	Yes	No	No
LED Locator	No	Yes	Yes	Yes
LED Suppression	Yes	Yes	Yes	Yes
Nebula Cloud Management	Yes	Yes	Yes	Yes
CAPWAP Managed AP Mode	No	No	No	No
AC (AP Controller) Discovery	No	No	No	No
802.11r Fast Roaming Support in Managed AP Mode	No	No	No	No
Bluetooth Low Energy (BLE)	No	No	No	No
Maximum number of log messages	512 event logs or 1024 debug logs			

Table 2 NWA5000 Series Comparison Table

FEATURES	NWA5121-N	NWA5121-NI	NWA5123-AC	NWA5123-AC HD	NWA5123-NI	NWA5301-NJ
Supported Wireless Standards	IEEE 802.11b IEEE 802.11g IEEE 802.11n	IEEE 802.11b IEEE 802.11g IEEE 802.11n	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n	IEEE 802.11b IEEE 802.11g IEEE 802.11n
Supported Frequency Bands	2.4 GHz	2.4 GHz	2.4 GHz 5 GHz	2.4 GHz 5 GHz	2.4 GHz 5 GHz	2.4 GHz
Available Security Modes	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX
Number of SSID Profiles	64	64	64	64	64	64

Table 2 NWA5000 Series Comparison Table

FEATURES	NWA5121-N	NWA5121-NI	NWA5123-AC	NWA5123-AC HD	NWA5123-NI	NWA5301-NJ
Number of Wireless Radios	1	1	2	2	2	1
Monitor Mode & Rogue APs Containment	Yes	Yes	Yes	No	Yes	No
Rogue APs Detection	Yes	Yes	Yes	Yes	Yes	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes	Yes	Yes	No	Yes	Yes
Tunnel Forwarding Mode	No	No	No	No	No	No
Layer-2 Isolation	Yes	Yes	Yes	Yes	Yes	Yes
Power Detection	No	No	No	Yes	No	No
External Antennas	Yes	No	No	No	No	No
Internal Antennas	No	Yes	Yes	Yes	Yes	Yes
Antenna Switch	No	No	No	No	No	No
LED Locator	No	No	No	Yes	No	No
LED Suppression	Yes	Yes	Yes	Yes	Yes	Yes
Nebula Cloud Management	No	No	No	No	No	No
CAPWAP Managed AP Mode	Yes	Yes	Yes	Yes	Yes	Yes
AC (AP Controller) Discovery	Yes	Yes	Yes	Yes	Yes	Yes
802.11r Fast Roaming Support in Managed AP Mode	Yes	Yes	Yes	Yes	Yes	Yes
802.11k/v Assisted Roaming	No	No	Yes	No	No	No
Bluetooth Low Energy (BLE)	No	No	No	No	No	No
Maximum number of log messages	256 event logs or 1 debug logs	256 event logs or 1 debug logs	512 event logs or 1024 debug logs	512 event logs or 1024 debug logs	256 event logs or 1 debug logs	256 event logs or 1 debug logs

Table 3 WAC5000/6000 Series Comparison Table

FEATURES	WAC5302D-S	WAC6103D-I	WAC6303D-S
Supported Wireless Standards	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac
Supported Frequency Bands	2.4 GHz 5 GHz	2.4 GHz 5 GHz	2.4 GHz 5 GHz

Table 3 WAC5000/6000 Series Comparison Table

FEATURES	WAC5302D-S	WAC6103D-I	WAC6303D-S
Available Security Modes	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX
Number of SSID Profiles	64	64	64
Number of Wireless Radios	2	2	2
Monitor Mode & Rogue APs Containment	No	Yes	No
Rogue APs Detection	Yes	Yes	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	No	Yes	Yes
Tunnel Forwarding Mode	No	Yes	Yes
Layer-2 Isolation	Yes	Yes	Yes
Power Detection	Yes	No	Yes
External Antennas	No	No	No
Internal Antennas	Yes	Yes	Yes
Antenna Switch	No	Yes	No
LED Locator	Yes	Yes	Yes
LED Suppression	Yes	Yes	Yes
Nebula Cloud Management	No	No	No
CAPWAP Managed AP Mode	Yes	Yes	Yes
AC (AP Controller) Discovery	Yes	Yes	Yes
802.11r Fast Roaming Support in Managed AP Mode	Yes	Yes	Yes
802.11k/v Assisted Roaming	No	Yes	No
Bluetooth Low Energy (BLE)	Yes	No	Yes
Maximum number of log messages	256 event logs or 1 debug logs	512 event logs or 1024 debug logs	512 event logs or 1024 debug logs

Table 4 WAC6500 Series Comparison Table

FEATURES	WAC6502D-E	WAC6502D-S	WAC6503D-S	WAC6552D-S	WAC6553D-E
Supported Wireless Standards	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac
Supported Frequency Bands	2.4 GHz 5 GHz	2.4 GHz 5 GHz	2.4 GHz 5 GHz	2.4 GHz 5 GHz	2.4 GHz 5 GHz

Table 4 WAC6500 Series Comparison Table

FEATURES	WAC6502D-E	WAC6502D-S	WAC6503D-S	WAC6552D-S	WAC6553D-E
Available Security Modes	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX
Number of SSID Profiles	64	64	64	64	64
Number of Wireless Radios	2	2	2	2	2
Monitor Mode & Rogue APs Containment	Yes	Yes	Yes	Yes	Yes
Rogue APs Detection	Yes	Yes	Yes	Yes	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes	Yes	Yes	Yes	Yes
Tunnel Forwarding Mode	Yes	Yes	Yes	Yes	Yes
Layer-2 Isolation	Yes	Yes	Yes	Yes	Yes
Power Detection	Yes	Yes	Yes	Yes	Yes
External Antennas	Yes	No	No	No	Yes
Internal Antennas	No	Yes	Yes	Yes	No
Antenna Switch	No	No	No	No	No
LED Locator	Yes	Yes	Yes	Yes	Yes
LED Suppression	Yes	Yes	Yes	Yes	Yes
Nebula Cloud Management	No	No	No	No	No
CAPWAP Managed AP Mode	Yes	Yes	Yes	Yes	Yes
AC (AP Controller) Discovery	Yes	Yes	Yes	Yes	Yes
802.11r Fast Roaming Support in Managed AP Mode	Yes	Yes	Yes	Yes	Yes
802.11k/v Assisted Roaming	Yes	Yes	Yes	Yes	Yes
Bluetooth Low Energy (BLE)	No	No	No	No	No
Maximum number of log messages	512 event logs or 1024 debug logs				

CHAPTER 2
Command Line Interface

This chapter describes how to access and use the CLI (Command Line Interface).

2.1 Overview

If you have problems with your NWA/WAC, customer support may request that you issue some of these commands to assist them in troubleshooting.

Use of undocumented commands or misconfiguration can damage the NWA/WAC and possibly render it unusable.

2.1.1 The Configuration File

When you configure the NWA/WAC using either the CLI (Command Line Interface) or the web configurator, the settings are saved as a series of commands in a configuration file on the NWA/WAC. You can store more than one configuration file on the NWA/WAC. However, only one configuration file is used at a time.

You can perform the following with a configuration file:

- Back up NWA/WAC configuration once the NWA/WAC is set up to work in your network.
- Restore NWA/WAC configuration.
- Save and edit a configuration file and upload it to multiple NWA/WACs in your network to have the same settings.

Note: You may also edit a configuration file using a text editor.

2.2 Accessing the CLI

You can access the CLI using a terminal emulation program on a computer connected to the console port, or access the NWA/WAC using Telnet or SSH (Secure SHell).

Note: The console port is not available in every model. Please check the User's Guide or datasheet, or refer to the product page at www.zyxel.com to see if your NWA/WAC has a console port.

Note: The NWA/WAC might force you to log out of your session if reauthentication time, lease time, or idle timeout is reached. See Chapter 8 on page 45 for more information about these settings.

2.2.1 Console Port

The default settings for the console port are as follows.

Table 5 Managing the NWA/WAC: Console Port

SETTING	VALUE
Speed	115200 bps
Data Bits	8
Parity	None
Stop Bit	1
Flow Control	Off

When you turn on your NWA/WAC, it performs several internal tests as well as line initialization. You can view the initialization information using the console port.

- Garbled text displays if your terminal emulation program's speed is set lower than the NWA/WAC's.
- No text displays if the speed is set higher than the NWA/WAC's.
- If changing your terminal emulation program's speed does not get anything to display, restart the NWA/WAC.
- If restarting the NWA/WAC does not get anything to display, contact your local customer support.

Figure 1 Console Port Power-on Display

```
FLASH: AMD 16M

BootModule Version: V1.13 | 06/25/2010 15:05:00
DRAM: Size = 256 Mbytes



DRAM POST: Testing: 262144K
```

After the initialization, the login screen displays.

Figure 2 Login Screen

```
Welcome to NWA3160-N

Username:
```

Enter the user name and password at the prompts.

Note: The default login username is **admin** and password is **1234**. The username and password are case-sensitive.

2.2.2 Telnet

Use the following steps to Telnet into your NWA/WAC.

1 If your computer is connected to the NWA/WAC over the Internet, skip to the next step. Make sure your computer IP address and the NWA/WAC IP address are on the same subnet.

2 In Windows, click **Start** (usually in the bottom left corner) and **Run**. Then type `telnet` and the NWA/WAC's IP address. For example, enter `telnet 192.168.1.2` (the default management IP address).

3 Click **OK**. A login screen displays. Enter the user name and password at the prompts.

Note: The default login username is **admin** and password is **1234**. The username and password are case-sensitive.

2.2.3 SSH (Secure SHell)

You can use an SSH client program to access the CLI. The following figure shows an example using a text-based SSH client program. Refer to the documentation that comes with your SSH program for information on using it.

Note: The default login username is **admin** and password is **1234**. The username and password are case-sensitive.

Figure 3 SSH Login Example

```
C:\>ssh2 admin@192.168.1.2
Host key not found from database.
Key fingerprint:
xolor-takel-fipef-zevit-visom-gydog-vetan-bisol-lysob-cuvun-muxex
You can get a public key's fingerprint by running
% ssh-keygen -F publickey.pub
on the keyfile.
Are you sure you want to continue connecting (yes/no)? yes

Host key saved to C:/Documents and Settings/user/Application Data/SSH/
hostkeys/
ey_22_192.168.1.2.pub
host key for 192.168.1.2, accepted by user Tue Aug 09 2005 07:38:28
admin's password:
Authentication successful.
```

2.3 How to Find Commands in this Guide

You can simply look for the feature chapter to find commands. In addition, you can use the List of Commands (Alphabetical) at the end of the guide. This section lists the commands in alphabetical order that they appear in this guide.

If you are looking at the CLI Reference Guide electronically, you might have additional options (for example, bookmarks or **Find...**) as well.

2.4 How Commands Are Explained

Each chapter explains the commands for one keyword. The chapters are divided into the following sections.

2.4.1 Background Information

Note: See the User's Guide for background information about most features.

This section provides background information about features that you cannot configure in the web configurator. In addition, this section identifies related commands in other chapters.

2.4.2 Command Input Values

This section lists common input values for the commands for the feature in one or more tables

2.4.3 Command Summary

This section lists the commands for the feature in one or more tables.

2.4.4 Command Examples

This section contains any examples for the commands in this feature.

2.4.5 Command Syntax

The following conventions are used in this User's Guide.

- A command or keyword in courier new must be entered literally as shown. Do not abbreviate.
- Values that you need to provide are in *italics*.
- Required fields that have multiple choices are enclosed in curly brackets {}.
- A range of numbers is enclosed in angle brackets <>.
- Optional fields are enclosed in square brackets [].
- The | symbol means OR.

2.4.6 Changing the Password

It is highly recommended that you change the password for accessing the NWA/WAC. See Section 8.2 on page 45 for the appropriate commands.

2.5 CLI Modes

You run CLI commands in one of several modes.

Table 6 CLI Modes

	USER	PRIVILEGE	CONFIGURATION	SUB-COMMAND
What **User** users can do	• Look at (but not run) available commands	Unable to access	Unable to access	Unable to access
What **Limited-Admin** users can do	• Look at system information (like **Status** screen) • Run basic diagnostics	• Look at system information (like **Status** screen) • Run basic diagnostics	Unable to access	Unable to access
What **Admin** users can do	• Look at system information (like **Status** screen) • Run basic diagnostics	• Look at system information (like **Status** screen) • Run basic diagnostics	• Configure simple features (such as an address object) • Create or remove complex parts (such as an interface)	• Configure complex parts (such as an interface) in the NWA/WAC
How you enter it	Log in to the NWA/WAC	Type **enable** in **User** mode	Type **configure terminal** in **User** or **Privilege** mode	Type the command used to create the specific part in **Configuration** mode

What the prompt looks like	`Router>`	`Router#`	`Router(config)#`	(varies by part)
				`Router(config-if-brg)#`
				`...`

How you exit it	Type **exit**	Type **disable**	Type **exit**	Type **exit**

See Chapter 8 on page 45 for more information about the user types. **User** users can only log in, look at (but not run) the available commands in **User** mode, and log out. **Limited-Admin** users can look at the configuration in the web configurator and CLI, and they can run basic diagnostics in the CLI. **Admin** users can configure the NWA/WAC in the web configurator or CLI.

At the time of writing, there is not much difference between **User** and **Privilege** mode for admin users. This is reserved for future use.

2.6 Shortcuts and Help

2.6.1 List of Available Commands

A list of valid commands can be found by typing ? or [TAB] at the command prompt. To view a list of available commands within a command group, enter <command> ? or <command> [TAB].

Figure 4 Help: Available Commands Example 1

```
Router> ?
<cr>
apply
atse
clear
configure
------------------[Snip]-------------------
shutdown
telnet
test
traceroute
wlan-report
write
Router>
```

Figure 5 Help: Available Command Example 2

```
Router> show ?
<wlan ap interface>
aaa
account
app-watch-dog
apply
arp-table
------------------[Snip]--------------------
wlan-security-profile
wlan-ssid-profile
wtp-logging
Router> show
```

2.6.2 List of Sub-commands or Required User Input

To view detailed help information for a command, enter <command> <sub command> ?.

Figure 6 Help: Sub-command Information Example

```
Router(config)# ip telnet server ?
;
<cr>
port
rule
|
Router(config)# ip telnet server
```

Figure 7 Help: Required User Input Example

```
Router(config)# ip telnet server port ?
<1..65535>
Router(config)# ip telnet server port
```

2.6.3 Entering Partial Commands

The CLI does not accept partial or incomplete commands. You may enter a unique part of a command and press [TAB] to have the NWA/WAC automatically display the full command.

For example, if you enter **config** and press [TAB] , the full command of **configure** automatically displays.

If you enter a partial command that is not unique and press [TAB], the NWA/WAC displays a list of commands that start with the partial command.

Figure 8 Non-Unique Partial Command Example

```
Router# c [TAB]
clear      configure  copy
Router# co [TAB]
configure  copy
```

2.6.4 Entering a ? in a Command

Typing a ? (question mark) usually displays help information. However, some commands allow you to input a ?, for example as part of a string. Press [CTRL+V] on your keyboard to enter a ? without the NWA/WAC treating it as a help query.

2.6.5 Command History

The NWA/WAC keeps a list of commands you have entered for the current CLI session. You can use any commands in the history again by pressing the up (↑) or down (↓) arrow key to scroll through the previously used commands and press [ENTER].

2.6.6 Navigation

Press [CTRL]+A to move the cursor to the beginning of the line. Press [CTRL]+E to move the cursor to the end of the line.

2.6.7 Erase Current Command

Press [CTRL]+U to erase whatever you have currently typed at the prompt (before pressing [ENTER]).

2.6.8 The no Commands

When entering the no commands described in this document, you may not need to type the whole command. For example, with the "[no] mss <536..1452>" command, you use "mss 536" to specify the MSS value. But to disable the MSS setting, you only need to type "no mss" instead of "no mss 536".

2.7 Input Values

You can use the ? or [TAB] to get more information about the next input value that is required for a command. In some cases, the next input value is a string whose length and allowable characters may

not be displayed in the screen. For example, in the following example, the next input value is a string called <description>.

```
Router# configure terminal
Router(config)# interface lan
Router(config-if-brg)# description ?
<description>
```

The following table provides more information about input values like <description>.

Table 7 Input-Value Formats for Strings in CLI Commands

TAG	# VALUES	LEGAL VALUES
*	1	*
all	--	ALL
authentication key	32-40 16-20	"0x" or "0X" + 32-40 hexadecimal values alphanumeric or ;|`~!@#$%^&*()_+\\{}':,./<>=-
	Used in MD5 authentication keys and text authentication key	
	0-16	alphanumeric or _-
	Used in text authentication keys	
	0-8	alphanumeric or _-
certificate name	1-31	alphanumeric or ;`~!@#$%^&()_+[\]{}',.=-
community string	0-63	alphanumeric or .- first character: alphanumeric or -
connection_id	1+	alphanumeric or -_:
contact	1-61	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-.
country code	0 or 2	alphanumeric
custom signature file name	0-30	alphanumeric or _-. first character: letter
description	Used in keyword criteria for log entries	
	1-64	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-.
	Used in other commands	
	1-61	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-
distinguished name	1-511	alphanumeric, spaces, or .@=,_-
domain name	0+	lower-case letters, numbers, or .-
	Used in ip dns server	
	1-248	alphanumeric or .- first character: alphanumeric or -
	Used in domainname, ip dhcp pool, and ip domain	
	1-255	alphanumeric or ._- first character: alphanumeric or -
email	1-63	alphanumeric or .@_-
e-mail	1-64	alphanumeric or .@_-
encryption key	16-64 8-32	"0x" or "0X" + 16-64 hexadecimal values alphanumeric or ;|`~!@#$%^&*()_+\\{}':,./ <>=-

Table 7 Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
file name	0-31	alphanumeric or _-
filter extension	1-256	alphanumeric, spaces, or '()+,/:=?;!*#@$_%.-
fqdn	Used in ip dns server	
	1-253	alphanumeric or .- first character: alphanumeric or -
	Used in ip, time server, device HA, certificates, and interface ping check	
	1-255	alphanumeric or .- first character: alphanumeric or -
full file name	0-256	alphanumeric or _/.-
hostname	Used in hostname command	
	1-64	alphanumeric or .-_ first character: alphanumeric or -
	Used in other commands	
	1-253	alphanumeric or .- first character: alphanumeric or -
import configuration file	1-26+".conf"	alphanumeric or ;`~!@#$%^&()_+[]{}',.=- add ".conf" at the end
import shell script	1-26+".zysh"	alphanumeric or ;`~!@#$%^&()_+[]{}',.=- add ".zysh" at the end
initial string	1-64	alphanumeric, spaces, or '()+,/:=!*#@$_%-.&
key length	--	512, 768, 1024, 1536, 2048
license key	25	"S-" + 6 upper-case letters or numbers + "-" + 16 upper-case letters or numbers
mac address	--	aa:bb:cc:dd:ee:ff (hexadecimal)
mail server fqdn		lower-case letters, numbers, or -.
name	1-31	alphanumeric or _-
notification message	1-81	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-
password: less than 15 chars	1-15	alphanumeric or `~!@#$%^&*()_\-+={}|\;:'<,>./
password: less than 8 chars	1-8	alphanumeric or ;/?:@&=+$\.-_!~*'()%,#$
password	Used in user and ip	
	1-63	alphanumeric or `~!@#$%^&*()_-+={}|\;:'<,>./
	Used in e-mail log profile SMTP authentication	
	1-63	alphanumeric or `~!@#$%^&*()_-+={}|\;:'<>./
	Used in device HA synchronization	
	1-63	alphanumeric or ~#%^*_-={}:,.
	Used in registration	
	6-20	alphanumeric or .@_-
phone number	1-20	numbers or ,+

Table 7 Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
preshared key	16-64	“0x” or “0X” + 16-64 hexadecimal values alphanumeric or ;|`~!@#$%^&*()_+\{}':,./<>=-
profile name	1-31	alphanumeric or _- first character: letters or _-
proto name	1-16	lower-case letters, numbers, or -
protocol name	1-31	alphanumeric or _- first character: letters or _-
quoted string less than 255 chars	1-255	alphanumeric, spaces, or ;/?:@&=+$\.- _!~*'()%,
quoted string less than 63 chars	1-63	alphanumeric, spaces, or ;/?:@&=+$\.-_!~*'()%
quoted string	0+	alphanumeric, spaces, or punctuation marks enclosed in double quotation marks (“) must put a backslash (\) before double quotation marks that are part of input value itself
realm	1-253	alphanumeric or -_ first character: alphanumeric or -_ used in domain authentication
service name	0-63	alphanumeric or -_@$./
spi	2-8	hexadecimal
string less than 15 chars	1-15	alphanumeric or -_
string: less than 63 chars	1-63	alphanumeric or `~!@#$%^&*()_-+={}|\;:'<,>./
string	1+	alphanumeric or -_@
subject	1-61	alphanumeric, spaces, or '()+,./:=?;!*#@$_%-
system type	0-2	hexadecimal
timezone [-+]*hh*	--	-12 through +12 (with or without “+”)
url	1-511	alphanumeric or '()+,/:.=?;!*#@$_%-
url	“http://”+ “https://”+	alphanumeric or ;/?:@&=+$\.-_!~*'()%, starts with “http://” or “https://” may contain one pound sign (#)
user name	1-31	alphanumeric or _- first character: letters or _-
username	1-31	alphanumeric or _- first character: alphanumeric or _- domain authorization
username	6-20	alphanumeric or .@_- registration
user name	1+	alphanumeric or -_. logging commands
user@domainname	1-80	alphanumeric or .@_-
vrrp group name: less than 15 chars	1-15	alphanumeric or _-

Table 7 Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
week-day sequence, i.e. 1=first,2=second	1	1-4
xauth method	1-31	alphanumeric or _-
xauth password	1-31	alphanumeric or ;|`~!@#$%^&*()_+\{}':,./<>=-
mac address	0-12 (even number)	hexadecimal for example: xx-xx-xx-xx-xx-xx

2.8 Saving Configuration Changes

Use the `write` command to save the current configuration to the NWA/WAC.

Note: Always save the changes before you log out after each management session. All unsaved changes will be lost after the system restarts.

2.9 Logging Out

Enter the `exit` or end command in configure mode to go to privilege mode.

Enter the `exit` command in user mode or privilege mode to log out of the CLI.

CHAPTER 3
User and Privilege Modes

This chapter describes how to use these two modes.

3.1 User And Privilege Modes

This is the mode you are in when you first log into the CLI. (Do not confuse 'user mode' with types of user accounts the NWA/WAC uses. See Chapter 8 on page 45 for more information about the user types. 'User' type accounts can only run 'exit' in this mode. However, they may need to log into the device in order to be authenticated for 'user-aware' policies, for example a firewall rule that a particular user is exempt from.)

Type 'enable' to go to 'privilege mode'. No password is required. All commands can be run from here except those marked with an asterisk. Many of these commands are for trouble-shooting purposes, for example the htm (hardware test module) and debug commands. Customer support may ask you to run some of these commands and send the results if you need assistance troubleshooting your device.

For admin logins, all commands are visible in 'user mode' but not all can be run there. The following table displays which commands can be run in 'user mode'. All commands can be run in 'privilege mode'.

The `htm` and `psm` commands are for Zyxel's internal manufacturing process.

Table 8 User (U) and Privilege (P) Mode Commands

COMMAND	MODE	DESCRIPTION
`apply`	P	Applies a configuration file.
`atse`	U/P	Displays the seed code
`clear`	U/P	Clears system or debug logs or DHCP binding.
`configure`	U/P	Use 'configure terminal' to enter configuration mode.
`copy`	P	Copies configuration files.
`daily-report`	U/P	Sets how and where to send daily reports and what reports to send.
`debug (*)`	U/P	For support personnel only! The device needs to have the debug flag enabled.
`delete`	P	Deletes configuration files.
`details`	P	Performs diagnostic commands.
`diag`	P	Provided for support personnel to collect internal system information. It is not recommended that you use these.
`diag-info`	P	Has the NWA/WAC create a new diagnostic file.
`dir`	P	Lists files in a directory.
`disable`	U/P	Goes from privilege mode to user mode

Table 8 User (U) and Privilege (P) Mode Commands (continued)

COMMAND	MODE	DESCRIPTION
enable	U/P	Goes from user mode to privilege mode
exit	U/P	Goes to a previous mode or logs out.
htm	U/P	Goes to htm (hardware test module) mode for testing hardware components. You may need to use the htm commands if your customer support Engineer asks you to during troubleshooting. Note: These commands are for Zyxel's internal manufacturing process.
interface	U/P	Dials or disconnects an interface.
no packet-trace	U/P	Turns off packet tracing.
nslookup	U/P	Resolves an IP address to a host name and vice-versa.
packet-trace	U/P	Performs a packet trace.
ping	U/P	Pings an IP address or host name.
psm	U/P	Goes to psm (product support module) mode for setting product parameters. You may need to use the htm commands if your customer support Engineer asks you to during troubleshooting. Note: These commands are for Zyxel's internal manufacturing process.
reboot	P	Restarts the device.
release	P	Releases DHCP information from an interface.
rename	P	Renames a configuration file.
renew	P	Renews DHCP information for an interface.
run	P	Runs a script.
setenv	U/P	Turns stop-on-error on (terminates booting if an error is found in a configuration file) or off (ignores configuration file errors and continues booting).
show	U/P	Displays command statistics. See the associated command chapter in this guide.
shutdown	P	Writes all d data to disk and stops the system processes. It does not turn off the power.
telnet	U/P	Establishes a connection to the TCP port number 23 of the specified host name or IP address.
test aaa	U/P	Tests whether the specified user name can be successfully authenticated by an external authentication server.
traceroute	P	Traces the route to the specified host name or IP address.
write	P	Saves the current configuration to the NWA/WAC. All unsaved changes are lost after the NWA/WAC restarts.

Subsequent chapters in this guide describe the configuration commands. User/privilege mode commands that are also configuration commands (for example, 'show') are described in more detail in the related configuration command chapter.

3.1.1 Debug Commands

Debug commands marked with an asterisk (*) are not available when the debug flag is on and are for Zyxel service personnel use only. The debug commands follow a syntax that is Linux-based, so if there is a

Linux equivalent, it is displayed in this chapter for your reference. You must know a command listed here well before you use it. Otherwise, it may cause undesired results.

Table 9 Debug Commands

COMMAND SYNTAX	DESCRIPTION	LINUX COMMAND EQUIVALENT
debug app show l7protocol (*)	Shows app patrol protocol list	> cat /etc/l7_protocols/ protocol.list
debug ca (*)	Certificate debug commands	
debug device-ha (*)	Device HA debug commands	
debug gui (*)	Web Configurator related debug commands	
debug hardware (*)	Hardware debug commands	
debug interface	Interface debug commands	
debug interface ifconfig	Shows system interfaces detail	> ifconfig [interface]
debug ip dns	DNS debug commands	
debug logging	System logging debug commands	
debug manufacture	Manufacturing related debug commands	
debug network arpignore (*)	Enable/Display the ignoring of ARP responses for interfaces which don't own the IP address	cat /proc/sys/net/ipv4/ conf/*/arp_ignore
debug policy-route (*)	Policy route debug command	
debug [cmdexec|corefile|ip |kernel|mac-id-rewrite|observer|switch |system|zyinetpkt] (*)	ZLD internal debug commands	

PART II
Reference

CHAPTER 4
Object Reference

This chapter describes how to use object reference commands.

4.1 Object Reference Commands

The object reference commands are used to see which configuration settings reference a specific object. You can use this table when you want to delete an object because you have to remove references to the object first.

Table 10 show reference Commands

COMMAND	DESCRIPTION
show reference object username [*username*]	Displays which configuration settings reference the specified user object.
show reference object aaa authentication [default | *profile*]	Displays which configuration settings reference the specified AAA authentication object.
show reference object ca category {local|remote} [*cert_name*]	Displays which configuration settings reference the specified authentication method object.
show reference object [*wlan-radio-profile*]	Displays the specified radio profile object.
show reference object [*wlan-monitor-profile*]	Displays the specified monitor profile object.
show reference object [*wlan-ssid-profile*]	Displays the specified SSID profile object.
show reference object [*wlan-security-profile*]	Displays the specified security profile object.
show reference object [*wlan-macfilter-profile*]	Displays the specified macfilter profile object.

4.1.1 Object Reference Command Example

This example shows the names of the WLAN profiles and which security profile each is set to use.

```
Router(config)# show reference object aaa authentication

default References:
Category
Rule Priority        Rule Name
Description
================================================================================
WLAN Profile SECURITY
1                    default
N/A
WWW
N/A                  N/A
N/A
```

CHAPTER 5
Status

This chapter explains some commands you can use to display information about the NWA/WAC's current operational state.

Table 11 Status Show Commands

COMMAND	DESCRIPTION
show boot status	Displays details about the NWA/WAC's startup state.
show cpu status	Displays the CPU utilization.
show disk	Displays the disk utilization.
show extension-slot	Displays the status of the extension card slot and the USB ports and the names of any connected devices.
show led status	Displays the status of each LED on the NWA/WAC.
show mac	Displays the NWA/WAC's MAC address.
show mem status	Displays what percentage of the NWA/WAC's memory is currently being used.
show power mode	Displays the NWA/WAC's power status. **Full** - the NWA/WAC receives power using a power adaptor and/or through a PoE switch/injector using IEEE 802.3at PoE plus. **Limited** - the NWA/WAC receives power through a PoE switch/injector using IEEE 802.3af PoE even when it is also connected to a power source using a power adaptor. When the NWA/WAC is in limited power mode, the NWA/WAC throughput decreases and has just one transmitting radio chain. It always shows **Full** if the NWA/WAC does not support power detection.
show ram-size	Displays the size of the NWA/WAC's on-board RAM.
show serial-number	Displays the serial number of this NWA/WAC.
show socket listen	Displays the NWA/WAC's listening ports
show socket open	Displays the ports that are open on the NWA/WAC.
show system uptime	Displays how long the NWA/WAC has been running since it last restarted or was turned on.
show version	Displays the NWA/WAC's model, firmware and build information.

Here are examples of the commands that display the CPU and disk utilization.

```
Router# show cpu status
CPU utilization: 0 %
CPU utilization for 1 min: 0 %
CPU utilization for 5 min: 0 %
Router# show disk
No. Disk                Size(MB)        Usage
================================================================================
1   image               65              82%
2   onboard flash       154             36%
```

Here are examples of the commands that display the MAC address, memory usage, RAM size, and serial number.

```
Router(config)# show mac
MAC address: 40:4A:03:42:70:16-40:4A:03:42:70:17
Router(config)# show mem status
memory usage: 19%
Router(config)# show ram-size
ram size: 256MB
Router(config)# show serial-number
serial number: S100D42007115
```

Here is an example of the command that displays the listening ports.

```
Router(config)# show socket listen
No.   Proto Local_Address         Foreign_Address       State
==========================================================================
1     tcp   0.0.0.0:80            0.0.0.0:0             LISTEN
2     tcp   192.168.1.245:53      0.0.0.0:0             LISTEN
3     tcp   127.0.0.1:53          0.0.0.0:0             LISTEN
4     tcp   0.0.0.0:21            0.0.0.0:0             LISTEN
5     tcp   0.0.0.0:22            0.0.0.0:0             LISTEN
6     tcp   127.0.0.1:953         0.0.0.0:0             LISTEN
```

Here is an example of the command that displays the open ports.

```
Router(config)# show socket open
No.   Proto Local_Address         Foreign_Address       State
==========================================================================
1     udp   0.0.0.0:1812          0.0.0.0:0
2     udp   0.0.0.0:1814          0.0.0.0:0
3     udp   0.0.0.0:161           0.0.0.0:0
4     udp   172.23.26.245:53      0.0.0.0:0
5     0.0.1:53          0.0.0.0:0
6     udp   0.0.0.0:43386         0.0.0.0:0
7     udp   0.0.0.0:5246          0.0.0.0:0
```

Here are examples of the commands that display the system uptime and model, firmware, and build information.

```
Router> show system uptime
system uptime: 04:18:00
Router> show version
Zyxel Communications Corp.
model           : NWA3160-N
firmware version: 2.23(UJA.0)b2
BM version      : 1.13
build date      : 2010-12-21 09:10:11
```

This example shows the current LED states on the NWA/WAC. The **SYS** LED lights on and green.

```
Router> show led status
sys: green
Router>
```

CHAPTER 6
Interfaces

This chapter shows you how to use interface-related commands.

6.1 Interface Overview

In general, an interface has the following characteristics.

- An interface is a logical entity through which (layer-3) packets pass.
- An interface is bound to a physical port or another interface.
- Many interfaces can share the same physical port.

Some characteristics do not apply to some types of interfaces.

6.2 Interface General Commands Summary

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 12 Input Values for General Interface Commands

LABEL	DESCRIPTION
interface_name	The name of the interface. Ethernet interface: ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your NWA/WAC model. VLAN interface: vlan*x*, *x* = 0 - 511
domain_name	Fully-qualified domain name. You may up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.

The following sections introduce commands that are supported by several types of interfaces.

6.2.1 Basic Interface Properties and IP Address Commands

This table lists basic properties and IP address commands.

Table 13 interface General Commands: Basic Properties and IP Address Assignment

COMMAND	DESCRIPTION
capwap ap vlan vlan-id <*1..4094*> <tag|untag>	When the NWA/WAC is in managed AP mode, this sets the AP's VLAN identification number and sets it to send tagged or untagged packets.
interface-name {*bridge_interface*} *user_defined_name*	Specifies a name for a bridge interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long. *ethernet_interface*: This must be the system name of a bridge interface. Use the show interface-name command to see the system name of interfaces. *user_defined_name*: • This name cannot be one of the follows: "ethernet", "ppp", "vlan", "bridge", "virtual", "wlan", "cellular", "aux", "tunnel", "status", "summary", "all" • This name cannot begin with one of the follows either: "ge", "ppp", "vlan", "wlan-", "br", "cellular", "aux", "tunnel".
interface-rename *old_user_defined_name new_user_defined_name*	Modifies the user-defined name of an Ethernet interface.
interface send statistics interval <15..3600>	Sets how often the NWA/WAC sends interface statistics to external servers. For example, a syslog server.
[no] interface *interface_name*	Creates the specified interface if necessary and enters sub-command mode. The no command deletes the specified interface.
[no] description *description*	Specifies the description for the specified interface. The no command clears the description. *description*: You can use alphanumeric and ()+/ :=?!*#@$_%- characters, and it can be up to 60 characters long.
[no] downstream <0..1048576>	This is reserved for future use. Specifies the downstream bandwidth for the specified interface. The no command sets the downstream bandwidth to 1048576.
exit	Leaves the sub-command mode.
[no] ip address dhcp	Makes the specified interface a DHCP client; the DHCP server gives the specified interface its IP address, subnet mask, and gateway. The no command makes the IP address static IP address for the specified interface. (See the next command to set this IP address.)
[no] ip address *ip subnet_mask*	Assigns the specified IP address and subnet mask to the specified interface. The no command clears the IP address and the subnet mask.
[no] ip gateway *ip*	Adds the specified gateway using the specified interface. The no command removes the gateway.
ip gateway *ip* metric <0..15>	Sets the priority (relative to every gateway on every interface) for the specified gateway. The lower the number, the higher the priority.

Table 13 interface General Commands: Basic Properties and IP Address Assignment (continued)

COMMAND	DESCRIPTION
[no] metric <0..15>	Sets the interface's priority relative to other interfaces. The lower the number, the higher the priority.
[no] mss <536..1460>	Specifies the maximum segment size (MSS) the interface is to use. MSS is the largest amount of data, specified in bytes, that the interface can handle in a single, unfragmented piece. The no command has the interface use its default MSS.
[no] mtu <576..1500>	Specifies the Maximum Transmission Unit, which is the maximum number of bytes in each packet moving through this interface. The NWA/WAC divides larger packets into smaller fragments. The no command resets the MTU to 1500.
[no] shutdown	Deactivates the specified interface. The no command activates it.
traffic-prioritize {tcp-ack|dns} bandwidth <0..1048576> priority <1..7> [maximize-bandwidth-usage];	Applies traffic priority when the interface sends TCP-ACK traffic, or traffic for resolving domain names. It also sets how much bandwidth the traffic can use and can turn on maximize bandwidth usage.
traffic-prioritize {tcp-ack|dns} deactivate	Turns off traffic priority settings for when the interface sends the specified type of traffic.
[no] upstream <0..1048576>	Specifies the upstream bandwidth for the specified interface. The no command sets the upstream bandwidth to 1048576.
manager ap vlan vlan-id *<1..4094>* <tag|untag>	When the NWA/WAC is in standalone or cloud management mode, this sets the AP's VLAN identification number and sets it to send tagged or untagged packets.
manager ap vlan ip address [*ip subnet_mask* | dhcp]	Sets the management IPv4 address for the NWA/WAC.
manager ap vlan [no] ipv6 address *ipv6_addr/prefix*	Sets the IPv6 address and the prefix length for the LAN interface of the NWA/WAC. The no command removes the IPv6 address settings.
manager ap vlan [no] ipv6 dhcp6 {address-request | client}	Set the NWA/WAC to act as a DHCPv6 client or get this interface's IPv6 address from a DHCPv6 server. The no command sets the NWA/WAC to not get this interface's IPv6 address from the DHCPv6 server.
manager ap vlan [no] ipv6 dhcp6-request-object *dhcp6_profile*	For a DHCPv6 client interface, sets the profile of DHCPv6 request settings that determine what additional information to get from the DHCPv6 server. The no command removes the DHCPv6 request settings profile.
manager ap vlan [no] ipv6 enable	Enables IPv6 stateless auto-configuration on the NWA/WAC. The NWA/WAC will generate an IPv6 address itself from a prefix obtained from an IPv6 router in the network. The no command disables IPv6 stateless auto-configuration.
manager ap vlan [no] ipv6 gateway *ipv6_addr*	Sets the IPv6 address of the default outgoing gateway. The no command removes the IPv6 gateway settings.
manager ap vlan [no] ipv6 nd ra accept	Sets the IPv6 interface to accept IPv6 neighbor discovery router advertisement messages. The no command sets the IPv6 interface to discard IPv6 neighbor discovery router advertisement messages.
manager ap vlan [no] ip gateway *ip*	Sets the manager gateway address. The no command removes the gateway.

Table 13 interface General Commands: Basic Properties and IP Address Assignment (continued)

COMMAND	DESCRIPTION
show interface {ethernet | vlan} status	Displays the connection status of the specified type of interfaces.
show interface {*interface_name* | ethernet | vlan | all}	Displays information about the specified interface, specified type of interfaces, or all interfaces.
show interface send statistics interval	Displays the interval for how often the NWA/WAC refreshes the sent packet statistics for the interfaces.
show interface summary all	Displays basic information about the interfaces.
show interface summary all status	Displays the connection status of the interfaces.
show interface-name	Displays all Ethernet interface system name and user-defined name mappings.
show ipv6 interface {*interface_name* | bridge | vlan | ethernet | all}	Displays information about the specified IPv6 interface, specified type of IPv6 interfaces, or all IPv6 interfaces.
show ipv6 nd ra status *interface_name*	Displays the specified IPv6 interface's IPv6 router advertisement configuration.
show ipv6 static address interface *interface_name*	Displays the static IPv6 addresses configured on the specified IPv6 interface.

6.2.1.1 Basic Interface Properties Command Examples

Use these commands to set LAN settings. Use **manager ap vlan ip address** to set the LAN interface to use a static IP address or DHCP. If you set an attribute twice, the latter setting overrides the previous one.

The following commands configure the LAN Ethernet interface to use IP address 1.1.1.1, netmask 255.255.255.0, and gateway address 1.2.3.4.

```
Router(config)# manager ap vlan ip address 1.1.1.1 255.255.255.0
Router(config)# manager ap vlan ip gateway 1.2.3.4
```

The following command makes the LAN Ethernet interface a DHCP client.

```
Router(config)# manager ap vlan ip address dhcp
```

This example sets the LAN Ethernet interface's management VLAN Id to 100, untagged.

```
Router(config)# manager ap vlan vlan-id 100 untag
```

6.3 Port Commands

This section covers commands that are specific to ports.

Note: In CLI, representative interfaces are also called representative ports.

Table 14 Basic Interface Setting Commands

COMMAND	DESCRIPTION
no port <1..*x*>	Removes the specified physical port from its current representative interface and adds it to its default representative interface (for example, port *x* --> ge*x*).
port status Port<1..*x*>	Enters a sub-command mode to configure the specified port's settings.
[no] duplex <full | half>	Sets the port's duplex mode. The no command returns the default setting.
exit	Leaves the sub-command mode.
[no] negotiation auto	Sets the port to use auto-negotiation to determine the port speed and duplex. The no command turns off auto-negotiation.
[no] speed <100,10>	Sets the Ethernet port's connection speed in Mbps. The no command returns the default setting.
show port setting	Displays the Ethernet port negotiation, duplex, and speed settings.
show port status	Displays statistics for the Ethernet ports.
show port type	Displays the type of cable connection for each physical interface on the device.
show manager vlan	Displays the LAN interface's management interface settings.

6.3.1 Port Command Examples

The following example shows port status.

```
Router# show port status
Port Status    TxPkts    RxPkts    TxBcast    RxBcast    Colli.  TxB/s
RxB/s      Up Time      PVID
================================================================================
====
1    1000M/Full 465       5452       411        2647       0       812
612        00:13:28     1
2    Down      0         0         0         0         0      0         0
00:00:00     1
3    Down      0         0         0         0         0      0         0
00:00:00     1
4    Down      0         0         0         0         0      0         0
00:00:00     1
Router#
```

The following example shows port settings.

```
Router(config)# show port setting
Port Negotiation Duplex Speed EEE
================================================================================
====
1    auto        full   1000  no
```

The following example shows LAN settings.

```
Router(config)# show manager vlan
Management Interface:
        VLAN ID: 100
        VLAN Tag: untag
        IP Status: static
        IP Address: 192.168.1.2
        Mask: 255.255.255.0
        Gateway: 0.0.0.0
```

The following example shows each port's type of cable connection.

```
Router(config)# show port type
Port Type
================================================================================
1    Copper
```

CHAPTER 7
NCC Discovery

This chapter shows you how to configure the NCC discovery and proxy server settings on the NWA/WAC.

7.1 Overview

If your NWA/WAC can be managed through the Zyxel Nebula Control Center (NCC) and is behind a proxy server, you will need to enable NCC discovery and configure the proxy server settings so that the NWA/WAC can access the NCC through the proxy server.

7.2 NCC Discovery Commands

The following table describes the commands available for NCC discovery and proxy server. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 15 Command Summary: NCC Discovery

COMMAND	DESCRIPTION
`[no] netconf inactivate`	Turns off NCC discovery on the NWA/WAC. If NCC discovery is disabled, the NWA/WAC will not discover the NCC and remain in standalone AP mode. The `no` command turns on NCC discovery. The NWA/WAC will try to discover the NCC and go into cloud management mode when it is connected to the Internet and has been registered in the NCC.
`[no] netconf proxy`	Sets the NWA/WAC to access the NCC through the specified proxy server. The `no` command sets the NWA/WAC to not access the NCC through the specified proxy server.
`netconf proxy server {`*`ip`*`|`*`host_name`*`}`	Sets the IP address or URL of the proxy server.
`netconf proxy port <1..65535>`	Sets the service port number used by the proxy server.
`[no] netconf proxy-auth`	Turns on proxy authentication. The `no` command turns it off. Enable this if the proxy server requires authentication before it grants access to the Internet.
`netconf proxy-auth username` *`username`* `{password|encrypted-password} {`*`password`*`|`*`ciphertext`*`}`	Sets your proxy user name and password.
`show netconf proxy status`	Displays the proxy server settings.
`show netconf status`	Displays whether NCC discovery is enabled or not on the NWA/WAC.

7.2.1 NCC Discovery Command Example

The following example shows you how to turn on NCC discover on the NWA/WAC.

```
Router# configure terminal
Router(config)# no netconf inactivate
Router(config)#
```

The following example shows proxy server settings.

```
Router> show netconf proxy status
        active: yes
        proxy server: 172.16.15.253
        proxy port: 8080
        proxy-auth active: yes
        proxy-auth username: Joseph
        proxy-auth encrypted-password: $4$hT65kQTR$Uh8lp5zfcP7vEfm
O97C5MJ6U1B47M3DIiPvb6GcrPK2kEo3R7PTChiVWl7rRi+xr0xhg8DsdTPU$
Router>
```

CHAPTER 8
Users

This chapter describes how to set up user accounts and user settings for the NWA/WAC. You can also set up rules that control when users have to log in to the NWA/WAC before the NWA/WAC routes traffic for them.

8.1 User Account Overview

A user account defines the privileges of a user logged into the NWA/WAC. User accounts are used in firewall rules and application patrol, in addition to controlling access to configuration and services in the NWA/WAC.

8.1.1 User Types

These are the types of user accounts the NWA/WAC uses.

Table 16 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
admin	Change NWA/WAC configuration (web, CLI)	WWW, TELNET, SSH, FTP, Console,
limited-admin	Look at NWA/WAC configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH, Console
Access Users		
user	Used for the embedded RADIUS server and SNMPv3 user access Browse user-mode commands (CLI)	

8.2 User Commands Summary

The following table identify the values required for many `username` commands. Other input values are discussed with the corresponding commands.

Table 17 user Command Input Values

LABEL	DESCRIPTION
username	The name of the user (account). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following sections list the `username` commands.

8.2.1 Username and User Commands

The first table lists the commands for users.

Table 18 username Commands Summary: Users

COMMAND	DESCRIPTION
show username [*username*]	Displays information about the specified user or about all users set up in the NWA/WAC.
username *username* nopassword user-type {admin | guest | limited-admin | user}	Creates the specified user (if necessary), disables the password, and sets the user type for the specified user.
username *username* password *password* user-type {admin | guest | limited-admin | user}	Creates the specified user (if necessary); enables and sets the password; and sets the user type for the specified user. *password*: You can use 1-63 printable ASCII characters, except double quotation marks (“) and question marks (?).
username *username* encrypted-password <*ciphertext*> user-type {admin | guest | limited-admin | user}	Sets a user account password by ciphertext.
username *username* user-type ext-group-user	Creates the specified user (if necessary) and sets the user type to **Ext-User**.
no username *username*	Deletes the specified user.
username rename *username username*	Renames the specified user (first *username*) to the specified username (second *username*).
username *username* [no] description *description*	Sets the description for the specified user. The no command clears the description. *description*: You can use alphanumeric and ()+/ :=?!*#@$_%- characters, and it can be up to 60 characters long.
username *username* encrypted-password <*password*>	Sets a user account password by ciphertext. Normally you would use username password <*clear text*> to set the password. In special case cases (for GUI apply), you can use username encrypted-password <*ciphertext*> to set password.
username *username* logon-time-setting <default | manual>	Sets the account to use the factory default lease and reauthentication times or custom ones.
username *username* [no] logon-lease-time <0..1440>	Sets the lease time for the specified user. Set it to zero to set unlimited lease time. The no command sets the lease time to five minutes (regardless of the current default setting for new users).
username *username* [no] logon-re-auth-time <0..1440>	Sets the reauthorization time for the specified user. Set it to zero to set unlimited reauthorization time. The no command sets the reauthorization time to thirty minutes (regardless of the current default setting for new users).

8.2.2 User Setting Commands

This table lists the commands for user settings.

Table 19 users Commands Summary: Settings

COMMAND	DESCRIPTION
show users default-setting {all | user-type {admin | limited-admin}}	Displays the default lease and reauthentication times for the specified type of user accounts.
users default-setting [no] logon-lease-time <0..1440>	Sets the default lease time (in minutes) for each new user. Set it to zero to set unlimited lease time. The no command sets the default lease time to five.
users default-setting [no] logon-re-auth-time <0..1440>	Sets the default reauthorization time (in minutes) for each new user. Set it to zero to set unlimited reauthorization time. The no command sets the default reauthorization time to thirty.
users default-setting [no] user-type <admin |limited-admin>	Sets the default user type for each new user. The no command sets the default user type to user.
show users retry-settings	Displays the current retry limit settings for users.
[no] users retry-limit	Enables the retry limit for users. The no command disables the retry limit.
[no] users retry-count <1..99>	Sets the number of failed login attempts a user can have before the account or IP address is locked out for lockout-period minutes. The no command sets the retry-count to five.
[no] users lockout-period <1..65535>	Sets the amount of time, in minutes, a user or IP address is locked out after retry-count number of failed login attempts. The no command sets the lockout period to thirty minutes.
show users simultaneous-logon-settings	Displays the current settings for simultaneous logins by users.
[no] users simultaneous-logon {administration | access} enforce	Enables the limit on the number of simultaneous logins by users of the specified account-type. The no command disables the limit, or allows an unlimited number of simultaneous logins.
[no] users simultaneous-logon {administration | access} limit <1..1024>	Sets the limit for the number of simultaneous logins by users of the specified account-type. The no command sets the limit to one.

8.2.2.1 User Setting Command Examples

The following commands show the current settings for the number of simultaneous logins.

```
Router# configure terminal
Router(config)# show users simultaneous-logon-settings
enable simultaneous logon limitation for administration account: no
maximum simultaneous logon per administration account          : 1
```

8.2.3 Additional User Commands

This table lists additional commands for users.

Table 20 users Commands Summary: Additional

COMMAND	DESCRIPTION
show users {*username* | all | current}	Displays information about the users logged onto the system.
show lockout-users	Displays users who are currently locked out.
unlock lockout-users *ip* | console	Unlocks the specified IP address.
users force-logout *ip* | *username*	Logs out the specified logins.

8.2.3.1 Additional User Command Examples

The following commands display the users that are currently logged in to the NWA/WAC and forces the logout of all logins from a specific IP address.

```
Router# configure terminal
outer(config)# show users all
No.  Name                 Type       From
     Service    Session Time Idle Time    Lease Timeout Re-Auth. Timeout
==============================================================================
1    admin                admin      172.17.16.101
     http/https 04:31:01     unlimited    unlimited     unlimited
2    admin                admin      console
     console    04:23:51     unlimited    unlimited     unlimited
Router(config)# users force-logout 172.17.16.101
Logout user 'admin'(from 172.17.16.101): OK
Total 1 user has been forced logout
Router(config)# show users all
No.  Name                 Type       From
     Service    Session Time Idle Time    Lease Timeout Re-Auth. Timeout
==============================================================================
1    admin                admin      console
     console    04:24:55     unlimited    unlimited     unlimited
```

The following commands display the users that are currently locked out and then unlocks the user who is displayed.

```
Router# configure terminal
Router(config)# show lockout-users
No.  Username Tried                  From            Lockout Time Remaining
================================================================================
No.  From            Failed Login Attempt    Record Expired Timer
================================================================================
1    172.17.13.60    2                       46

Router(config)# unlock lockout-users 172.17.13.60
User from 172.17.13.60 is unlocked
Router(config)# show lockout-users
No.  Username Tried                  From            Lockout Time Remaining
================================================================================
No.  From            Failed Login Attempt    Record Expired Timer
================================================================================
```

CHAPTER 9
AP Management

This chapter shows you how to configure wireless AP management options on your NWA/WAC.

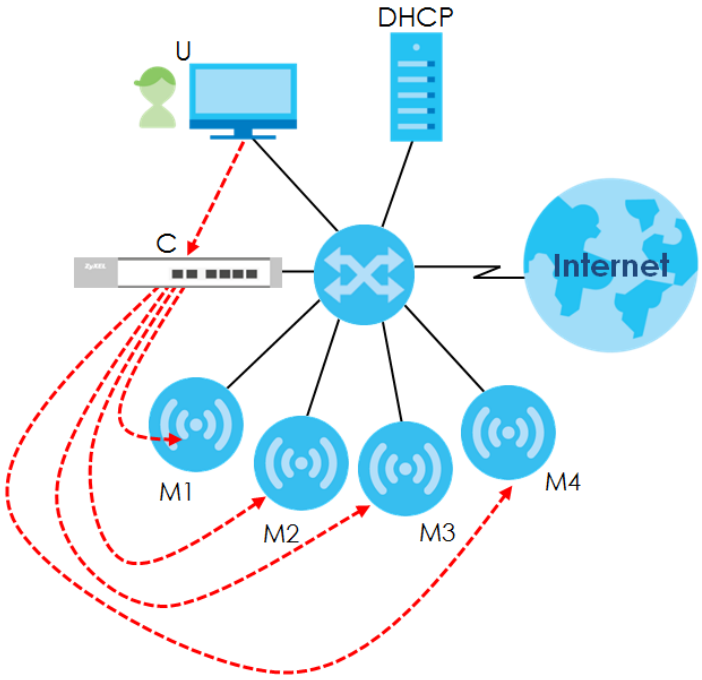
9.1 AP Management Overview

The NWA/WAC supports CAPWAP. This is Zyxel's implementation of the CAPWAP protocol (RFC 5415). The CAPWAP data flow is protected by Datagram Transport Layer Security (DTLS).

The NWA/WAC can be a standalone AP (default), or a CAPWAP managed AP.

The following figure illustrates a CAPWAP wireless network. The user (**U**) configures the AP controller (**C**), which then automatically updates the configurations of the managed APs (**M1** ~ **M4**).

Figure 9 CAPWAP Network Example



CAPWAP Discovery and Management

The link between CAPWAP-enabled access points proceeds as follows:

1 An AP in managed AP mode joins a wired network (receives a dynamic IP address).

2 The AP sends out a discovery request, looking for a CAPWAP AP controller.

3 If there is an AP controller on the network, it receives the discovery request. If the AP controller is in **Manual** mode it adds the details of the AP to its **Unmanaged Access Points** list, and you decide which available APs to manage. If the AP controller is in **Always Accept** mode, it automatically adds the AP to its **Managed Access Points** list and provides the managed AP with default configuration information, as well as securely transmitting the DTLS pre-shared key. The managed AP is ready for association with wireless clients.

Managed AP Finds the Controller

A managed NWA/WAC can find the controller in one of the following ways:

- Manually specify the controller's IP address in the Web Configurator's **AC** (AP Controller) **Discovery** screen or using the `capwap ap ac-ip` command.
- Get the controller's IP address from a DHCP server with the controller's IP address configured as option 138.
- Get the controller's IP address from a DNS server SRV (Service) record.
- Broadcasting to discover the controller within the broadcast domain.

Note: The AP controller needs to have a static IP address. If it is a DHCP client, set the DHCP server to reserve an IP address for the AP controller.

CAPWAP and IP Subnets

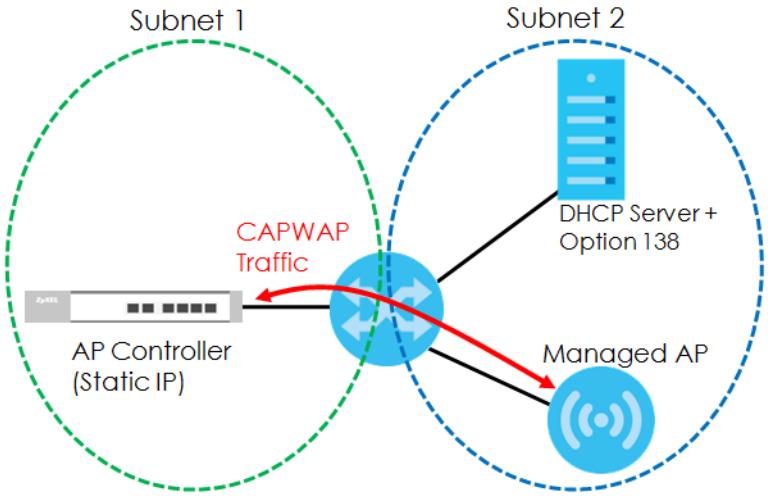
By default, CAPWAP works only between devices with IP addresses in the same subnet.

However, you can configure CAPWAP to operate between devices with IP addresses in different subnets by doing the following.

- Activate DHCP. Your network's DHCP server must support option 138 defined in RFC 5415.
- Configure DHCP option 138 with the IP address of the CAPWAP AP controller on your network.

DHCP Option 138 allows the CAPWAP management request (from the AP in managed AP mode) to reach the AP controller in a different subnet, as shown in the following figure.

Figure 10 CAPWAP and DHCP Option 138



Notes on CAPWAP

This section lists some additional features of Zyxel's implementation of the CAPWAP protocol.

- When the AP controller uses its internal Remote Authentication Dial In User Service (RADIUS) server, managed APs also use the AP controller's authentication server to authenticate wireless clients.
- If a managed AP's link to the AP controller is broken, the managed AP continues to use the wireless settings with which it was last provided.

9.2 AP Management Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 21 Input Values for General AP Management Commands

LABEL	DESCRIPTION
ap_mac	The Ethernet MAC address of the managed AP. Enter 6 hexadecimal pairs separated by colons. You can use 0-9, a-z and A-Z.
slot_name	The slot name for the AP's on-board wireless LAN card. Use either *slot1* or *slot2*. (Not all NWA/WACs support 2 radio slots.)
profile_name	The wireless LAN radio profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
ap_description	The AP description. This is strictly used for reference purposes and has no effect on any other settings. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
sta_mac	The Ethernet MAC address of the managed station (or wireless client). Enter 6 hexadecimal pairs separated by colons. You can use 0-9, a-z and A-Z.

The following table describes the commands available for AP management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 22 Command Summary: AP Management

COMMAND	DESCRIPTION
`wlan` *slot_name*	Enters the sub-command mode for the specified radio on the NWA/WAC.
`[no] activate`	Enables the specified radio. The no command disables the radio.
`ap profile` *radio_profile_name*	Sets the radio (*slot_name*) to AP mode and assigns a created radio profile to the radio.
`output-power` *power*	Sets the output power (between 0 to 30 dBm) for the specified radio.
`repeater profile` *radio_profile_name*	Sets the specified radio (*slot_name*) to repeater mode and assigns a created radio profile to the radio.
`rootap profile` *radio_profile_name*	Sets the specified radio (*slot_name*) to root AP mode and assigns a created radio profile to the radio.
`ssid profile index` *ssid_profile_name*	Assigns an SSID profile to this radio. Requires an existing SSID profile.
`wds_profile` *wds_profile_name*	Selects the WDS profile the radio (in repeater or root AP mode) uses to connect to a root AP or repeater.

Table 22 Command Summary: AP Management (continued)

COMMAND	DESCRIPTION
wds_uplink {auto | manual bssid *mac_address*}	Sets how the radio (in repeater mode) connect to a root AP or repeater. auto: to have the NWA/WAC automatically use the settings in the applied WDS profile to connect to a root AP or repeater. manual: to have the NWA/WAC connect to the root AP or repeater with the specified MAC address. You need to configure the MAC address of the root AP or repeater with which you want the NWA/WAC to associate.
wireless-bridge {enable | disable}	Enables or disables wireless bridging on the specified radio (*slot_name*). The NWA/WAC must support LAN provision and the radio should be in repeater mode. VLAN and bridge interfaces are created automatically according to the LAN port's VLAN settings. When wireless bridging is enabled, the NWA/WAC in repeater mode can still transmit data through its Ethernet port(s) after the WDS link is up. Be careful to avoid bridge loops. The NWA/WACs in the same WDS must use the same static VLAN ID.
show wlan *slot_name*	Displays the operating mode and profile settings for the specified radio.
show wlan *slot_name* detail	Displays the SSID, MAC address, VLAN ID and security mode for the specified radio.
show wlan *slot_name* list all sta	Displays statistics for the specified radio's wireless traffic.
show wlan country-code	Displays the country code of the NWA/WAC.
show wlan channels {11A|11G} [cw {20|20/40|20/40/80}] [country *country_code*] [indoor|outdoor]	Displays the channels available for the specified frequency band, channel width, and/or country. You can also specify whether the channels are for indoor or outdoor use.
show wlan radio macaddr	Displays the MAC address(es) assigned to the NWA/WAC's radio(s).
show wireless-hal current channel	Displays the channel number the NWA/WAC's radio is using.
show wireless-hal station info	Displays the connected station information of the NWA/WAC's radio.
show wireless-hal station number	Displays the number of wireless clients that are currently connected to the NWA/WAC.
show wireless-hal statistic	Displays the overall traffic information of the NWA/WAC's radio.
show wireless-hal wds info {all | downlink | uplink}	Displays the WDS traffic statistics between the NWA/WAC and a root AP or repeaters Uplink refers to the WDS link from the repeaters to the root AP. Downlink refers to the WDS link from the root AP to the repeaters.
show wireless-hal wds interface {all | downlink | uplink}	Displays status information for the WDS links. Uplink refers to the WDS link from the repeaters to the root AP. Downlink refers to the WDS link from the root AP to the repeaters.
show wireless-hal wds number	Displays the number of the root AP or repeater to which the NWA/WAC is connected using WDS.

9.3 AP Management Client Commands

The following table describes the commands available for configuring CAPWAP AP settings. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 23 Command Summary: CAPWAP AP Commands

COMMAND	DESCRIPTION
`capwap ap ac-ip {primary ip secondary ip | auto}`	Sets the AP controller's address or sets the NWA/WAC (in managed mode) to use DHCP option 138 to get the AP controller's IP address.
`capwap ap vlan ip address {ip subnet_mask | dhcp}`	Sets the IP address of the NWA/WAC or sets it to use DHCP.
`capwap ap vlan [no] ip gateway ip`	Adds the gateway address of the NWA/WAC. The `no` command removes the gateway setting.
`capwap ap vlan [no] ipv6 address ipv6_addr/prefix`	Sets the IPv6 address and the prefix length of the NWA/WAC. The no command removes the IPv6 address settings.
`capwap ap vlan [no] ipv6 dhcp6 {address-request | client}`	Set the NWA/WAC to act as a DHCPv6 client or get an IPv6 address from a DHCPv6 server. The no command sets the NWA/WAC to not get the IPv6 address from the DHCPv6 server.
`capwap ap vlan [no] ipv6 dhcp6-request-object dhcp6_profile`	Sets the profile of DHCPv6 request settings that determine what additional information to get from the DHCPv6 server. The no command removes the DHCPv6 request settings profile.
`capwap ap vlan [no] ipv6 enable`	Enables IPv6 stateless auto-configuration on the NWA/WAC. The NWA/WAC will generate an IPv6 address itself from a prefix obtained from an IPv6 router in the network. The no command disables IPv6 stateless auto-configuration.
`capwap ap vlan [no] ipv6 gateway ipv6_addr`	Sets the IPv6 address of the default outgoing gateway. The no command removes the IPv6 gateway settings.
`capwap ap vlan [no] ipv6 nd ra accept`	Sets the NWA/WAC to accept IPv6 neighbor discovery router advertisement messages. The no command sets the NWA/WAC to discard IPv6 neighbor discovery router advertisement messages.
`capwap ap vlan vlan-id <1..4094> [tag | untag]`	Sets the VLAN ID and tagging setting of the NWA/WAC.
`hybrid-mode [managed | standalone]`	Sets the NWA/WAC to act as a CAPWAP managed AP, or uses it in its default standalone mode. When the NWA/WAC is in standalone mode, you can manage the NWA/WAC using its own web configurator or commands. When the NWA/WAC is in managed mode, it can be configured ONLY by the AP controller.
`show capwap ap info`	Displays information about the NWA/WAC's wireless usage.
`show capwap ap discovery-type`	Displays how the NWA/WAC gets its IP address.
`show capwap ap ac-ip`	Displays the controller's IP address.
`show hybrid-mode`	Displays the NWA/WAC management mode.

9.3.1 AP Management Client Commands Example

The following example shows you how to configure the NWA/WAC management mode to allow it to be managed by an AP controller and check the NWA/WAC management mode.

```
Router# configure terminal
Router(config)# hybrid-mode managed
Router(config)# show hybrid-mode
mode: managed
Router(config)#
```

The following example shows you how to configure the interface of the NWA/WAC, set the AP controller IP address and display the related settings.

```
Router# configure terminal
Router(config)# show capwap_wtp ap discovery-type
Discovery type : Broadcast
Router(config)# capwap ap vlan ip address 192.168.1.37 255.255.255.0
Router(config)# capwap ap vlan ip gateway 192.168.1.32
Router(config)# capwap ap ac-ip 192.168.1.1 192.168.1.2
Router(config)# show capwap ap discovery-type
Discovery type : Static AC IP
Router(config)# show capwap ap ac-ip
AC IP: 192.168.1.1 192.168.1.2
Router(config)# exit
Router# show capwap ap info
             SM-State                    RUN(8)
        msg-buf-usage                    0/10 (Usage/Max)
       capwap-version                    10118
         Radio Number                    1/4 (Usage/Max)
           BSS Number                    8/8 (Usage/Max)
              IANA ID                    037a
          Description                    AP-0013499999FF
```

CHAPTER 10
Wireless LAN Profiles

This chapter shows you how to configure wireless LAN profiles on your NWA/WAC.

10.1 Wireless LAN Profiles Overview

The NWA/WACs are designed to work explicitly with your NWA/WACs. If you do not have on-board configuration files, you must create "profiles" to manage them. Profiles are preset configurations that are uploaded to the APs and which manage them. They include: Radio and Monitor profiles, SSID profiles, Security profiles, and MAC Filter profiles. Altogether, these profiles give you absolute control over your wireless network.

10.2 AP Radio & Monitor Profile Commands

The radio profile commands allow you to set up configurations for the radios onboard your various APs. The monitor profile commands allow you to set up monitor mode configurations that allow your APS to scan for other APs in the vicinity.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 24 Input Values for General Radio and Monitor Profile Commands

LABEL	DESCRIPTION
radio_profile_name	The radio profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
monitor_profile_name	The monitor profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
wireless_channel_2g	Sets the 2 Ghz channel used by this radio profile. The channel range is 1 ~ 14. Note: Your choice of channel may be restricted by regional regulations.
wireless_channel_5g	Sets the 5 Ghz channel used by this radio profile. The channel range is 36 ~ 165. Note: Your choice of channel may be restricted by regional regulations.
wlan_hctw	Sets the HT channel width. Select either 20, 20/40, or 20/40/80.
wlan_htgi	Sets the HT guard interval. Select either long or short.
chain_mask	Sets the network traffic chain mask. The range is 1 ~ 7.
scan_method	Sets the radio's scan method while in Monitor mode. Select manual or auto.

Table 24 Input Values for General Radio and Monitor Profile Commands (continued)

LABEL	DESCRIPTION
wlan_interface_index	Sets the radio interface index number. The range is 1 ~ 8.
wds_lan_interface_index	Sets the AP-WDS mode interface's index number. The range is 1 ~ 8.

The following table describes the commands available for radio and monitor profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 25 Command Summary: Radio Profile

COMMAND	DESCRIPTION
`show wlan-radio-profile {ap | monitor} {all | rule_count | [radio_profile_name]}`	Displays the radio profile(s). `all`: Displays all profiles for the selected operating mode. `rule_count`: Displays how many radio profiles are created on the NWA/WAC. *radio_profile_name*: Displays the specified profile for the selected operating mode.
`wlan-radio-profile rename` *radio_profile_name1 radio_profile_name2*	Gives an existing radio profile (*radio_profile_name1*) a new name (*radio_profile_name2*).
`[no] wlan-radio-profile` *radio_profile_name*	Enters configuration mode for the specified radio profile. Use the *no* parameter to remove the specified profile.
`[no] activate`	Makes this profile active or inactive.
`band` *wlan_band* `band_mode` *wlan_band_mode*	Sets the radio band (2.4 GHz or 5 GHz) and 80.211 wireless mode for this profile. *wlan_band*: 2.4G or 5G *wlan_band_mode*: 11n, bg, bgn, a, ac, an
`2g-channel` *wireless_channel_2g*	Sets the broadcast band for this profile in the 2.4 Ghz frequency range. The default is 6.
`2g-multicast-speed` *wlan_2g_support_speed*	When you disable multicast to unicast, use this command to set the data rate {1.0 | 2.0 | …} in Mbps for 2.4 GHz multicast traffic.
`5g-channel` *wireless_channel_5g*	Sets the broadcast band for this profile in the 5 GHz frequency range.
`5g-multicast-speed` *wlan_5g_basic_speed*	When you disable multicast to unicast, use this command to set the data rate {6.0 | 9.0 | …} in Mbps for 5 GHz multicast traffic.
`[no] ampdu`	Activates MPDU frame aggregation for this profile. Use the *no* parameter to disable it. Message Protocol Data Unit (MPDU) aggregation collects Ethernet frames along with their 802.11n headers and wraps them in a 802.11n MAC header. This method is useful for increasing bandwidth throughput in environments that are prone to high error rates. By default this is enabled.

Table 25 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
[no] amsdu	Activates MPDU frame aggregation for this profile. Use the *no* parameter to disable it. Mac Service Data Unit (MSDU) aggregation collects Ethernet frames without any of their 802.11n headers and wraps the header-less payload in a single 802.11n MAC header. This method is useful for increasing bandwidth throughput. It is also more efficient than A-MPDU except in environments that are prone to high error rates. By default this is enabled.
beacon-interval <40..1000>	Sets the beacon interval for this profile. When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. This value can be set from 40ms to 1000ms. A high value helps save current consumption of the access point. The default is 100.
[no] block-ack	Makes block-ack active or inactive. Use the *no* parameter to disable it.
ch-width *wlan_htcw*	Sets the channel width for this profile.
[no] ctsrts <0..2347>	Sets or removes the RTS/CTS value for this profile. Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions). A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the fragmentation threshold to turn RTS/CTS off. The default is 2347.
[no] disable-dfs-switch	Makes the DFS switch active or inactive. By default this is inactive.
dtim-period <1..255>	Sets the DTIM period for this profile. Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255. The default is 1.
description *description*	Sets the description for the profile. You may use up to 60 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive
dcs time-interval *interval*	Sets the interval that specifies how often DCS should run.
dcs sensitivity-level *{*high|medium|low*}*	Sets how sensitive DCS is to radio channel changes in the vicinity of the AP running the scan.
dcs client-aware {enable|disable}	When enabled, this ensures that the NWA/WAC will not change channels as long as a client is connected to it. If disabled, the NWA/WAC may change channels regardless of whether it has clients connected to it or not.

Table 25 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
dcs channel-deployment {3-channel|4-channel}	Sets either a 3-channel deployment or a 4-channel deployment. In a 3-channel deployment, the AP running the scan alternates between the following channels: 1, 6, and 11. In a 4-channel deployment, the AP running the scan alternates between the following channels: 1, 4, 7, and 11 (FCC) or 1, 5, 9, and 13 (ETSI). Set the option that is applicable to your region. (Channel deployment may be regulated differently between countries and locales.)
dcs 2g-selected-channel *2.4g_channels*	Specifies the channels that are available in the 2.4 GHz band when you manually configure the channels the NWA/WAC can use.
dcs 5g-selected-channel *5g_channels*	Specifies the channels that are available in the 5 GHz band when you manually configure the channels the NWA/WAC can use.
dcs dcs-2g-method {auto|manual}	Sets the NWA/WAC to automatically search for available channels or manually configure the channels the NWA/WAC uses in the 2.4 GHz band.
dcs dcs-5g-method {auto|manual}	Sets the NWA/WAC to automatically search for available channels or manually configure the channels the NWA/WAC uses in the 5 GHz band.
dcs dfs-aware {enable|disable}	Enable this to allow an NWA/WAC to avoid phase DFS channels below the 5 GHz spectrum.
dcs mode {interval|schedule}	Sets the NWA/WAC to use DCS at the end of the specified time interval or at a specific time on selected days of the week.
dcs schedule <hh:mm> {mon|tue|wed|thu|fri|sat|sun}	Sets what time of day (in 24-hour format) the NWA/WAC starts to use DCS on the specified day(s) of the week.
[no] dot11n-disable-coexistence	Fixes the channel bandwidth as 40 MHz. The no command has the NWA/WAC automatically choose 40 MHz if all the clients support it or 20 MHz if some clients only support 20 MHz.
[no] frag <256..2346>	Sets or removes the fragmentation value for this profile. The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. The default is 2346.
guard-interval *wlan_htgi*	Sets the guard interval for this profile. The default for this is *short*.
[no] htprotect	Activates HT protection for this profile. Use the *no* parameter to disable it. By default, this is disabled.
limit-ampdu < 100..65535>	Sets the maximum frame size to be aggregated. By default this is 50000.
subframe-ampdu <2..64>	Sets the maximum number of frames to be aggregated each time. By default this is 32.
limit-amsdu <2290..4096>	Sets the maximum frame size to be aggregated. The default is 4096.

Table 25 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
[no] multicast-to-unicast	"Multicast to unicast" broadcasts wireless multicast traffic to all wireless clients as unicast traffic to provide more reliable transmission. The data rate changes dynamically based on the application's bandwidth requirements. Although unicast provides more reliable transmission of the multicast traffic, it also produces duplicate packets. The no command turns multicast to unicast off to send wireless multicast traffic at the rate you specify with the 2g-multicast-speed or 5g-multicast-speed command.
[no] reject-legacy-station	Allows only 802.11 n/ac clients to connect, and reject 802.11a/b/g clients. Use the no command to also allow 802.11a/b/g clients.
role {ap}	Sets the profile's wireless LAN radio operating mode. Use ap to have the radio function as an access point with one or more BSSIDs.
rssi-dbm <-20~-76>	When using the RSSI threshold, set a minimum client signal strength for connecting to the AP. -20 dBm is the strongest signal you can require and -76 is the weakest.
rssi-kickout <-20~-90>	Sets a minimum kick-off signal strength. When a wireless client's signal strength is lower than the specified threshold, the NWA/WAC disconnects the wireless client. -20 dBm is the strongest signal you can require and -90 is the weakest.
[no] rssi-retry	Allows a wireless client to try to associate with the NWA/WAC again after it is disconnected due to weak signal strength. Use the *no* parameter to disallow it.
rssi-retrycount <1~100>	Sets the maximum number of times a wireless client can attempt to re-connect to the NWA/WAC.
[no] rssi-thres	Sets whether or not to use the Received Signal Strength Indication (RSSI) threshold to ensure wireless clients receive good throughput. This allows only wireless clients with a strong signal to connect to the NWA/WAC.
tx-mask *chain_mask*	Sets the outgoing chain mask.
rx-mask *chain_mask*	Sets the incoming chain mask.
exit	Exits configuration mode for this profile.
show wlan-monitor-profile {all|rule_count|*[monitor_profile_name]*}	Displays all monitor profiles or just the specified one. rule_count: Displays how many monitor profiles are created on the NWA/WAC.
wlan-monitor-profile rename *monitor_profile_name1 monitor_profile_name2*	Gives an existing monitor profile (*monitor_profile_name1*) a new name (*monitor_profile_name2*).
[no] wlan-monitor-profile *monitor_profile_name*	Enters configuration mode for the specified monitor profile. Use the *no* parameter to remove the specified profile.
[no] activate	Makes this profile active or inactive. By default, this is enabled.
description *description*	Sets the description for the profile. You may use up to 60 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive

Table 25 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
scan-method *scan_method*	Sets the channel scanning method for this profile.
[no] 2g-scan-channel *wireless_channel_2g*	Sets the broadcast band for this profile in the 2.4 Ghz frequency range. Use the *no* parameter to disable it.
[no] 5g-scan-channel *wireless_channel_5g*	Sets the broadcast band for this profile in the 5 GHz frequency range. Use the *no* parameter to disable it.
scan-dwell *<100..1000>*	Sets the duration in milliseconds that the device using this profile scans each channel.
exit	Exits configuration mode for this profile.

10.2.1 AP radio & Monitor Profile Commands Example

The following example shows you how to set up the radio profile named 'RADIO01', activate it, and configure it to use the following settings:

- 2.4G band and 802.11ac wireless mode with channel 6
- channel width of 20MHz
- a DTIM period of 2
- a beacon interval of 100ms
- AMPDU frame aggregation enabled
- an AMPDU buffer limit of 65535 bytes
- an AMPDU subframe limit of 64 frames
- AMSDU frame aggregation enabled
- an AMSDU buffer limit of 4096
- block acknowledgement enabled
- a short guard interval

```
Router(config)# wlan-radio-profile RADIO01
Router(config-profile-radio)# activate
Router(config-profile-radio)# band 2.4G band_mode ac
Router(config-profile-radio)# 2g-channel 6
Router(config-profile-radio)# ch-width 20m
Router(config-profile-radio)# dtim-period 2
Router(config-profile-radio)# beacon-interval 100
Router(config-profile-radio)# ampdu
Router(config-profile-radio)# limit-ampdu 65535
Router(config-profile-radio)# subframe-ampdu 64
Router(config-profile-radio)# amsdu
Router(config-profile-radio)# limit-amsdu 4096
Router(config-profile-radio)# block-ack
Router(config-profile-radio)# guard-interval short
Router(config-profile-radio)# tx-mask 5
Router(config-profile-radio)# rx-mask 7
```

10.3 SSID Profile Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 26 Input Values for General SSID Profile Commands

LABEL	DESCRIPTION
ssid_profile_name	The SSID profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
ssid	The SSID broadcast name. You may use 1-32 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive.
wlan_qos	Sets the type of QoS the SSID should use. *disable*: Turns off QoS for this SSID. *wmm*: Turns on QoS for this SSID. It automatically assigns Access Categories to packets as the device inspects them in transit. *wmm_be*: Assigns the "best effort" Access Category to all traffic moving through the SSID regardless of origin. *wmm_bk*: Assigns the "background" Access Category to all traffic moving through the SSID regardless of origin. *wmm_vi*: Assigns the "video" Access Category to all traffic moving through the SSID regardless of origin. *wmm_vo*: Assigns the "voice" Access Category to all traffic moving through the SSID regardless of origin.
securityprofile	Assigns an existing security profile to the SSID profile. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
macfilterprofile	Assigns an existing MAC filter profile to the SSID profile. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
description2	Sets the description of the profile. You may use up to 60 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive.

The following table describes the commands available for SSID profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 27 Command Summary: SSID Profile

COMMAND	DESCRIPTION
`show wlan-ssid-profile {all | rule_count | ssid_profile_name}`	Displays the SSID profile(s). `all`: Displays all profiles. `rule_count`: Displays how many SSID profiles are created on the NWA/WAC. *ssid_profile_name*: Displays the specified profile.
`wlan-ssid-profile rename ssid_profile_name1 ssid_profile_name2`	Gives an existing SSID profile (*ssid_profile_name1*) a new name (*ssid_profile_name2*).
`[no] wlan-ssid-profile ssid_profile_name`	Enters configuration mode for the specified SSID profile. Use the *no* parameter to remove the specified profile.

Table 27 Command Summary: SSID Profile (continued)

COMMAND	DESCRIPTION
[no] block-intra	Enables intra-BSSID traffic blocking. Use the no parameter to disable it in this profile. By default this is disabled.
description *description*	Sets a descriptive name for this profile.
[no] dot11k-v activate	Enable IEEE 802.11k/v assisted roaming on the NWA/WAC. When the connected clients request 802.11k neighbor lists, the NWA/WAC will response with a list of neighbor APs that can be candidates for roaming. Use the no parameter to disable it in this profile.
downlink-rate-limit *data_rate*	Sets the maximum incoming transmission data rate (either in mbps or kbps) on a per-station basis.
exit	Exits configuration mode for this profile.
[no] hide	Prevents the SSID from being publicly broadcast. Use the no parameter to re-enable public broadcast of the SSID in this profile. By default this is disabled.
[no] l2isolation *l2profile*	Assigns the specified layer-2 isolation profile to this SSID profile. Use the no parameter to remove it. By default, no layer-2 isolation profile is assigned.
[no] macfilter *macfilterprofile*	Assigns the specified MAC filtering profile to this SSID profile. Use the no parameter to remove it. By default, no MAC filter is assigned.
[no] proxy-arp	Sets the NWA/WAC to answer ARP requests for an IP address on behalf of a client associated with this SSID. This can reduce broadcast traffic and improve network performance. Use the no parameter to disable Proxy ARP.
qos *wlan_qos*	Sets the type of QoS used by this SSID.
security *securityprofile*	Assigns the specified security profile to this SSID profile.
ssid	Sets the SSID. This is the name visible on the network to wireless clients. Enter up to 32 characters, spaces and underscores are allowed.
[no] ssid-schedule	Enables the SSID schedule. Use the no parameter to disable the SSID schedule.
{mon|tue|wed|thu|fri|sat|sun} {disable | enable} <hh:mm> <hh:mm>	Sets whether the SSID is enabled or disabled on each day of the week. This also specifies the hour and minute (in 24-hour format) to set the time period of each day during which the SSID is enabled/ enabled. <hh:mm> <hh:mm>: If you set both start time and end time to 00:00, it indicates a whole day event. Note: The end time must be larger than the start time.
[no] uapsd	Enables Unscheduled Automatic Power Save Delivery (U-APSD), which is also known as WMM-Power Save. This helps increase battery life for battery-powered wireless clients connected to the NWA/WAC using this SSID profile. Use the no parameter to disable the U-APSD feature.

Table 27 Command Summary: SSID Profile (continued)

COMMAND	DESCRIPTION
uplink-rate-limit *data_rate*	Sets the maximum outgoing transmission data rate (either in mbps or kbps) on a per-station basis.
[no] vlan-id <1..4094>	Applies to each SSID profile. If the VLAN ID is equal to the AP's native VLAN ID then traffic originating from the SSID is not tagged. The default VLAN ID is 1.

10.3.1 SSID Profile Example

The following example creates an SSID profile with the name 'Zyxel'. It makes the assumption that both the security profile (SECURITY01) and the MAC filter profile (MACFILTER01) already exist.

```
Router(config)# wlan-ssid-profile SSID01
Router(config-ssid-radio)# ssid Zyxel
Router(config-ssid-radio)# qos wmm
Router(config-ssid-radio)# security SECURITY01
Router(config-ssid-radio)# macfilter MACFILTER01
Router(config-ssid-radio)# exit
Router(config)#
```

10.4 Security Profile Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 28 Input Values for General Security Profile Commands

LABEL	DESCRIPTION
security_profile_name	The security profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
wep_key	Sets the WEP key encryption strength. Select either *64bit* or *128bit*.
wpa_key	Sets the WPA/WPA2 pre-shared key in ASCII. You may use 8~63 alphanumeric characters. This value is case-sensitive.
wpa_key_64	Sets the WPA/WPA2 pre-shared key in HEX. You muse use 64 alphanumeric characters.
secret	Sets the shared secret used by your network's RADIUS server.
auth-method	The authentication method used by the security profile.

The following table describes the commands available for security profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 29 Command Summary: Security Profile

COMMAND	DESCRIPTION
`show wlan-security-profile {all | rule_count | [security_profile_name]}`	Displays the security profile(s). `all`: Displays all profiles. `rule_count`: Displays how many security profiles are created on the NWA/WAC. *security_profile_name*: Displays the specified profile.
`wlan-security-profile rename` *security_profile_name1 security_profile_name2*	Gives existing security profile (*security_profile_name1*) a new name, (*security_profile_name2*).
`[no] wlan-security-profile` *security_profile_name*	Enters configuration mode for the specified security profile. Use the *no* parameter to remove the specified profile.
`[no] accounting interim-interval <1..1440>`	Sets the time interval for how often the NWA/WAC is to send an interim update message with current client statistics to the accounting server. Use the no parameter to clear the interval setting.
`[no] accounting interim-update`	Sets the NWA/WAC to send accounting update messages to the accounting server at the specified interval. Use the no parameter to disable it.
`description` *description*	Sets the description for the profile. You may use up to 60 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive
`[no] dot11w`	Data frames in 802.11 WLANs can be encrypted and authenticated with WEP, WPA or WPA2. But 802.11 management frames, such as beacon/probe response, association request, association response, de-authentication and disassociation are always unauthenticated and unencrypted. IEEE 802.11w Protected Management Frames allows APs to use the existing security mechanisms (encryption and authentication methods defined in IEEE 802.11i WPA/WPA2) to protect management frames. This helps prevent wireless DoS attacks. Enables management frame protection (MFP) to add security to 802.11 management frames. Use the no parameter to disable it.
`dot11w-op <1..2>`	Sets whether wireless clients have to support management frame protection in order to access the wireless network. 1: if you do not require the wireless clients to support MFP. Management frames will be encrypted if the clients support MFP. 2: wireless clients must support MFP in order to join the NWA/WAC's wireless network.
`[no] dot1x-eap`	Enables 802.1x secure authentication. Use the no parameter to disable it.
`eap {external | internal` *auth_method*`}`	Sets the 802.1x authentication method.
`group-key <30..30000>`	Sets the interval (in seconds) at which the AP updates the group WPA/WPA2 encryption key. The default is 1800.

Table 29 Command Summary: Security Profile (continued)

COMMAND	DESCRIPTION
idle <30..30000>	Sets the idle interval (in seconds) that a client can be idle before authentication is discontinued. The default is 3000.
[no] mac-auth activate	MAC authentication has the AP use an external server to authenticate wireless clients by their MAC addresses. Users cannot get an IP address if the MAC authentication fails. The no parameter turns it off. RADIUS servers can require the MAC address in the wireless client's account (username/password) or Calling Station ID RADIUS attribute.
mac-auth auth-method *auth_method*	Sets the authentication method for MAC authentication.
mac-auth case account {upper | lower}	Sets the case (upper or lower) the external server requires for using MAC addresses as the account username and password. For example, use mac-auth case account upper and mac-auth delimiter account dash if you need to use a MAC address formatted like 00-11-AC-01-A0-11 as the username and password.
mac-auth case calling-station-id {upper | lower}	Sets the case (upper or lower) the external server requires for letters in MAC addresses in the Calling Station ID RADIUS attribute.
mac-auth delimiter account {colon | dash | none}	Specify the separator the external server uses for the two-character pairs within MAC addresses used as the account username and password. For example, use mac-auth case account upper and mac-auth delimiter account dash if you need to use a MAC address formatted like 00-11-AC-01-A0-11 as the username and password.
mac-auth delimiter calling-station-id {colon | dash | none}	Select the separator the external server uses for the pairs in MAC addresses in the Calling Station ID RADIUS attribute.
mode <*none* | *wep* | *wpa2* | *wpa2-mix*>	Sets the security mode for this profile.
[no] server-auth <1..2> activate	Activates server authentication. Use the no parameter to deactivate.
radius-attr nas-id *string*	Sets the NAS (Network Access Server) identifier attribute if the RADIUS server requires the NWA/WAC to provide it. The NAS identifier is to identify the source of access request. It could be the NAS's fully qualified domain name.
radius-attr nas-ip *ip*	Sets the NAS (Network Access Server) IP address attribute if the RADIUS server requires the NWA/WAC to provide it.
[no] reauth <30..30000>	Sets the interval (in seconds) between authentication requests. The default is 0.
server-auth <1..2> IPv4 port *port* secret *secret*	Sets the server authentication IPv4 port and shared secret.
[no] server-auth <1..2>	Clears the server authentication setting.
wep-auth-type <*open* | *share*>	Sets the authentication key type to either *open* or *share*.
wep <*64* | *128*> default-key <*1..4*>	Sets the WEP encryption strength (*64 or 128*) and the default key index (*1 ~ 4*).

Table 29 Command Summary: Security Profile (continued)

COMMAND	DESCRIPTION
wep-key *<1..4> wep_key*	If you select WEP-64 enter 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x11AA22BB33) for each Key used; or enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for each Key used. If you select WEP-128 enter 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x00112233445566778899AABBCC) for each Key used; or enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for each Key used. You can save up to four different keys. Enter the default-key (*1 ~ 4*) to save your WEP to one of those four available slots.
wpa-encrypt <aes | auto>	Sets the WPA/WPA2 encryption cipher type. auto: This automatically chooses the best available cipher based on the cipher in use by the wireless client that is attempting to make a connection. aes: This is the Advanced Encryption Standard encryption method, a newer more robust algorithm than TKIP Not all wireless clients may support this.
wpa-psk *{wpa_key | wpa_key_64}*	Sets the WPA/WPA2 pre-shared key.
[no] wpa2-preauth	Enables pre-authentication to allow wireless clients to switch APs without having to re-authenticate their network connection. The RADIUS server puts a temporary PMK Security Authorization cache on the wireless clients. It contains their session ID and a pre-authorized list of viable APs. Use the no parameter to disable this.
exit	Exits configuration mode for this profile.

10.4.1 Security Profile Example

The following example creates a security profile with the name 'SECURITY01'..

```
Router(config)# wlan-security-profile SECURITY01
Router(config-security-profile)# mode wpa2
Router(config-security-profile)# wpa-encrypt aes
Router(config-security-profile)# wpa-psk 12345678
Router(config-security-profile)# idle 3600
Router(config-security-profile)# reauth 1800
Router(config-security-profile)# group-key 1800
Router(config-security-profile)# exit
Router(config)#
```

10.5 MAC Filter Profile Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 30 Input Values for General MAC Filter Profile Commands

LABEL	DESCRIPTION
macfilter_profile_name	The MAC filter profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
description	Sets the description of the MAC address. You may use up to 60 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive.

The following table describes the commands available for MAC filter profile management. You must use the configure terminal command to enter the configuration mode before you can use these commands.

Table 31 Command Summary: MAC Filter Profile

COMMAND	DESCRIPTION
`show wlan-macfilter-profile {all | rule_count | [macfilter_profile_name]}`	Displays the MAC filter profile(s). `all`: Displays all profiles. `rule_count`: Displays how many MAC filter profiles are created on the NWA/WAC. *macfilter_profile_name*: Displays the specified profile.
`wlan-macfilter-profile rename` *macfilter_profile_name1 macfilter_profile_name2*	Gives an existing MAC filter profile (*macfilter_profile_name1*) a new name (*macfilter_profile_name2*).
`[no] wlan-macfilter-profile` *macfilter_profile_name*	Enters configuration mode for the specified MAC filter profile. Use the *no* parameter to remove the specified profile.
`filter-action {allow | deny}`	Permits the wireless client with the MAC addresses in this profile to connect to the network through the associated SSID; select deny to block the wireless clients with the specified MAC addresses. The default is set to *deny*.
`[no] mac_addr [description description]`	Specifies a MAC address associated with this profile. You can also set a description for the MAC address. Enter up to 60 characters. Spaces and underscores allowed.
`exit`	Exits configuration mode for this profile.

10.5.1 MAC Filter Profile Example

The following example creates a MAC filter profile with the name ‘MACFILTER01’..

```
Router(config)# wlan-macfilter-profile MACFILTER01
Router(config-macfilter-profile)# filter-action deny
Router(config-macfilter-profile)# 01:02:03:04:05:06  description MAC01
Router(config-macfilter-profile)# 01:02:03:04:05:07  description MAC02
Router(config-macfilter-profile)# 01:02:03:04:05:08  description MAC03
Router(config-macfilter-profile)# exit
Router(config)#
```

10.6 Layer-2 Isolation Profile Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 32 Input Values for General Layer-2 Isolation Profile Commands

LABEL	DESCRIPTION
l2isolation_profile_name	The layer-2 isolation profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
mac_address	The MAC address of the device that is allowed to communicate with the NWA/WAC's wireless clients. Enter 6 hexadecimal pairs separated by colons. You can use 0-9, a-z and A-Z.
description	Sets the description name of MAC address in the profile. You may use 1-60 alphanumeric characters, underscores (_), or dashes (-).

The following table describes the commands available for Layer-2 Isolation profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 33 Command Summary: Layer-2 Isolation Profile

COMMAND	DESCRIPTION
`show wlan-l2isolation-profile {all | rule_count | [l2isolation_profile_name]}`	Displays the layer-2 isolation profile(s) settings. `all`: Displays settings of all layer-2 isolation profiles configured on the NWA/WAC. `rule_count`: Displays how many layer-2 isolation profiles are created on the NWA/WAC. *l2isolation_profile_name*: Displays settings of the specified profile.
`wlan-l2isolation-profile rename` *l2isolation_profile_name1 l2isolation_profile_name2*	Gives the existing layer-2 isolation profile (*l2isolation_profile_name1*) a new name, (*l2isolation_profile_name2*).
`[no] wlan-l2isolation-profile` *l2isolation_profile_name*	Enters configuration mode for the specified layer-2 isolation profile. Use the *no* parameter to remove the specified profile.
`[no]` *mac_address*	Sets the MAC address of the device that is allowed to communicate with the NWA/WAC's wireless clients in this profile.
`description` *description*	Sets the description name for the MAC address associated with this profile.
`exit`	Exits configuration mode for this profile.

10.6.1 Layer-2 Isolation Profile Example

The following example creates a layer-2 isolation profile with the name 'test1'.

```
Router(config)# wlan-l2isolation-profile test1
Router(config-wlan-l2isolation test1)# 00:a0:c5:01:23:45
Router(config-wlan-l2isolation test1)# description user1
Router(config-wlan-l2isolation test1)# exit
Router(config)#
```

10.7 WDS Profile Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 34 Input Values for General WDS Profile Commands

LABEL	DESCRIPTION
wds_profile_name	The WDS profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following table describes the commands available for WDS profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 35 Command Summary: WDS Profile

COMMAND	DESCRIPTION
`show wlan-wds-profile {all | rule_count | [wds_profile_name]}`	Displays the WDS profile(s) settings. `all`: Displays settings of all WDS profiles configured on the NWA/WAC. `rule_count`: Displays how many WDS profiles are created on the NWA/WAC. *wds_profile_name*: Displays settings of the specified profile.
`wlan-wds-profile rename wds_profile_name1 wds_profile_name2`	Gives the existing WDS profile (*wds_profile_name1*) a new name, (*wds_profile_name2*).
`[no] wlan-wds-profile wds_profile_name`	Enters configuration mode for the specified WDS profile.
`psk psk`	Sets a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.The key is used to encrypt the traffic between the APs.
`ssid ssid`	Sets the SSID with which you want the NWA/WAC to connect to a root AP or repeater to form a WDS.
`exit`	Exits configuration mode for this profile.

10.7.1 WDS Profile Example

The following example creates a WDS profile with the name 'WDS1', and shows the profile settings.

```
Router(config)# wlan-wds-profile WDS1
Router(config-wlan-wds WDS1)# ssid Zyxel-WDS
Router(config-wlan-wds WDS1)# psk qwer1234
Router(config-wlan-wds WDS1)# exit
Router(config)# show wlan-wds-profile WDS1
wds profile: WDS1
  reference: 0
  Id: 2
  Description:
  WDS_SSID: Zyxel-WDS
  WDS_PSK: qwer1234
Router(config)#
```

CHAPTER 11
Rogue AP

This chapter shows you how to set up Rogue Access Point (AP) detection and containment.

11.1 Rogue AP Detection Overview

Rogue APs are wireless access points operating in a network's coverage area that are not under the control of the network's administrators, and can potentially open holes in the network security. Attackers can take advantage of a rogue AP's weaker (or non-existent) security to gain illicit access to the network, or set up their own rogue APs in order to capture information from wireless clients.

Conversely, a friendly AP is one that the NWA/WAC network administrator regards as non-threatening. This does not necessarily mean the friendly AP must belong to the network managed by the NWA/WAC; rather, it is any unmanaged AP within range of the NWA/WAC's own wireless network that is allowed to operate without being contained. This can include APs from neighboring companies, for example, or even APs maintained by your company's employees that operate outside of the established network.

11.2 Rogue AP Detection Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 36 Input Values for Rogue AP Detection Commands

LABEL	DESCRIPTION
ap_mac	Specifies the MAC address (in XX:XX:XX:XX:XX:XX or XX-XX-XX-XX-XX-XX format) of the AP to be added to either the rogue AP or friendly AP list. The no command removes the entry.
description2	Sets the description of the AP. You may use 1-60 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive.

The following table describes the commands available for rogue AP detection. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 37 Command Summary: Rogue AP Detection

COMMAND	DESCRIPTION
`rogue-ap detection`	Enters sub-command mode for rogue AP detection.
`[no] activate`	Activates rogue AP detection. Use the no parameter to deactivate rogue AP detection.
`[no] ap-mode detection activate`	Sets the NWA/WAC to detect Rogue APs in the network. Use the no parameter to disable rogue AP detection.

Table 37 Command Summary: Rogue AP Detection (continued)

COMMAND	DESCRIPTION
detect interval <10..1440>	Sets the time interval (in seconds) at which the NWA/WAC scans for rogues APs.
friendly-ap *ap_mac description2*	Sets the device that owns the specified MAC address as a friendly AP. You can also assign a description to this entry on the friendly AP list.
no friendly-ap *ap_mac*	Removes the device that owns the specified MAC address from the friendly AP list.
rogue-ap *ap_mac description2*	Sets the device that owns the specified MAC address as a rogue AP. You can also assign a description to this entry on the rogue AP list.
no rogue-ap *ap_mac*	Removes the device that owns the specified MAC address from the rogue AP list.
[no] rogue-rule {hidden-ssid|ssid-keyword|weak-security}	Specifies the characteristic(s) an AP should have for the NWA/WAC to classify it as a Rogue AP. Use the no parameter to remove the classification rule.
[no] rogue-rule keyword <*ssid*>	Adds an SSID Keyword. Use the no parameter to remove the SSID keyword.
exit	Exits configuration mode for rogue AP detection.
show rogue-ap detection keyword list	Displays the SSID keyword(s) an AP should have for the NWA/WAC to rule it as a Rogue AP.
show rogue-ap detection monitoring	Displays a table of detected APs and information about them, such as their MAC addresses, when they were last seen, and their SSIDs, to name a few.
show rogue-ap detection list *{rogue|friendly|all}*	Displays the specified rogue/friendly/all AP list.
show rogue-ap detection status	Displays whether rogue AP detection is on or off.
show rogue-ap detection info	Displays a summary of the number of detected devices from the following categories: rogue, friendly, ad-hoc, unclassified, and total.

11.2.1 Rogue AP Detection Examples

This example sets the device associated with MAC address 00:13:49:11:11:11 as a rogue AP, and the device associated with MAC address 00:13:49:11:11:22 as a friendly AP. It then removes MAC address from the rogue AP list with the assumption that it was misidentified.

```
Router(config)# rogue-ap detection
Router(config-detection)# rogue-ap 00:13:49:11:11:11 rogue
Router(config-detection)# friendly-ap 00:13:49:11:11:22 friendly
Router(config-detection)# no rogue-ap 00:13:49:11:11:11
Router(config-detection)# exit
```

This example displays the rogue AP detection list.

```
Router(config)# show rogue-ap detection list rogue
no.   mac               description
contain
================================================================================
1    00:13:49:18:15:5A
0
```

This example shows the friendly AP detection list.

```
Router(config)# show rogue-ap detection list friendly
no.   mac                 description
================================================================================
1     11:11:11:11:11:11   third floor
2     00:13:49:11:22:33
3     00:13:49:00:00:05
4     00:13:49:00:00:01
5     00:0D:0B:CB:39:33   dept1
```

This example shows the combined rogue and friendly AP detection list.

```
Router(config)# show rogue-ap detection list all
no.   role         mac                 description
================================================================================
1     friendly-ap  11:11:11:11:11:11   third floor
2     friendly-ap  00:13:49:11:22:33
3     friendly-ap  00:13:49:00:00:05
4     friendly-ap  00:13:49:00:00:01
5     friendly-ap  00:0D:0B:CB:39:33   dept1
6     rogue-ap     00:13:49:18:15:5A
```

This example shows both the status of rogue AP detection and the summary of detected APs.

```
Router(config)# show rogue-ap detection status
rogue-ap detection status: on

Router(config)# show rogue-ap detection info
rogue ap: 1
friendly ap: 4
adhoc: 4
unclassified ap: 0
total devices: 0
```

11.3 Rogue AP Containment Overview

These commands enable rogue AP containment. You can use them to isolate a device that is flagged as a rogue AP. They are global in that they apply to all managed APs on the network (all APs utilize the same containment list, but only APs set to monitor mode can actively engage in containment of rogue APs). This means if we add a MAC address of a device to the containment list, then every AP on the network will respect it.

Note: Containing a rogue AP means broadcasting unviable login data at it, preventing legitimate wireless clients from connecting to it. This is a kind of Denial of Service attack.

11.4 Rogue AP Containment Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 38 Input Values for Rogue AP Containment Commands

LABEL	DESCRIPTION
ap_mac	Specifies the MAC address (in XX:XX:XX:XX:XX:XX format) of the AP to be contained. The no command removes the entry.

The following table describes the commands available for rogue AP containment. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 39 Command Summary: Rogue AP Containment

COMMAND	DESCRIPTION
`rogue-ap containment`	Enters sub-command mode for rogue AP containment.
`[no] activate`	Activates rogue AP containment. Use the no parameter to deactivate rogue AP containment.
`[no] contain` *ap_mac*	Isolates the device associated with the specified MAC address. Use the no parameter to remove this device from the containment list.
`exit`	Exits configuration mode for rogue AP containment.
`show rogue-ap containment list`	Displays the rogue AP containment list.

11.4.1 Rogue AP Containment Example

This example contains the device associated with MAC address 00:13:49:11:11:12 then displays the containment list for confirmation.

```
Router(config)# rogue-ap containment
Router(config-containment)# activate
Router(config-containment)# contain 00:13:49:11:11:12
Router(config-containment)# exit
Router(config)# show rogue-ap containment list
no.   mac
=================================================================
1     00:13:49:11:11:12
```

CHAPTER 12
Wireless Frame Capture

This chapter shows you how to configure and use wireless frame capture on the NWA/WAC.

12.1 Wireless Frame Capture Overview

Troubleshooting wireless LAN issues has always been a challenge. Wireless sniffer tools like Ethereal can help capture and decode packets of information, which can then be analyzed for debugging. It works well for local data traffic, but if your devices are spaced increasingly farther away then it often becomes correspondingly difficult to attempt remote debugging. Complicated wireless packet collection is arguably an arduous and perplexing process. The wireless frame capture feature in the NWA/WAC can help.

This chapter describes the wireless frame capture commands, which allows a network administrator to capture wireless traffic information and download it to an Ethereal/Tcpdump compatible format packet file for analysis.

12.2 Wireless Frame Capture Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 40 Input Values for Wireless Frame Capture Commands

LABEL	DESCRIPTION
ip_address	The IP address of the Access Point (AP) that you want to monitor. Enter a standard IPv4 IP address (for example, 192.168.1.2).
mon_file_size	The size (in kbytes) of file to be captured. It stops the capture and generates the capture file when either it reaches this size or the total combined size of all files in the directory reaches the maximum size which is 50 megabytes (51200 kbytes).
file_name	The file name prefix for each captured file. The default prefix is monitor while the default file name is monitor.dump. You can use 1-31 alphanumeric characters, underscores or dashes but the first character cannot be a number. This string is case sensitive.

The following table describes the commands available for wireless frame capture. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 41 Command Summary: Wireless Frame Capture

COMMAND	DESCRIPTION
`frame-capture configure`	Enters sub-command mode for wireless frame capture.
`src-ip add` *ip_address*	Sets the IP address of an AP controlled by the NWA/WAC that you want to monitor. You can use this command multiple times to add additional IPs to the monitor list.
`file-prefix` *file_name*	Sets the file name prefix for each captured file. Enter up to 31 alphanumeric characters. Spaces and underscores are not allowed.
`files-size` *mon_file_size*	Sets the size (in kbytes) of files to be captured.
`exit`	Exits configuration mode for wireless frame capture.
`[no] frame-capture activate`	Starts wireless frame capture. Use the no parameter to turn it off.
`show frame-capture status`	Displays whether frame capture is running or not.
`show frame-capture config`	Displays the frame capture configuration.

12.2.1 Wireless Frame Capture Examples

This example configures the wireless frame capture parameters for an AP located at IP address 192.168.1.2.

```
Router(config)# frame-capture configure
Router(frame-capture)# src-ip add 192.168.1.2
Router(frame-capture)# file-prefix monitor
Router(frame-capture)# files-size 1000
Router(frame-capture)# exit
Router(config)#
```

This example shows frame capture status and configuration.

```
Router(config)# show frame-capture status
capture status: off

Router(config)# show frame-capture config
capture source: 192.168.1.2
file prefix: monitor
file size: 1000
```

CHAPTER 13
Dynamic Channel Selection

This chapter shows you how to configure and use dynamic channel selection on the NWA/WAC.

13.1 DCS Overview

Dynamic Channel Selection (DCS) is a feature that allows an AP to automatically select the radio channel upon which it broadcasts by passively listening to the area around it and determining what channels are currently being broadcast on by other devices.

When numerous APs broadcast within a given area, they introduce the possibility of heightened radio interference, especially if some or all of them are broadcasting on the same radio channel. This can make accessing the network potentially rather difficult for the stations connected to them. If the interference becomes too great, then the network administrator must open his AP configuration options and manually change the channel to one that no other AP is using (or at least a channel that has a lower level of interference) in order to give the connected stations a minimum degree of channel interference.

13.2 DCS Commands

See Section 10.2 on page 56 for detailed information about how to configure DCS settings in a radio profile.

The following table describes the commands available for dynamic channel selection. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 42 Command Summary: DCS

COMMAND	DESCRIPTION
`dcs now`	Sets the NWA/WAC to scan for and select an available channel immediately.

CHAPTER 14
Wireless Load Balancing

This chapter shows you how to configure wireless load balancing.

14.1 Wireless Load Balancing Overview

Wireless load balancing is the process whereby you limit the number of connections allowed on an wireless access point (AP) or you limit the amount of wireless traffic transmitted and received on it. Because there is a hard upper limit on the AP's wireless bandwidth, this can be a crucial function in areas crowded with wireless users. Rather than let every user connect and subsequently dilute the available bandwidth to the point where each connecting device receives a meager trickle, the load balanced AP instead limits the incoming connections as a means to maintain bandwidth integrity.

14.2 Wireless Load Balancing Commands

The following table describes the commands available for wireless load balancing. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 43 Command Summary: Load Balancing

COMMAND	DESCRIPTION
`[no] load-balancing kickout`	Enables an overloaded AP to disconnect ("kick") idle clients or clients with noticeably weak connections.
`load-balancing mode {station | traffic | smart-classroom}`	Enables load balancing based on either number of stations (also known as wireless clients) or wireless traffic on an AP. *station* or *traffic*: once the threshold is crossed (either the maximum station numbers or with network traffic), the NWA/WAC delays association request and authentication request packets from any new station that attempts to make a connection. *smart-classroom*: the NWA/WAC ignores association request and authentication request packets from any new station when the maximum number of stations is reached.
`load-balancing max sta <1..127>`	If load balancing by the number of stations/wireless clients, this sets the maximum number of devices allowed to connect to a load-balanced AP.
`load-balancing traffic level {high | low | medium}`	If load balancing by traffic threshold, this sets the traffic threshold level.

Table 43 Command Summary: Load Balancing (continued)

COMMAND	DESCRIPTION
load-balancing alpha <1..255>	Sets the load balancing alpha value. When the AP is balanced, then this setting delays a client's association with it by this number of seconds. Note: This parameter has been optimized for the NWA/WAC and should not be changed unless you have been specifically directed to do so by Zyxel support.
load-balancing beta <1..255>	Sets the load balancing beta value. When the AP is overloaded, then this setting delays a client's association with it by this number of seconds. Note: This parameter has been optimized for the NWA/WAC and should not be changed unless you have been specifically directed to do so by Zyxel support.
load-balancing sigma <51..100>	Sets the load balancing sigma value. This value is algorithm parameter used to calculate whether an AP is considered overloaded, balanced, or underloaded. It only applies to 'by traffic mode'. Note: This parameter has been optimized for the NWA/WAC and should not be changed unless you have been specifically directed to do so by Zyxel support.
load-balancing timeout <1..255>	Sets the length of time that an AP retains load balancing information it receives from other APs within its range.
load-balancing liInterval <1..255>	Sets the interval in seconds that each AP communicates with the other APs in its range for calculating the load balancing algorithm. Note: This parameter has been optimized for the NWA/WAC and should not be changed unless you have been specifically directed to do so by Zyxel support.
load-balancing kickInterval <1..255>	Enables the kickout feature for load balancing and also sets the kickout interval in seconds. While load balancing is enabled, the AP periodically disconnects stations at intervals equal to this setting. This occurs until the load balancing threshold is no longer exceeded.
show load-balancing config	Displays the load balancing configuration.
show load-balancing loading	Displays the loading status per radio (underload / balance / overload) when you enable the load balancing function.
[no] load-balancing activate	Enables load balancing. Use the no parameter to disable it.

14.2.1 Wireless Load Balancing Examples

The following example shows you how to configure AP load balancing in "by station" mode. The maximum number of stations is set to 1.

```
Router(config)# load-balancing mode station
Router(config)# load-balancing max sta 1
Router(config)# show load-balancing config
load balancing config:
Activate: yes
Kickout: no
Mode: station
Max-sta: 1
Traffic-level: high
Alpha: 5
Beta: 10
Sigma: 60
Timeout: 20
LIInterval: 10
KickoutInterval: 20
```

The following example shows you how to configure AP load balancing in "by traffic" mode. The traffic level is set to low, and "disassociate station" is enabled.

```
Router(config)# load-balancing mode traffic
Router(config)# load-balancing traffic level low
Router(config)# load-balancing kickout
Router(config)# show load-balancing config
load balancing config:
Activate: yes
Kickout: yes
Mode: traffic
Max-sta: 1
Traffic-level: low
Alpha: 5
Beta: 10
Sigma: 60
Timeout: 20
LIInterval: 10
KickoutInterval: 20
```

CHAPTER 15
Bluetooth

This chapter shows you how to configure the Bluetooth advertising settings for the NWA/WAC that supports Bluetooth Low Energy (BLE). Bluetooth Low Energy, which is also known as Bluetooth Smart, transmits less data over a shorter distance and consumes less power than classic Bluetooth.

15.1 Bluetooth Overview

iBeacon is Apple's communication protocol on top of Bluetooth Low Energy wireless technology. Beacons (Bluetooth radio transmitters) or BLE enabled devices broadcast packets to every device around it to announce their presence. Advertising packets contain their iBeacon ID which mainly consists of the UUID, major number, minor number and TX (transmit) power. The ID is used to distinguish beacons in your network.

The universally unique identifier (UUID) is a 128-bit (16-byte) number which can be used to identify a service, a device, a manufacturer or an owner. The 2-byte major number is to identify and distinguish a group, and the 2-byte minor number is to identify and distinguish an individual.

For example, you can set all the beacons in one network to share the same UUID, the beacons in a particular room to use the same major number, and each beacon in the room can have its own minor number.

	NETWORK A		
	ROOM X		**ROOM Y**
	BEACON 1	**BEACON 2**	**BEACON 3**
UUID	EBAECFAF-DFE0-4039-BE5A-F030EED4303C		
Major	10	10	20
Minor	1	2	1

15.2 Bluetooth Commands

The following table describes the commands available for Bluetooth advertising settings. You must use the `configure terminal` command before you can use these commands.

Table 44 Bluetooth Commands

COMMAND	DESCRIPTION
`ble` *slot_name*	Enters the Bluetooth sub-command mode for the specified radio on the NWA/WAC.
`ibeacon index <1..5> no activate`	Disables the specified iBeacon ID.

Table 44 Bluetooth Commands

COMMAND	DESCRIPTION
ibeacon index <1..5> activate	Enables the specified iBeacon ID.
ibeacon index <1..5> uuid *uuid* major <0..65535> minor <0..65535>	Adds a new iBeacon ID to be included in the Bluetooth advertising packets by specifying the UUID, major number and minor number. UUID: Enter 32 hexadecimal digits in the range of "A-F", "a-f" and "0-9", split into five groups separated by hyphens (-). The UUID format is as follows: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx (8-4-4-4-12). Major/minor number: Enter an integer from 0 to 65535.
show ble advertising	Displays the Bluetooth advertising settings (beacon IDs) of the NWA/WAC.
show ble uuid-gen	Displays the UUID that is automatically generated by the NWA/WAC.
show ble status	Displays the NWA/WAC's Bluetooth status and detailed information.

15.2.1 Bluetooth Commands Example

The following example adds a beacon ID and displays the Bluetooth advertising settings.

```
Router(config)# show ble uuid-gen
UUID: 72F3CCD4-2D00-4158-8BA0-AF1A586E92AD
Router(config)# ble slot1
Router(config-ble-slot)# ibeacon index 1 uuid 72F3CCD4-2D00-4158-8BA0-
AF1A586E92AD major 1 minor 1
Router(config-ble-slot)# ibeacon index 1 activate
Router(config-ble-slot)# exit
Router(config)# show ble advertising
Slot  Index  Activate  UUID                                    Major  Minor
=========================================================================
1     1      1         72F3CCD4-2D00-4158-8BA0-AF1A586E92AD  1      1
1     2      0                                                0      0
1     3      0                                                0      0
1     4      0                                                0      0
1     5      0                                                0      0
Router(config)#
```

CHAPTER 16
Certificates

This chapter explains how to use the certificates.

16.1 Certificates Overview

The NWA/WAC can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the NWA/WAC to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

16.2 Certificate Commands

This section describes the commands for configuring certificates.

16.3 Certificates Commands Input Values

The following table explains the values you can input with the `certificate` commands.

Table 45 Certificates Commands Input Values

LABEL	DESCRIPTION
certificate_name	The name of a certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
cn_address	A common name IP address identifies the certificate's owner. Type the IP address in dotted decimal notation.
cn_domain_name	A common name domain name identifies the certificate's owner. The domain name is for identification purposes only and can be any string. The domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods.
cn_email	A common name e-mail address identifies the certificate's owner. The e-mail address is for identification purposes only and can be any string. The e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.
organizational_unit	Identify the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.

Table 45 Certificates Commands Input Values (continued)

LABEL	DESCRIPTION
organization	Identify the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
country	Identify the nation where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
key_length	Type a number to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
password	When you have the NWA/WAC enroll for a certificate immediately online, the certification authority may want you to include a key (password) to identify your certification request. Use up to 31 of the following characters. a-zA-Z0-9;|`~!@#$%^&*()_+\{}':,./<>=-
ca_name	When you have the NWA/WAC enroll for a certificate immediately online, you must have the certification authority's certificate already imported as a trusted certificate. Specify the name of the certification authority's certificate. It can be up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
url	When you have the NWA/WAC enroll for a certificate immediately online, enter the IP address (or URL) of the certification authority server. You can use up to 511 of the following characters. a-zA-Z0-9'()+,/:.=?;!*#@$_%-

16.4 Certificates Commands Summary

The following table lists the commands that you can use to display and manage the NWA/WAC's summary list of certificates and certification requests. You can also create certificates or certification requests. Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

Table 46 ca Commands Summary

COMMAND	DESCRIPTION
ca enroll cmp name *certificate_name* cn-type {ip cn *cn_address*|fqdn cn *cn_domain_name*|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|dsa} key-len *key_length* num <0..99999999> password *password* ca *ca_name* url *url*;	Enrolls a certificate with a CA using Certificate Management Protocol (CMP). The certification authority may want you to include a reference number and key (password) to identify your certification request.
ca enroll scep name *certificate_name* cn-type {ip cn *cn_address*|fqdn cn *cn_domain_name*|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|dsa} key-len *key_length* password *password* ca *ca_name* url *url*	Enrolls a certificate with a CA using Simple Certificate Enrollment Protocol (SCEP). The certification authority may want you to include a key (password) to identify your certification request.
ca generate pkcs10 name *certificate_name* cn-type {ip cn *cn_address*|fqdn cn *cn_domain_name*|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|rsa-sha256|rsa-sha512|dsa|dsa-sha256} key-len *key_length* [extend-key {svr-client-ike |svr-client|svr-ike|svr|client-ike|client |ike}]	Generates a PKCS#10 certification request.

Table 46 ca Commands Summary (continued)

COMMAND	DESCRIPTION
ca generate pkcs12 name *name* password *password*	Generates a PKCS#12 certificate.
ca generate x509 name *certificate_name* cn-type {ip cn *cn_address*|fqdn cn *cn_domain_name*|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|rsa-sha256|rsa-sha512|dsa|dsa-sha256} key-len *key_length* [extend-key {svr-client-ike |svr-client|svr-ike|svr|client-ike|client |ike}]	Generates a self-signed x509 certificate.
ca rename category {local|remote} *old_name new_name*	Renames a local (my certificates) or remote (trusted certificates) certificate.
ca validation *remote_certificate*	Enters the sub command mode for validation of certificates signed by the specified remote (trusted) certificates.
no ca category {local|remote} *certificate_name*	Deletes the specified local (my certificates) or remote (trusted certificates) certificate.
no ca validation *name*	Removes the validation configuration for the specified remote (trusted) certificate.
show ca category {local|remote} name *certificate_name* certpath	Displays the certification path of the specified local (my certificates) or remote (trusted certificates) certificate.
show ca category {local|remote} [name *certificate_name* format {text|pem}]	Displays a summary of the certificates in the specified category (local for my certificates or remote for trusted certificates) or the details of a specified certificate.
show ca validation name *name*	Displays the validation configuration for the specified remote (trusted) certificate.
show ca spaceusage	Displays the storage space in use by certificates.

16.5 Certificates Commands Examples

The following example creates a self-signed X.509 certificate with IP address 10.0.0.58 as the common name. It uses the RSA key type with a 512 bit key. Then it displays the list of local certificates. Finally it deletes the pkcs12request certification request.

```
Router# configure terminal
Router(config)# ca generate x509 name test_x509 cn-type ip cn 10.0.0.58 key-
type rsa key-len 512
Router(config)# show ca category local
certificate: default
  type: SELF
  subject: CN=nwa3160-n_00134905820A
  issuer: CN=nwa3160-n_00134905820A
  status: EXPIRED
  ID: nwa3160-n_00134905820A
    type: EMAIL
  valid from: 1970-01-01 02:09:16 GMT
  valid to: 1989-12-27 02:09:16 GMT
Router(config)# no ca category local pkcs12request
```

CHAPTER 17
System

This chapter provides information on the commands that correspond to what you can configure in the system screens.

17.1 System Overview

Use these commands to configure general NWA/WAC information, the system time and the console port connection speed for a terminal emulation program. They also allow you to configure DNS settings and determine which services/protocols can access which NWA/WAC zones (if any) from which computers.

17.2 Host Name Commands

The following table describes the commands available for the hostname and domain name. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 47 Command Summary: Host Name

COMMAND	DESCRIPTION
`[no] domainname <domain_name>`	Sets the domain name. The `no` command removes the domain name. *domain_name*: This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
`[no] hostname <hostname>`	Sets a descriptive name to identify your NWA/WAC. The `no` command removes the host name.
`show fqdn`	Displays the fully qualified domain name.

17.3 Roaming Group Commands

The following table describes the commands available for the roaming group. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 48 Command Summary: Host Name

COMMAND	DESCRIPTION
`[no] roaming group` *group_name*	Sets the name of the roaming group to which the NWA/WAC belongs. The 802.11k neighbor list a client requests from the NWA/WAC is generated according to the roaming group and RCPI (Received Channel Power Indicator) value of its neighbor APs. When a client wants to roam from the current AP to another, other APs in the same roaming group or not in a roaming group will be candidates for roaming. Neighbor APs in a different roaming group will be excluded from the 802.11k neighbor lists even when the neighbor AP has the best signal strength. If the NWA/WAC's roaming group is not configured, any neighbor APs can be candidates for roaming. The `no` command removes the roaming group name. *group_name*: This name can be up to 31 alphanumeric and @# characters. Dashes and underscores are also allowed. The name should start with a letter or digit.
`show roaming group`	Displays the name of the roaming group to which the NWA/WAC belongs.

17.4 Time and Date

For effective scheduling and logging, the NWA/WAC system time must be accurate. There is also a software mechanism to set the time manually or get the current time and date from an external server.

17.4.1 Date/Time Commands

The following table describes the commands available for date and time setup. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 49 Command Summary: Date/Time

COMMAND	DESCRIPTION
`clock date <`*yyyy-mm-dd*`> time <`*hh:mm:ss*`>`	Sets the new date in year, month and day format manually and the new time in hour, minute and second format.
`[no] clock daylight-saving`	Enables daylight saving. The `no` command disables daylight saving.

Table 49 Command Summary: Date/Time (continued)

COMMAND	DESCRIPTION
[no] clock saving-interval begin {apr|aug|dec|feb|jan|jul|jun|mar|may|nov|oct|sep} {1|2|3|4|last} {fri|mon|sat|sun|thu|tue|wed} *hh:mm* end {apr|aug|dec|feb|jan|jul|jun|mar|may|nov|oct|sep} {1|2|3|4|last} {fri|mon|sat|sun|thu|tue|wed} *hh:mm* offset	Configures the day and time when Daylight Saving Time starts and ends. The no command removes the day and time when Daylight Saving Time starts and ends. offset: a number from 1 to 5.5 (by 0.5 increments)
clock time *hh:mm:ss*	Sets the new time in hour, minute and second format.
[no] clock time-zone {-|+*hh:mm*}	Sets your time zone. The no command removes time zone settings.
[no] ntp	Saves your date and time and time zone settings and updates the data and time every 24 hours. The no command stops updating the data and time every 24 hours.
[no] ntp server {*fqdn*|*w.x.y.z*}	Sets the IP address or URL of your NTP time server. The no command removes time server information.
ntp sync	Gets the time and date from a NTP time server.
show clock date	Displays the current date of your NWA/WAC.
show clock status	Displays your time zone and daylight saving settings.
show clock time	Displays the current time of your NWA/WAC.
show ntp server	Displays time server settings.

17.5 Console Port Speed

This section shows you how to set the console port speed when you connect to the NWA/WAC via the console port using a terminal emulation program. The following table describes the console port commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 50 Command Summary: Console Port Speed

COMMAND	DESCRIPTION
[no] console baud *baud_rate*	Sets the speed of the console port. The no command resets the console port speed to the default (115200). *baud_rate*: 9600, 19200, 38400, 57600 or 115200.
show console	Displays console port speed.

17.6 DNS Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

17.6.1 DNS Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 51 Input Values for General DNS Commands

LABEL	DESCRIPTION
address_object	The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
interface_name	The name of the interface. Ethernet interface: ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your NWA/WAC model. VLAN interface: vlan*x*, *x* = 0 - 511.

The following table describes the commands available for DNS. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 52 Command Summary: DNS

COMMAND	DESCRIPTION
`[no] ip dns server a-record` *`fqdn w.x.y.z`*	Sets an A record that specifies the mapping of a fully qualified domain name (FQDN) to an IP address. The `no` command deletes an A record.
`ip dns server cache-flush`	Clears the DNS server cache.
`[no] ip dns server mx-record` *`domain_name`* `{`*`w.x.y.z`*`|`*`fqdn`*`}`	Sets a MX record that specifies a mail server that is responsible for handling the mail for a particular domain. The `no` command deletes a MX record.
`ip dns server rule {<1..32>|append|insert <1..32>} access-group {ALL|`*`profile_name`*`} zone {ALL|`*`profile_name`*`} action {accept|deny}`	Sets a service control rule for DNS requests.
`ip dns server rule move <1..32> to <1..32>`	Changes the number of a service control rule.
`ip dns server zone-forwarder {<1..32>|append|insert <1..32>} {`*`domain_zone_name`*`|*} user-defined` *`w.x.y.z`* `[private | interface {`*`interface_name`*` | auto}]`	Sets a domain zone forwarder record that specifies a DNS server's IP address. `private | interface`: Use `private` if the NWA/WAC connects to the DNS server through a VPN tunnel. Otherwise, use the `interface` command to set the interface through which the NWA/WAC sends DNS queries to a DNS server. The `auto` means any interface that the NWA/WAC uses to send DNS queries to a DNS server according to the routing rule.
`ip dns server zone-forwarder move <1..32> to <1..32>`	Changes the index number of a zone forwarder record.
`no ip dns server rule <1..32>`	Deletes a service control rule.
`show ip dns server database`	Displays all configured records.
`show ip dns server status`	Displays whether this service is enabled or not.

17.6.2 DNS Command Example

This command sets an A record that specifies the mapping of a fully qualified domain name (www.abc.com) to an IP address (210.17.2.13).

```
Router# configure terminal
Router(config)# ip dns server a-record www.abc.com 210.17.2.13
```

CHAPTER 18
System Remote Management

This chapter shows you how to determine which services/protocols can access which NWA/WAC zones (if any) from which computers.

Note: To allow the NWA/WAC to be accessed from a specified computer using a service, make sure you do not have a service control rule or to-NWA/WAC rule to block that traffic.

18.1 System Timeout

There is a lease timeout for administrators. The NWA/WAC automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

Each user is also forced to log in the NWA/WAC for authentication again when the reauthentication time expires.

18.2 HTTP/HTTPS Commands

The following table describes the commands available for HTTP/HTTPS. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 53 Command Summary: HTTP/HTTPS

COMMAND	DESCRIPTION
`[no] ip http authentication` *auth_method*	Sets an authentication method used by the HTTP/HTTPS server. The `no` command resets the authentication method used by the HTTP/HTTPS server to the factory default (`default`). *auth_method*: The name of the authentication method. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`[no] ip http port <1..65535>`	Sets the HTTP service port number. The `no` command resets the HTTP service port number to the factory default (80).
`[no] ip http secure-port <1..65535>`	Sets the HTTPS service port number. The `no` command resets the HTTPS service port number to the factory default (443).

Table 53 Command Summary: HTTP/HTTPS (continued)

COMMAND	DESCRIPTION
[no] ip http secure-server	Enables HTTPS access to the NWA/WAC web configurator. The no command disables HTTPS access to the NWA/WAC web configurator.
[no] ip http secure-server auth-client	Sets the client to authenticate itself to the HTTPS server. The no command sets the client not to authenticate itself to the HTTPS server.
[no] ip http secure-server cert *certificate_name*	Specifies a certificate used by the HTTPS server. The no command resets the certificate used by the HTTPS server to the factory default (default). *certificate_name*: The name of the certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
[no] ip http secure-server force-redirect	Redirects all HTTP connection requests to a HTTPS URL. The no command disables forwarding HTTP connection requests to a HTTPS URL.
ip http secure-server cipher-suite {*cipher_algorithm*} [*cipher_algorithm*] [*cipher_algorithm*] [*cipher_algorithm*]	Sets the encryption algorithms (up to four) that the NWA/WAC uses for the SSL in HTTPS connections and the sequence in which it uses them. The *cipher_algorithm* can be any of the following. rc4: RC4 (RC4 may impact the NWA/WAC's CPU performance since the NWA/WAC's encryption accelerator does not support it). aes: AES des: DES 3des: Triple DES.
no ip http secure-server cipher-suite {*cipher_algorithm*}	Has the NWA/WAC not use the specified encryption algorithm for the SSL in HTTPS connections.
[no] ip http server	Allows HTTP access to the NWA/WAC web configurator. The no command disables HTTP access to the NWA/WAC web configurator.
show ip http server status	Displays HTTP settings.
show ip http server secure status	Displays HTTPS settings.

18.2.1 HTTP/HTTPS Command Examples

This command sets an authentication method used by the HTTP/HTTPS server to authenticate the client(s).

```
Router# configure terminal
Router(config)# ip http authentication Example
```

This following example sets a certificate named MyCert used by the HTTPS server to authenticate itself to the SSL client.

```
Router# configure terminal
Router(config)# ip http secure-server cert MyCert
```

18.3 SSH

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

18.3.1 SSH Implementation on the NWA/WAC

Your NWA/WAC supports SSH versions 1 and 2 using RSA authentication and four encryption methods (AES, 3DES, Archfour, and Blowfish). The SSH server is implemented on the NWA/WAC for remote management on port 22 (by default).

18.3.2 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the NWA/WAC over SSH.

18.3.3 SSH Commands

The following table describes the commands available for SSH. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 54 Command Summary: SSH

COMMAND	DESCRIPTION
`[no] ip ssh server`	Allows SSH access to the NWA/WAC CLI. The `no` command disables SSH access to the NWA/WAC CLI.
`[no] ip ssh server cert` *certificate_name*	Sets a certificate whose corresponding private key is to be used to identify the NWA/WAC for SSH connections. The `no` command resets the certificate used by the SSH server to the factory default (`default`). *certificate_name*: The name of the certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
`[no] ip ssh server port <1..65535>`	Sets the SSH service port number. The `no` command resets the SSH service port number to the factory default (22).
`[no] ip ssh server v1`	Enables remote management using SSH v1. The `no` command stops the NWA/WAC from using SSH v1.
`show ip ssh server status`	Displays SSH settings.

18.3.4 SSH Command Examples

This command sets a certificate (Default) to be used to identify the NWA/WAC.

```
Router# configure terminal
Router(config)# ip ssh server cert Default
```

18.4 Telnet

You can configure your NWA/WAC for remote Telnet access.

18.5 Telnet Commands

The following table describes the commands available for Telnet. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 55 Command Summary: Telnet

COMMAND	DESCRIPTION
`[no] ip telnet server`	Allows Telnet access to the NWA/WAC CLI. The `no` command disables Telnet access to the NWA/WAC CLI.
`[no] ip telnet server port <1..65535>`	Sets the Telnet service port number. The `no` command resets the Telnet service port number back to the factory default (23).
`show ip telnet server status`	Displays Telnet settings.

18.5.1 Telnet Commands Examples

This command displays Telnet settings.

```
Router# configure terminal
Router(config)# show ip telnet server status
active     : yes
port       : 23
service control:
No.  Zone                        Address                     Action
================================================================================
Router(config)#
```

18.6 Configuring FTP

You can upload and download the NWA/WAC's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

18.6.1 FTP Commands

The following table describes the commands available for FTP. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 56 Command Summary: FTP

COMMAND	DESCRIPTION
`[no] ip ftp server`	Allows FTP access to the NWA/WAC. The `no` command disables FTP access to the NWA/WAC.
`[no] ip ftp server cert` *certificate_name*	Sets a certificate to be used to identify the NWA/WAC. The `no` command resets the certificate used by the FTP server to the factory default.
`[no] ip ftp server port <1..65535>`	Sets the FTP service port number. The `no` command resets the FTP service port number to the factory default (21).
`[no] ip ftp server tls-required`	Allows FTP access over TLS. The `no` command disables FTP access over TLS.
`show ip ftp server status`	Displays FTP settings.

18.6.2 FTP Commands Examples

This command displays FTP settings.

```
Router# configure terminal
Router(config)# show ip ftp server status
active     : yes
port       : 21
certificate: default
TLS        : no
service control:
No.  Zone                      Address                      Action
================================================================================
```

18.7 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your NWA/WAC supports SNMP agent functionality, which allows a manager station to manage and monitor the NWA/WAC through the network. The NWA/WAC supports SNMP version one (v1) and version three (v3).

18.7.1 Supported MIBs

The NWA/WAC supports MIB II that is defined in RFC-1213 and RFC-1215. The NWA/WAC also supports private MIBs (ZYXEL-ES-SMI.MIB, ZYXEL-ES-CAPWAP.MIB, ZYXEL-ES-COMMON.MIB, ZYXEL-ES-HybridAP.MIB, ZYXEL-ES-ProWLAN.MIB, ZYXEL-ES-RFMGMT.MIB and ZYXEL-ES-WIRELESS.MIB) to collect information about CPU and memory usage. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance. You can download the NWA/WAC's MIBs from www.zyxel.com.

18.7.2 SNMP Traps

The NWA/WAC will send traps to the SNMP manager when any one of the following events occurs:

Table 57 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the NWA/WAC is turned on or an agent restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.

18.7.3 SNMP Commands

The following table describes the commands available for SNMP. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 58 Command Summary: SNMP

COMMAND	DESCRIPTION
`[no] snmp-server version <v2c|v3>`	Sets the SNMP version support. The no command removes the SNMP version support.
`[no] snmp-server host {`*`fqdn`*`|`*`w.x.y.z`*`} [`*`community_string`*`]`	Sets the domain name or IP address of the host that receives the SNMP notifications. The no command removes the host that receives the SNMP notifications.
`[no] snmp-server enable traps {wireless|capwap}`	Sets the trap control to receive the wireless/capwap trap notifications. The no command removes the wireless/ capwap trap notifications.
`snmp-server v3user username <`*`username`*`> authentication <none|MD5|SHA> privacy <none|DES|AES> privilege <ro|rw>`	Sets the SNMPv3 user account and its privilege of read-only (ro) or read-write (rw) access.
`no snmp-server v3user username <username>`	The no command removes the SNMPv3 user account.
`show snmp status`	Displays SNMP settings.
`show snmp-server v3user status`	Displays SNMPv3 user status.
`[no] snmp-server`	Allows SNMP access to the NWA/WAC. The no command disables SNMP access to the NWA/WAC.
`[no] snmp-server community `*`community_string`* `{ro|rw}`	Enters up to 64 characters to set the password for read-only (ro) or read-write (rw) access. The no command resets the password for read-only (ro) or read-write (rw) access to the default.
`[no] snmp-server contact `*`description`*	Sets the contact information (of up to 60 characters) for the person in charge of the NWA/WAC. The no command removes the contact information for the person in charge of the NWA/WAC.
`[no] snmp-server enable {informs|traps}`	Enables all SNMP notifications (informs or traps). The no command disables all SNMP notifications (informs or traps).
`[no] snmp-server location `*`description`*	Sets the geographic location (of up to 60 characters) for the NWA/WAC. The no command removes the geographic location for the NWA/WAC.
`[no] snmp-server port <1..65535>`	Sets the SNMP service port number. The no command resets the SNMP service port number to the factory default (161).

CHAPTER 19
AAA Server

This chapter introduces and shows you how to configure the NWA/WAC to use external authentication servers.

19.1 AAA Server Overview

You can use an AAA (Authentication, Authorization, Accounting) server to provide access control to your network.

The following lists the types of authentication server the NWA/WAC supports.

- Local user database

  The NWA/WAC uses the built-in local user database to authenticate administrative users logging into the NWA/WAC's web configurator or network access users logging into the network through the NWA/WAC. You can also use the local user database to authenticate VPN users.

- Directory Service (LDAP/AD)

  LDAP (Lightweight Directory Access Protocol)/AD (Active Directory) is a directory service that is both a directory and a protocol for controlling access to a network. The directory consists of a database specialized for fast information retrieval and filtering activities. You create and store user profile and login information on the external server.

- RADIUS

  RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external or built-in RADIUS server. RADIUS authentication allows you to validate a large number of users from a central location.

19.2 Authentication Server Command Summary

This section describes the commands for authentication server settings.

19.2.1 radius-server Commands

The following table lists the `radius-server` commands you use to set the default RADIUS server.

Table 59 radius-server Commands

COMMAND	DESCRIPTION
`show radius-server`	Displays the default RADIUS server settings.
`[no] radius-server host` *`radius_server`* `auth-port` *`auth_port`*	Sets the RADIUS server address and service port number. Enter the IP address (in dotted decimal notation) or the domain name of a RADIUS server. The `no` command clears the settings.

Table 59 radius-server Commands (continued)

COMMAND	DESCRIPTION
[no] radius-server key *secret*	Sets a password (up to 15 alphanumeric characters) as the key to be shared between the RADIUS server and the NWA/WAC. The no command clears this setting.
[no] radius-server timeout *time*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting.

19.2.2 radius-server Command Example

The following example sets the secret key and timeout period of the default RADIUS server (172.23.10.100) to "87643210" and 80 seconds.

```
Router# configure terminal
Router(config)# radius-server host 172.23.10.100 auth-port 1812
Router(config)# radius-server key 876543210
Router(config)# radius-server timeout 80
Router(config)# show radius-server
host               : 172.23.10.100
authentication port: 1812
key                : 876543210
timeout            : 80
Router(config)#
```

19.2.3 aaa group server ad Commands

The following table lists the aaa group server ad commands you use to configure a group of AD servers.

Table 60 aaa group server ad Commands

COMMAND	DESCRIPTION
clear aaa group server ad [*group-name*]	Deletes all AD server groups or the specified AD server group. Note: You can NOT delete a server group that is currently in use.
show aaa group server ad *group-name*	Displays the specified AD server group settings.
[no] aaa group server ad *group-name*	Sets a descriptive name for an AD server group. Use this command to enter the sub-command mode. The no command deletes the specified server group.
aaa group server ad rename *group-name group-name*	Changes the descriptive name for an AD server group.
aaa group server ad *group-name*	Enter the sub-command mode to configure an AD server group.
[no] server alternative-cn-identifier *uid*	Sets the second type of identifier that the users can use to log in if any. For example "name" or "e-mail address". The no command clears this setting.
[no] server basedn *basedn*	Sets the base DN to point to the AD directory on the AD server group. The no command clears this setting.
[no] server binddn *binddn*	Sets the user name the NWA/WAC uses to log into the AD server group. The no command clears this setting.

Table 60 aaa group server ad Commands (continued)

COMMAND	DESCRIPTION
[no] server cn-identifier *uid*	Sets the user name the NWA/WAC uses to log into the AD server group. The no command clears this setting.
[no] server description *description*	Sets the descriptive information for the AD server group. You can use up to 60 printable ASCII characters. The no command clears the setting.
[no] server group-attribute *group-attribute*	Sets the name of the attribute that the NWA/WAC is to check to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add ext-group-user user objects to identify groups based on these group identifier values. For example you could have an attribute named "memberOf" with values like "sales", "RD", and "management". Then you could also create an ext-group-user user object for each group. One with "sales" as the group identifier, another for "RD" and a third for "management". The no command clears the setting.
[no] server host *ad_server*	Enter the IP address (in dotted decimal notation) or the domain name of an AD server to add to this group. The no command clears this setting.
[no] server password *password*	Sets the bind password (up to 15 alphanumerical characters). The no command clears this setting.
[no] server domain-auth activate	Activates server domain authentication. The no parameter deactivates it.
server domain-auth username [username] password [password]	Sets the user name and password for domain authentication.
server domain-auth realm [realm]	Sets the realm for domain authentication.
[no] server port *port_no*	Sets the AD port number. Enter a number between 1 and 65535. The default is 389. The no command clears this setting.
[no] server search-time-limit *time*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting and set this to the default setting of 5 seconds.
[no] server ssl	Enables the NWA/WAC to establish a secure connection to the AD server. The no command disables this feature.

19.2.4 aaa group server ldap Commands

The following table lists the aaa group server ldap commands you use to configure a group of LDAP servers.

Table 61 aaa group server ldap Commands

COMMAND	DESCRIPTION
clear aaa group server ldap [*group-name*]	Deletes all LDAP server groups or the specified LDAP server group. Note: You can NOT delete a server group that is currently in use.
show aaa group server ldap *group-name*	Displays the specified LDAP server group settings.

Table 61 aaa group server ldap Commands (continued)

COMMAND	DESCRIPTION
[no] aaa group server ldap *group-name*	Sets a descriptive name for an LDAP server group. Use this command to enter the sub-command mode. The no command deletes the specified server group.
aaa group server ldap rename *group-name group-name*	Changes the descriptive name for an LDAP server group.
aaa group server ldap *group-name*	Enter the sub-command mode.
[no] server alternative-cn-identifier *uid*	Sets the second type of identifier that the users can use to log in if any. For example "name" or "e-mail address". The no command clears this setting.
[no] server basedn *basedn*	Sets the base DN to point to the LDAP directory on the LDAP server group. The no command clears this setting.
[no] server binddn *binddn*	Sets the user name the NWA/WAC uses to log into the LDAP server group. The no command clears this setting.
[no] server cn-identifier *uid*	Sets the user name the NWA/WAC uses to log into the LDAP server group. The no command clears this setting.
[no] server description *description*	Sets the descriptive information for the LDAP server group. You can use up to 60 printable ASCII characters. The no command clears this setting.
[no] server group-attribute *group-attribute*	Sets the name of the attribute that the NWA/WAC is to check to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add ext-group-user user objects to identify groups based on these group identifier values. For example you could have an attribute named "memberOf" with values like "sales", "RD", and "management". Then you could also create an ext-group-user user object for each group. One with "sales" as the group identifier, another for "RD" and a third for "management". The no command clears the setting.
[no] server host *ldap_server*	Enter the IP address (in dotted decimal notation) or the domain name of an LDAP server to add to this group. The no command clears this setting.
[no] server password *password*	Sets the bind password (up to 15 characters). The no command clears this setting.
[no] server port *port_no*	Sets the LDAP port number. Enter a number between 1 and 65535. The default is 389. The no command clears this setting.
[no] server search-time-limit *time*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting and set this to the default setting of 5 seconds.
[no] server ssl	Enables the NWA/WAC to establish a secure connection to the LDAP server. The no command disables this feature.

19.2.5 aaa group server radius Commands

The following table lists the `aaa group server radius` commands you use to configure a group of RADIUS servers.

Table 62 aaa group server radius Commands

COMMAND	DESCRIPTION
`clear aaa group server radius` *group-name*	Deletes all RADIUS server groups or the specified RADIUS server group. Note: You can NOT delete a server group that is currently in use.
`show aaa group server radius` *group-name*	Displays the specified RADIUS server group settings.
`[no] aaa group server radius` *group-name*	Sets a descriptive name for the RADIUS server group. The `no` command deletes the specified server group.
`aaa group server radius rename` {*group-name-old*} *group-name-new*	Sets the server group name.
`aaa group server radius` *group-name*	Enter the sub-command mode.
`[no] server description` *description*	Sets the descriptive information for the RADIUS server group. You can use up to 60 printable ASCII characters. The `no` command clears the setting.
`[no] server group-attribute` <1-255>	Sets the value of an attribute that the NWA/WAC is used to determine to which group a user belongs. This attribute's value is called a group identifier. You can add **ext-group-user** user objects to identify groups based on different group identifier values. For example, you could configure attributes 1,10 and 100 and create a **ext-group-user** user object for each of them. The `no` command clears the setting.
`[no] server host` *radius_server*	Enter the IP address (in dotted decimal notation) or the domain name of a RADIUS server to add to this server group. The `no` command clears this setting.
`[no] server key` *secret*	Sets a password (up to 15 alphanumeric characters) as the key to be shared between the RADIUS server(s) and the NWA/WAC. The `no` command clears this setting.
`[no] server timeout` *time*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The `no` command clears this setting and set this to the default setting of 5 seconds.

19.2.6 aaa group server Command Example

The following example creates a RADIUS server group with two members and sets the secret key to "12345678" and the timeout to 100 seconds. Then this example also shows how to view the RADIUS group settings.

```
Router# configure terminal
Router(config)# aaa group server radius RADIUSGroup1
Router(group-server-radius)# server host 192.168.1.100 auth-port 1812
Router(group-server-radius)# server host 172.23.22.100 auth-port 1812
Router(group-server-radius)# server key 12345678
Router(group-server-radius)# server timeout 100
Router(group-server-radius)# exit
Router(config)# show aaa group server radius RADIUSGroup1
key                : 12345678
timeout            : 100
description        :
group attribute    : 11

No.  Host Member                                                    Auth. Port

==========================================================================
1    192.168.1.100                                                    1812

2    172.23.22.100                                                    1812
```

CHAPTER 20
Authentication Objects

This chapter shows you how to select different authentication methods for user authentication using the AAA servers or the internal user database.

20.1 Authentication Objects Overview

After you have created the AAA server objects, you can specify the authentication objects (containing the AAA server information) that the NWA/WAC uses to authenticate users (such as managing through HTTP/HTTPS or Captive Portal).

20.2 aaa authentication Commands

The following table lists the `aaa authentication` commands you use to configure an authentication profile.

Table 63 aaa authentication Commands

COMMAND	DESCRIPTION
`aaa authentication rename` *`profile-name-old profile-name-new`*	Changes the profile name. *`profile-name`*: You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`clear aaa authentication` *`profile-name`*	Deletes all authentication profiles or the specified authentication profile. Note: You can NOT delete a profile that is currently in use.
`show aaa authentication {`*`group-name`*`|default}`	Displays the specified authentication server profile settings.
`[no] aaa authentication` *`profile-name`*	Sets a descriptive name for the authentication profile. The `no` command deletes a profile.
`[no] aaa authentication {`*`profile-name`*`} local`	Creates an authentication profile to authenticate users using the local user database

Table 63 aaa authentication Commands (continued)

COMMAND	DESCRIPTION
[no] aaa authentication default *member1* [*member2*] [*member3*] [*member4*]	Sets the default profile to use the authentication method(s) in the order specified. *member* = group radius, or local. Note: You must specify at least one member for each profile. Each type of member can only be used once in a profile. The no command clears the specified authentication method(s) for the profile.
[no] aaa authentication *profile-name member1* [*member2*] [*member3*] [*member4*]	Sets the profile to use the authentication method(s) in the order specified. *member* = group radius, or local. Note: You must specify at least one member for each profile. Each type of member can only be used once in a profile. The no command clears the specified authentication method(s) for the profile.

20.2.1 aaa authentication Command Example

The following example creates an authentication profile to authenticate users using the local user database.

```
Router# configure terminal
Router(config)# aaa authentication LDAPuser group local
Router(config)# show aaa authentication LDAPuser
No.  Method
================================================================================
0    ldap
1    local
Router(config)#
```

20.3 test aaa Command

The following table lists the `test aaa` command you use to teat a user account on an authentication server.

Table 64 test aaa Command

COMMAND	DESCRIPTION
`test aaa {server|secure-server} {ad|ldap} host {`*`hostname`*`|`*`ipv4-address`*`} [host {`*`hostname`*`|`*`ipv4-address`*`}] port <1..65535> base-dn `*`base-dn-string`*` [bind-dn `*`bind-dn-string`*` password `*`password`*`] login-name-attribute `*`attribute`*` [alternative-login-name-attribute `*`attribute`*`] account `*`account-name`*	Tests whether a user account exists on the specified authentication server.

20.3.1 Test a User Account Command Example

The following example shows how to test whether a user account named userABC exists on the AD authentication server which uses the following settings:

- IP address: 172.16.50.1
- Port: 389
- Base-dn: DC=Zyxel,DC=com
- Bind-dn: zyxel\engineerABC
- Password: abcdefg
- Login-name-attribute: sAMAccountName

The result shows the account exists on the AD server. Otherwise, the NWA/WAC returns an error.

```
Router> test aaa server ad host 172.16.50.1 port 389 base-dn DC=Zyxel,DC=com
bind-dn zyxel\engineerABC password abcdefg login-name-attribute
sAMAccountName account userABC

dn:: Q049MTIzNzco546L5aOr56uRKSxPVT1XaXRoTWFpbCxEQz1aeVhFTCxEQz1jb20=
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn:: MTIzNzco546L5aOr56uRKQ==
sn: User
l: 2341100
-------------------------SNIP!-----------------------------------------
```

CHAPTER 21
File Manager

This chapter covers how to work with the NWA/WAC's firmware, certificates, configuration files, packet trace results, shell scripts and temporary files.

21.1 File Directories

The NWA/WAC stores files in the following directories.

Table 65 FTP File Transfer Notes

DIRECTORY	FILE TYPE	FILE NAME EXTENSION
A	Firmware (upload only)	bin
cert	Non-PKCS#12 certificates	cer
conf	Configuration files	conf
packet_trace	Packet trace results (download only)	
script	Shell scripts	.zysh
tmp	Temporary system maintenance files and crash dumps for technical support use (download only)	

A. After you log in through FTP, you do not need to change directories in order to upload the firmware.

21.2 Configuration Files and Shell Scripts Overview

You can store multiple configuration files and shell script files on the NWA/WAC.

When you apply a configuration file, the NWA/WAC uses the factory default settings for any features that the configuration file does not include. Shell scripts are files of commands that you can store on the NWA/WAC and run when you need them. When you run a shell script, the NWA/WAC only applies the commands that it contains. Other settings do not change.

You can edit configuration files or shell scripts in a text editor and upload them to the NWA/WAC. Configuration files use a .conf extension and shell scripts use a .zysh extension.

These files have the same syntax, which is also identical to the way you run CLI commands manually. An example is shown below.

Figure 11 Configuration File / Shell Script: Example

```
## enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
#configure default radio profile, change 2GHz channel to 11 & Tx output
power # to 50%
wlan-radio-profile default
2g-channel 11
output-power 50%
exit
write
```

While configuration files and shell scripts have the same syntax, the NWA/WAC applies configuration files differently than it runs shell scripts. This is explained below.

Table 66 Configuration Files and Shell Scripts in the NWA/WAC

Configuration Files (.conf)	Shell Scripts (.zysh)
• Resets to default configuration. • Goes into CLI **Configuration** mode. • Runs the commands in the configuration file.	• Goes into CLI **Privilege** mode. • Runs the commands in the shell script.

You have to run the example in Table 11 on page 107 as a shell script because the first command is run in **Privilege** mode. If you remove the first command, you have to run the example as a configuration file because the rest of the commands are executed in **Configuration** mode. (See Section 2.5 on page 21 for more information about CLI modes.)

21.2.1 Comments in Configuration Files or Shell Scripts

In a configuration file or shell script, use "#" or "!" as the first character of a command line to have the NWA/WAC treat the line as a comment.

Your configuration files or shell scripts can use "exit" or a command line consisting of a single "!" to have the NWA/WAC exit sub command mode.

Note: "exit" or "!" must follow sub commands if it is to make the NWA/WAC exit sub command mode.

In the following example lines 1 and 2 are comments. Line 5 exits sub command mode.

```
! this is from Joe
# on 2010/12/05
wlan-ssid-profile default
ssid Joe-AP
qos wmm
security default
!
```

21.2.2 Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the NWA/WAC processes the file line-by-line. The NWA/WAC checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the NWA/WAC finds an error, it stops applying the configuration file or shell script and generates a log.

You can change the way a configuration file or shell script is applied. Include `setenv stop-on-error off` in the configuration file or shell script. The NWA/WAC ignores any errors in the configuration file or shell script and applies all of the valid commands. The NWA/WAC still generates a log for any errors.

21.2.3 NWA/WAC Configuration File Details

You can store multiple configuration files on the NWA/WAC. You can also have the NWA/WAC use a different configuration file without the NWA/WAC restarting.

- When you first receive the NWA/WAC, it uses the **system-default.conf** configuration file of default settings.
- When you change the configuration, the NWA/WAC creates a **startup-config.conf** file of the current configuration.
- The NWA/WAC checks the **startup-config.conf** file for errors when it restarts. If there is an error in the **startup-config.conf** file, the NWA/WAC copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file.
- When the NWA/WAC reboots, if the **startup-config.conf** file passes the error check, the NWA/WAC keeps a copy of the **startup-config.conf** file as the **lastgood.conf** configuration file for you as a back up file. If you upload and apply a configuration file with an error, you can apply **lastgood.conf** to return to a valid configuration.

21.2.4 Configuration File Flow at Restart

If there is not a **startup-config.conf** when you restart the NWA/WAC (whether through a management interface or by physically turning the power off and back on), the NWA/WAC uses the **system-default.conf** configuration file with the NWA/WAC's default settings.

If there is a **startup-config.conf**, the NWA/WAC checks it for errors and applies it. If there are no errors, the NWA/WAC uses it and copies it to the **lastgood.conf** configuration file. If there is an error, the NWA/WAC generates a log and copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file. If there isn't a **lastgood.conf** configuration file or it also has an error, the NWA/WAC applies the **system-default.conf** configuration file.

You can change the way the **startup-config.conf** file is applied. Include the `setenv-startup stop-on-error off` command. The NWA/WAC ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The NWA/WAC still generates a log for any errors.

21.3 File Manager Commands Input Values

The following table explains the values you can input with the file manager commands.

Table 67 File Manager Command Input Values

LABEL	DESCRIPTION
file_name	The name of a file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-).

21.4 File Manager Commands Summary

The following table lists the commands that you can use for file management.

Table 68 File Manager Commands Summary

COMMAND	DESCRIPTION
`apply /conf/`*`file_name.conf`* `[ignore-error] [rollback]`	Has the NWA/WAC use a specific configuration file. You must still use the `write` command to save your configuration changes to the flash ("non-volatile" or "long term") memory. Use this command without specify both `ignore-error` and `rollback`: this is not recommended because it would leave the rest of the configuration blank. If the interfaces were not configured before the first error, the console port may be the only way to access the device. Use `ignore-error` without `rollback`: this applies the valid parts of the configuration file and generates error logs for all of the configuration file's errors. This lets the NWA/WAC apply most of your configuration and you can refer to the logs for what to fix. Use both `ignore-error` and `rollback`: this applies the valid parts of the configuration file, generates error logs for all of the configuration file's errors, and starts the NWA/WAC with a fully valid configuration file. Use `rollback` without `ignore-error`: this gets the NWA/WAC started with a fully valid configuration file as quickly as possible. You can use the "`apply /conf/system-default.conf`" command to reset the NWA/WAC to go back to its system defaults.
`copy {/cert | /conf | /idp | /packet_trace | /script | /tmp}`*`file_name-a.conf`* `{/cert | /conf | /idp | /packet_trace | /script | /tmp}/`*`file_name-b.conf`*	Saves a duplicate of a file on the NWA/WAC from the source file name to the target file name. Specify the directory and file name of the file that you want to copy and the directory and file name to use for the duplicate. Always copy the file into the same directory.
`copy running-config startup-config`	Saves your configuration changes to the flash ("non-volatile" or "long term") memory. The NWA/WAC immediately uses configuration changes made via commands, but if you do not use this command or the write command, the changes will be lost when the NWA/WAC restarts.
`copy running-config /conf/`*`file_name.conf`*	Saves a duplicate of the configuration file that the NWA/WAC is currently using. You specify the file name to which to copy.
`delete {/cert | /conf | /idp | /packet_trace | /script | /tmp}/`*`file_name`*	Removes a file. Specify the directory and file name of the file that you want to delete.

Table 68 File Manager Commands Summary (continued)

COMMAND	DESCRIPTION
dir {/cert | /conf | /idp | /packet_trace | /script | /tmp}	Displays the list of files saved in the specified directory.
rename {/cert | /conf | /idp | /packet_trace | /script | /tmp}/*old-file_name* {/cert | /conf | /idp | /packet_trace | /script | /tmp}/*new-file_name*	Changes the name of a file. Specify the directory and file name of the file that you want to rename. Then specify the directory again followed by the new file name.
rename /script/*old-file_name* /script/*new-file_name*	Changes the name of a shell script.
run /script/*file_name.zysh*	Has the NWA/WAC execute a specific shell script file. You must still use the write command to save your configuration changes to the flash ("non-volatile" or "long term") memory.
show running-config	Displays the settings of the configuration file that the system is using.
setenv-startup stop-on-error off	Has the NWA/WAC ignore any errors in the startup-config.conf file and apply all of the valid commands.
show setenv-startup	Displays whether or not the NWA/WAC is set to ignore any errors in the startup-config.conf file and apply all of the valid commands.
write	Saves your configuration changes to the flash ("non-volatile" or "long term") memory. The NWA/WAC immediately uses configuration changes made via commands, but if you do not use the write command, the changes will be lost when the NWA/WAC restarts.

21.5 File Manager Command Example

This example saves a back up of the current configuration before applying a shell script file.

```
Router(config)# copy running-config /conf/backup.conf
Router(config)# run /script/mac_acl_setup.zysh
```

21.6 FTP File Transfer

You can use FTP to transfer files to and from the NWA/WAC for advanced maintenance and support.

21.6.1 Command Line FTP File Upload

1. Connect to the NWA/WAC.
2. Enter "bin" to set the transfer mode to binary.
3. You can upload the firmware after you log in through FTP. To upload other files, use "cd" to change to the corresponding directory.

4 Use “put” to transfer files from the computer to the NWA/WAC.[1] For example:

In the conf directory, use "put config.conf today.conf” to upload the configuration file (config.conf) to the NWA/WAC and rename it “today.conf”.

"put 1.00(XL.0).bin” transfers the firmware (1.00(XL.0).bin) to the NWA/WAC.

The firmware update can take up to five minutes. Do not turn off or reset the NWA/WAC while the firmware update is in progress! If you lose power during the firmware upload, you may need to refer to Section 21.8 on page 113 to recover the firmware.

21.6.2 Command Line FTP Configuration File Upload Example

The following example transfers a configuration file named tomorrow.conf from the computer and saves it on the NWA/WAC as next.conf.

Note: Uploading a custom signature file named "custom.rules”, overwrites all custom signatures on the NWA/WAC.

Figure 12 FTP Configuration File Upload Example

```
C:\>ftp 192.168.1.2
Connected to 192.168.1.2.
220 FTP Server [192.168.1.2]
User (192.168.1.2:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> cd conf
250 CWD command successful
ftp> bin
200 Type set to I
ftp> put tomorrow.conf next.conf
200 PORT command successful
150 Opening BINARY mode data connection for next.conf
226-Post action ok!!
226 Transfer complete.
ftp: 20231 bytes sent in 0.00Seconds 20231000.00Kbytes/sec.
```

21.6.3 Command Line FTP File Download

1 Connect to the NWA/WAC.

2 Enter “bin” to set the transfer mode to binary.

3 Use “cd” to change to the directory that contains the files you want to download.

4 Use “dir” or “ls” if you need to display a list of the files in the directory.

1. When you upload a custom signature, the NWA/WAC appends it to the existing custom signatures stored in the "custom.rules” file.

5 Use "get" to download files. For example:

"get vlan_setup.zysh vlan.zysh" transfers the vlan_setup.zysh configuration file on the NWA/WAC to your computer and renames it "vlan.zysh."

21.6.4 Command Line FTP Configuration File Download Example

The following example gets a configuration file named today.conf from the NWA/WAC and saves it on the computer as current.conf.

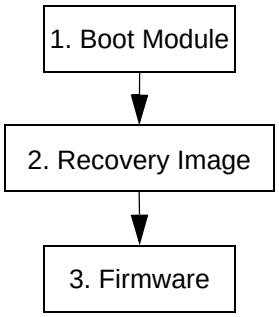
Figure 13 FTP Configuration File Download Example

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 FTP Server [192.168.1.1]
User (192.168.1.1:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> bin
200 Type set to I
ftp> cd conf
250 CWD command successful
ftp> get today.conf current.conf
200 PORT command successful
150 Opening BINARY mode data connection for conf/today.conf
(20220 bytes)
226 Transfer complete.
ftp: 20220 bytes received in 0.03Seconds 652.26Kbytes/sec.
```

21.7 NWA/WAC File Usage at Startup

The NWA/WAC uses the following files at system startup.

Figure 14 NWA/WAC File Usage at Startup



1 The boot module performs a basic hardware test. You cannot restore the boot module if it is damaged. The boot module also checks and loads the recovery image. The NWA/WAC notifies you if the recovery image is damaged.

2 The recovery image checks and loads the firmware. The NWA/WAC notifies you if the firmware is damaged.

21.8 Notification of a Damaged Recovery Image or Firmware

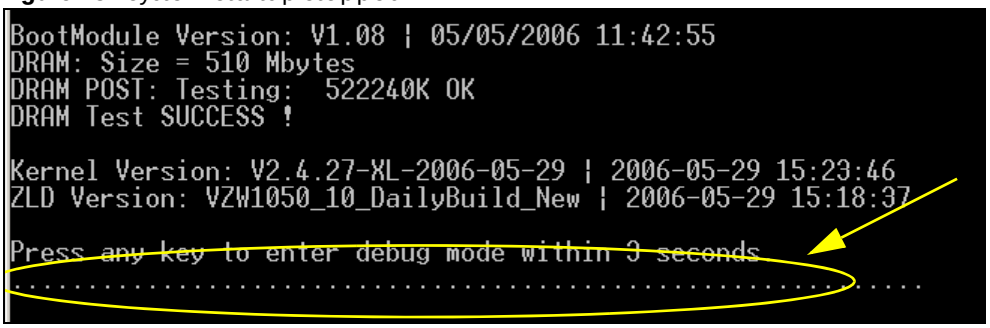
The NWA/WAC's recovery image and/or firmware could be damaged, for example by the power going off during a firmware upgrade. This section describes how the NWA/WAC notifies you of a damaged recovery image or firmware file. Use this section if your device has stopped responding for an extended period of time and you cannot access or ping it. Note that the NWA/WAC does not respond while starting up. It takes less than five minutes to start up with the default configuration, but the start up time increases with the complexity of your configuration.

1 Use a console cable and connect to the NWA/WAC via a terminal emulation program (such as HyperTerminal). Your console session displays the NWA/WAC's startup messages. If you cannot see any messages, check the terminal emulation program's settings (see Section 2.2.1 on page 18) and restart the NWA/WAC.

2 The system startup messages display followed by "Press any key to enter debug mode within 3 seconds."

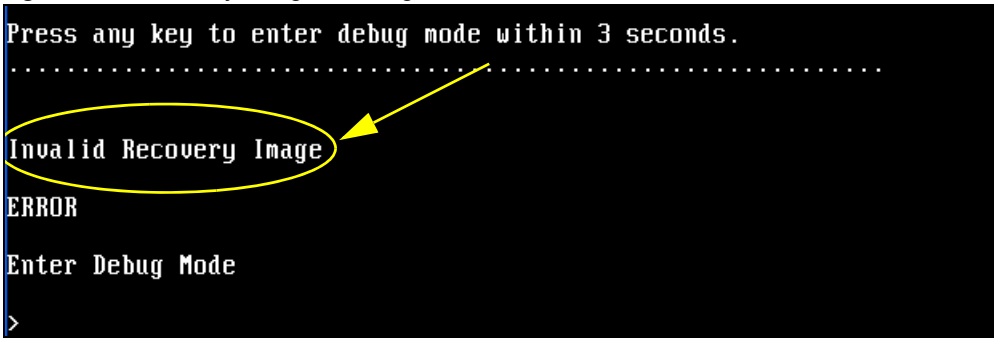
Note: Do not press any keys at this point. Wait to see what displays next.

Figure 15 System Startup Stopped



3 If the console session displays "Invalid Firmware", or "Invalid Recovery Image", or the console freezes at "Press any key to enter debug mode within 3 seconds" for more than one minute, go to Section 21.9 on page 114 to restore the recovery image.

Figure 16 Recovery Image Damaged



4 If "Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file" displays on the screen, the firmware file is damaged. Use the procedure in Section 21.10 on page 115 to restore it. If the message does not display, the firmware is OK and you do not need to use the firmware recovery procedure.

Figure 17 Firmware Damaged

```
Building ...

Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file.
```

21.9 Restoring the Recovery Image

This procedure requires the NWA/WAC's recovery image. Download the firmware package from www.zyxel.com and unzip it. The recovery image uses a .ri extension, for example, "1.01(XL.0)C0.ri". Do the following after you have obtained the recovery image file.

Note: You only need to use this section if you need to restore the recovery image.

1 Restart the NWA/WAC.

2 When "Press any key to enter debug mode within 3 seconds." displays, press a key to enter debug mode.

Figure 18 Enter Debug Mode

```
BootModule Version: V1.011 | 2007-03-30 12:22:57
DRAM: Size = 510 Mbytes
DRAM POST: Testing:  522240K OK
DRAM Test SUCCESS !

Kernel Version: V2.4.27-kernel-2006-08-21 | 2006-08-21 19:54:00
ZLD Version: V1.01(XL.0) | 2006-09-11 17:41:56

Press any key to enter debug mode within 3 seconds.
.............................
Enter Debug Mode

> 
```

3 Enter atuk to initialize the recovery process.If the screen displays "ERROR", enter atur to initialize the recovery process.

Note: You only need to use the atuk or atur command if the recovery image is damaged.

Figure 19 atuk Command for Restoring the Recovery Image

```
> atuk
This command is for restoring the "recovery image" (xxx.ri).
Use This command only when
1) the console displays "Invalid Recovery Image" or
2) the console freezes at "Press any key to enter debug mode within 3 seconds"
   for more than one minute.

Note:
Please exit this command immediately if you do not need to restore the
"recovery image".

Do you want to start the recovery process (Y/N)? (default N)
```

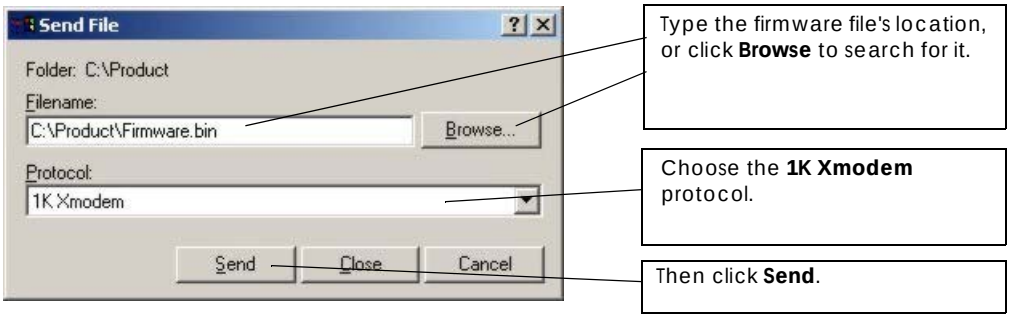
4 Enter Y and wait for the “Starting XMODEM upload” message before activating XMODEM upload on your terminal.

Figure 20 Starting Xmodem Upload

```
Do you want to start the recovery process (Y/N)? (default N)
Starting XMODEM upload (CRC mode)....
C
```

5 This is an example Xmodem configuration upload using HyperTerminal. Click **Transfer**, then **Send File** to display the following screen.

Figure 21 Example Xmodem Upload



6 Wait for about three and a half minutes for the Xmodem upload to finish.

Figure 22 Recovery Image Upload Complete

```
Total  1867264 bytes received.
programming ..........................................................
..........................................................
..........................................................
..........................................................
..........................................................
..........................................................

OK


> _
```

7 Enter `atgo`. The NWA/WAC starts up. If “Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file” displays on the screen, the firmware file is damaged and you need to use the procedure in Section 21.10 on page 115 to recover the firmware.

Figure 23 atgo Debug Command

```
> atgo
Booting...
```

21.10 Restoring the Firmware

This procedure requires the NWA/WAC’s firmware. Download the firmware package from www.zyxel.com and unzip it. The firmware file uses a .bin extension, for example, "1.01(XL.0)C0.bin". Do the following after you have obtained the firmware file.

Note: This section is not for normal firmware uploads. You only need to use this section if you need to recover the firmware.

1 Connect your computer to the NWA/WAC's port **1** (only port **1** can be used).

2 The NWA/WAC's FTP server IP address for firmware recovery is 192.168.1.1, so set your computer to use a static IP address from 192.168.1.2 ~192.168.1.254.

3 Use an FTP client on your computer to connect to the NWA/WAC. For example, in the Windows command prompt, type `ftp 192.168.1.1`. Keep the console session connected in order to see when the firmware recovery finishes.

4 Hit enter to log in anonymously.

5 Set the transfer mode to binary (type `bin`).

6 Transfer the firmware file from your computer to the NWA/WAC. Type `put` followed by the path and name of the firmware file. This examples uses `put e:\ftproot\ZLD FW \1.01(XL.0)C0.bin`.

Figure 24 FTP Firmware Transfer Command

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220-=(<*>)=-.:. (( Welcome to PureFTPd 1.0.11 )) .:.-=(<*>)=-
220-You are user number 1 of 50 allowed
220-Local time is now 21:33 and the load is 0.01. Server port: 21.
220-Only anonymous FTP is allowed here
220 You will be disconnected after 15 minutes of inactivity.
User (192.168.1.1:(none)):
230 Anonymous user logged in
ftp> bi
200 TYPE is now 8-bit binary
ftp> put E:\ftproot\ZLD_FW\100XL0c0\1.00(XL.0)C0.bin_
```

7 Wait for the file transfer to complete.

Figure 25 FTP Firmware Transfer Complete

```
200 PORT command successful
150 Connecting to port 1564
226-87.0 Mbytes free disk space
226-File successfully transferred
226 3.231 seconds (measured here), 10.83 Mbytes per second
ftp: 36708858 bytes sent in 3.23Seconds 11350.91Kbytes/sec.
ftp> _
```

8 After the transfer is complete, "Firmware received" or "ZLD-current received" displays. Wait (up to four minutes) while the NWA/WAC recovers the firmware.

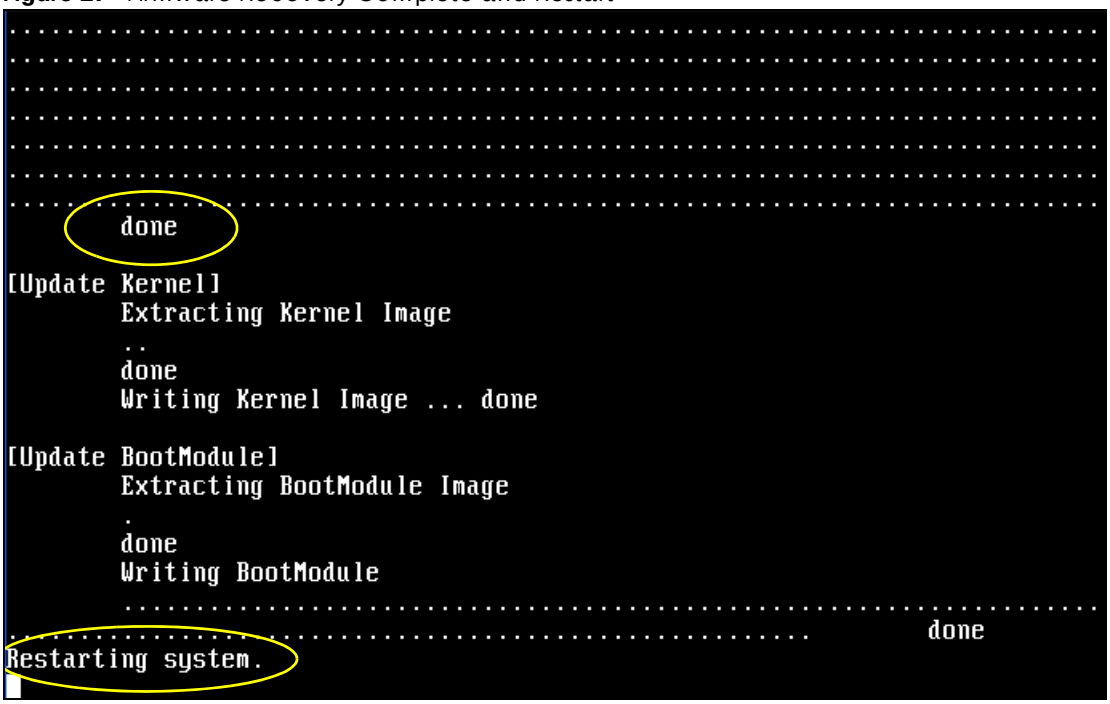
Figure 26 Firmware Received and Recovery Started

```
Firmware received ...

[Update Filesystem]
       Updating Code
       ..
```

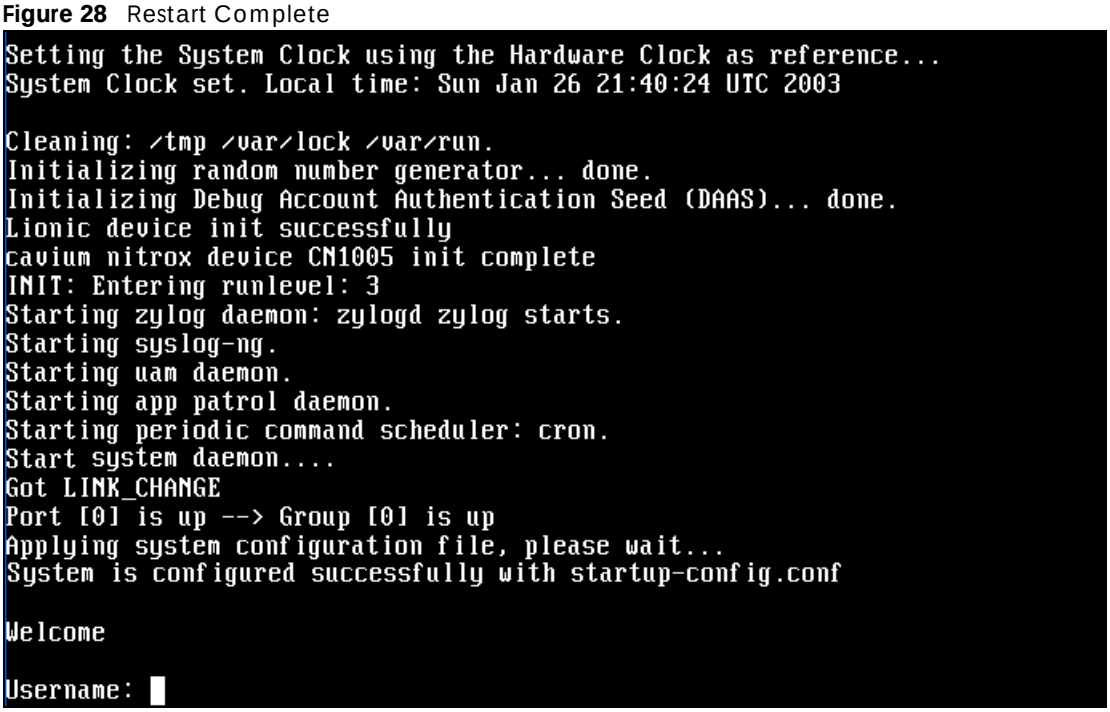
9 The console session displays "done" when the firmware recovery is complete. Then the NWA/WAC automatically restarts.

Figure 27 Firmware Recovery Complete and Restart



10 The username prompt displays after the NWA/WAC starts up successfully. The firmware recovery process is now complete and the NWA/WAC is ready to use.

Figure 28 Restart Complete



CHAPTER 22
Logs

This chapter provides information about the NWA/WAC's logs.

Note: When the system log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

See Section 1.1.1 on page 12 for the maximum number of system log messages in the NWA/WAC.

22.1 Log Commands Summary

The following table describes the values required for many log commands. Other values are discussed with the corresponding commands.

Table 69 Input Values for Log Commands

LABEL	DESCRIPTION
module_name	The name of the category; kernel, syslog, ... The default category includes debugging messages generated by open source software. The all category includes all messages in all categories.
ap_mac	The Ethernet MAC address for the specified Access Point.
pri	The log priority. Enter one of the following values: alert, crit, debug, emerg, error, info, notice, or warn.
ipv4	The standard version 4 IP address (such as 192.168.1.1).
service	The service object name.
keyword	The keyword search string. You may use up to 63 alphanumeric characters.
log_proto_accept	The log protocol. Enter one of the following values: icmp, tcp, udp, or others.
config_interface	The interface name. Enter up to 15 alphanumeric characters, including hyphens and underscores.

The following sections list the logging commands.

22.1.1 Log Entries Commands

This table lists the commands to look at log entries.

Table 70 logging Commands: Log Entries

COMMAND	DESCRIPTION
show logging entries [priority *pri*] [category *module_name*] [srcip *ip*] [dstip *ip*] [service *service_name]* [begin <1..1024> end <1..1024>] [keyword *keyword*]	Displays the selected entries in the system log. PRI: alert | crit | debug | emerg | error | info | notice | warn *keyword*: You can use alphanumeric and ()+/ :=?!*#@$_%- characters, and it can be up to 63 characters long.This searches the message, source, destination, and notes fields.
show logging entries field *field* [begin <1..1024> end <1..1024>]	Displays the selected fields in the system log. *field*: time | msg | src | dst | note | pri | cat | all

22.1.2 System Log Commands

This table lists the commands for the system log settings.

Table 71 logging Commands: System Log Settings

COMMAND	DESCRIPTION
show logging status system-log	Displays the current settings for the system log.
logging system-log category *module_name* {disable | level normal | level all}	Specifies what kind of information, if any, is logged in the system log and debugging log for the specified category.
[no] logging system-log suppression interval <10..600>	Sets the log consolidation interval for the system log. The no command sets the interval to ten.
[no] logging system-log suppression	Enables log consolidation in the system log. The no command disables log consolidation in the system log.
[no] connectivity-check continuous-log activate	Has the NWA/WAC generate a log for each connectivity check. The no command has the NWA/WAC only log the first connectivity check.
show connectivity-check continuous-log status	Displays whether or not the NWA/WAC generates a log for each connectivity check.
clear logging system-log buffer	Clears the system log.

22.1.2.1 System Log Command Examples

The following command displays the current status of the system log.

```
Router# configure terminal
Router(config)# show logging status system-log
18 events logged
suppression active  : yes
suppression interval: 10
category settings   :
    user              : normal , zysh              : normal ,
    built-in-service  : normal , system            : normal ,
    system-monitoring : no     , connectivity-check: normal ,
    device-ha         : normal , pki               : normal ,
    interface         : normal , interface-statistics: no     ,
    traffic-log       : no     , file-manage       : normal ,
    wlan              : normal , daily-report      : normal ,
    dhcp              : normal , default           : all    ,
    capwap            : normal , wlan-monitor      : normal ,
    wlan-rogueap      : normal , wlan-frame-capture: normal ,
    wlan-dcs          : normal , wlan-load-balancing: normal ,
```

22.1.3 Debug Log Commands

This table lists the commands for the debug log settings.

Table 72 logging Commands: Debug Log Settings

COMMAND	DESCRIPTION
`show logging debug status`	Displays the current settings for the debug log.
`show logging debug entries [priority pri] [category module_name] [srcip ip] [dstip ip] [service service_name] [begin <1..1024> end <1..1024>] [keyword keyword]`	Displays the selected entries in the debug log. *pri*: alert | crit | debug | emerg | error | info | notice | warn *keyword*: You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 63 characters long.This searches the message, source, destination, and notes fields.
`show logging debug entries field field [begin <1..1024> end <1..1024>]`	Displays the selected fields in the debug log. *field*: time | msg | src | dst | note | pri | cat | all
`[no] logging debug suppression`	Enables log consolidation in the debug log. The no command disables log consolidation in the debug log.
`[no] logging debug suppression interval <10..600>`	Sets the log consolidation interval for the debug log. The no command sets the interval to ten.
`clear logging debug buffer`	Clears the debug log.

22.1.4 Remote Syslog Server Log Commands

This table lists the commands for the remote syslog server settings.

Table 73 logging Commands: Remote Syslog Server Settings

COMMAND	DESCRIPTION
show logging status syslog	Displays the current settings for the remote servers.
[no] logging syslog <1..4>	Enables the specified remote server. The no command disables the specified remote server.
[no] logging syslog <1..4> address {*ip* | *hostname*}	Sets the URL or IP address of the specified remote server. The no command clears this field. *hostname*: You may up to 63 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.
[no] logging syslog <1..4> {disable | level normal | level all}	Specifies what kind of information, if any, is logged for the specified category.
[no] logging syslog <1..4> facility {local_1 | local_2 | local_3 | local_4 | local_5 | local_6 | local_7}	Sets the log facility for the specified remote server. The no command sets the facility to local_1.
[no] logging syslog <1..4> format {cef | vrpt}	Sets the format of the log information. cef: Common Event Format, syslog-compatible format. vrpt: Zyxel's Vantage Report, syslog-compatible format.

22.1.5 E-mail Profile Log Commands

This table lists the commands for the e-mail profile settings.

Table 74 logging Commands: E-mail Profile Settings

COMMAND	DESCRIPTION
show logging status mail	Displays the current settings for the e-mail profiles.
[no] logging mail <1..2>	Enables the specified e-mail profile. The no command disables the specified e-mail profile.
[no] logging mail <1..2> address {*ip* | *hostname*}	Sets the URL or IP address of the mail server for the specified e-mail profile. The no command clears the mail server field. *hostname*: You may up to 63 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.
logging mail <1..2> sending_now	Sends mail for the specified e-mail profile immediately, according to the current settings.
[no] logging mail <1..2> authentication	Enables SMTP authentication. The no command disables SMTP authentication.

Table 74 logging Commands: E-mail Profile Settings (continued)

COMMAND	DESCRIPTION
[no] logging mail <1..2> authentication username *username* password *password*	Sets the username and password required by the SMTP mail server. The no command clears the username and password fields. *username*: You can use alphanumeric characters, underscores (_), and dashes (-), and it can be up to 31 characters long. *password*: You can use most printable ASCII characters. You cannot use square brackets [ ], double quotation marks (“), question marks (?), tabs or spaces. It can be up to 31 characters long.
[no] logging mail <1..2> {send-log-to | send-alerts-to} *e_mail*	Sets the e-mail address for logs or alerts. The no command clears the specified field. *e_mail*: You can use up to 63 alphanumeric characters, underscores (_), or dashes (-), and you must use the @ character.
[no] logging mail <1..2> subject *subject*	Sets the subject line when the NWA/WAC mails to the specified e-mail profile. The no command clears this field. *subject*: You can use up to 60 alphanumeric characters, underscores (_), dashes (-), or !@#$%*()+=;:',./ characters.
[no] logging mail <1..2> subject-appending {date-time | system-name}	Sets the NWA/WAC to add the system date and time or the system name to the subject when the NWA/WAC mails to the specified e-mail profile. The no command sets the NWA/WAC to not add the system date/time or system name to the subject.
[no] logging mail <1..2> category *module_name* level {alert | all}	Specifies what kind of information is logged for the specified category. The no command disables logging for the specified category.
[no] logging mail <1..2> schedule {full | hourly}	Sets the e-mail schedule for the specified e-mail profile. The no command clears the schedule field.
logging mail <1..2> schedule daily hour <0..23> minute <0..59>	Sets a daily e-mail schedule for the specified e-mail profile.
logging mail <1..2> schedule weekly day *day* hour <0..23> minute <0..59>	Sets a weekly e-mail schedule for the specified e-mail profile. *day*: sun | mon | tue | wed | thu | fri | sat

22.1.5.1 E-mail Profile Command Examples

The following commands set up e-mail log 1.

```
Router# configure terminal
Router(config)# logging mail 1 address mail.zyxel.com.tw
Router(config)# logging mail 1 subject AAA
Router(config)# logging mail 1 authentication username lachang.li password
XXXXXX
Router(config)# logging mail 1 send-log-to lachang.li@zyxel.com.tw
Router(config)# logging mail 1 send-alerts-to lachang.li@zyxel.com.tw
Router(config)# logging mail 1 from lachang.li@zyxel.com.tw
Router(config)# logging mail 1 schedule weekly day mon hour 3 minute 3
Router(config)# logging mail 1
```

22.1.6 Console Port Log Commands

This table lists the commands for the console port settings.

Table 75 logging Commands: Console Port Settings

COMMAND	DESCRIPTION
show logging status console	Displays the current settings for the console log. (This log is not discussed above.)
[no] logging console	Enables the console log. The no command disables the console log.
logging console category *module_name* level {alert | crit | debug | emerg | error | info | notice | warn}	Controls whether or not debugging information for the specified priority is displayed in the console log, if logging for this category is enabled.
[no] logging console category *module_name*	Enables logging for the specified category in the console log. The no command disables logging.

22.1.7 Access Point Logging Commands

This table lists the commands for the Access Point settings.

Note: For the purposes of this device's CLI, Access Points are referred to as WTPs.

Table 76 logging Commands: Access Point Settings

COMMAND	DESCRIPTION
show wtp-logging status system-log [*ap_mac*]	Displays the system log for the specified AP.
show wtp-logging entries [priority *pri*] [category *module_name*] [srcip *ipv4*] [dstip *ipv4*] [service *service*] [srciface *config_interface*] [dstiface *config_interface*] [protocol *log_proto_accept*][begin <1..512> end <1..512>] [keyword *keyword*] [*ap_mac*]	Displays only the specified log entries for the specified AP.
show wtp-logging entries field {srcif|dstif|proto|time|msg|src|dst|note|pri|cat|all} [begin <1..512> end <1..512>] [*ap_mac*]	Displays only log entries for specified fields for the specified AP. You can display a range of field entries from 1-512.
show wtp-logging debug status *ap_mac*	Displays the debug status of the specified AP.
show wtp-logging debug entries [priority *pri*] [category *module_name*] [srcip *ipv4*] [dstip *ipv4*] [service *service*] [srciface *config_interface*] [dstiface *config_interface*] [protocol *log_proto_accept*] [begin <1..512> end <1..512>] [keyword *keyword*] [*ap_mac*]	Display only the specified debug log entries for the specified AP.
show wtp-logging % debug entries field { srcif|dstif|proto |time|msg|src|dst|note|pri|cat|all} [begin <1..1024> end <1..1024>] [*ap_mac*]	Displays only the log entries for the specified fields for the specified AP. You can display a range of field entries from 1-1024.
show wtp-logging status syslog [*ap_mac*]	Displays the logging status for the specified AP's syslog.
show wtp-logging status mail [*ap_mac*]	Displays the logging status for the specified AP's mail log.
show wtp-logging query-log *ap_mac*	Displays the specified AP's query log.
show wtp-logging query-dbg-log *ap_mac*	Displays the specified AP's query debug log.

Table 76 logging Commands: Access Point Settings (continued)

COMMAND	DESCRIPTION
show wtp-logging result-status	Displays the AP logging result status.
show wtp-logging dbg-result-status	Displays the AP logging debug result status.
show wtp-logging category	Displays the AP logging categories.
wtp-logging mail sending_now MAC	Sends the specified AP's mail log.
clear wtp-logging log-buffer MAC	Clears the specified AP's MAC address from the buffer.
[no] wtp-logging syslog *syslog_range* category *module_name* disable	Disables the logging of the specified syslog category.
[no] wtp-logging syslog *syslog_range* category *module_name* level {normal | all}	Enables logging of the specified syslog category and specifies the logging level.
[no] wtp-logging mail *mail_range* category *module_name* level {alert | all}	Enables mail logging on APs for the specified category.
[no] wtp-logging system-log category *module_name* level {normal | all }	Enables system logging on the APs for the specified category.
[no] wtp-logging system-log category *module_name* disable	Disables system logging on the APs for the specified category.
[no] wtp-logging debug suppression	Enables debug logging suppression. Use the no parameter to disable.
[no] wtp-logging debug suppression interval <10..600>	Enables debug logging suppression during the specified interval. Use the no parameter to disable.
[no] wtp-logging console	Enables logging of console activity. Use the no parameter to disable.
[no] wtp-logging console category *module_name* level *pri*	Enables logging of the specified category at the specified priority level.

CHAPTER 23
Reports and Reboot

This chapter provides information about the report associated commands and how to restart the NWA/WAC using commands. It also covers the daily report e-mail feature.

23.1 Report Commands Summary

The following sections list the report and session commands.

23.1.1 Report Commands

This table lists the commands for reports.

Table 77 report Commands

COMMAND	DESCRIPTION
`[no] report`	Begins data collection. The `no` command stops data collection.
`show report status`	Displays whether or not the NWA/WAC is collecting data and how long it has collected data.
`clear report [`*`interface_name`*`]`	Clears the report for the specified interface or for all interfaces.
`show report [`*`interface_name`* `{ip | service | url}]`	Displays the traffic report for the specified interface and controls the format of the report. Formats are: `ip` - traffic by IP address and direction `service` - traffic by service and direction `url` - hits by URL

23.1.2 Report Command Examples

The following commands start collecting data, display the traffic reports, and stop collecting data.

```
Router# configure terminal
Router(config)# show report lan ip
No. IP Address      User                  Amount          Direction
=================================================================
1   192.168.1.4     admin                 1273(bytes)     Outgoing
2   192.168.1.4     admin                 711(bytes)      Incoming
Router(config)# show report lan service
No. Port  Service          Amount          Direction
=================================================================
1   21    ftp              1273(bytes)     Outgoing
2   21    ftp              711(bytes)      Incoming
Router(config)# show report lan url
No. Hit        URL
=================================================================
1   1          140.114.79.60
Router(config)# show report status
Report status: on
Collection period: 0 days 0 hours 0 minutes 18 seconds
```

23.2 Email Daily Report Commands

The following table identifies the values used in some of these commands. Other input values are discussed with the corresponding commands.

Table 78 Input Values for Email Daily Report Commands

LABEL	DESCRIPTION
e_mail	An e-mail address. You can use up to 80 alphanumeric characters, underscores (_), periods (.), or dashes (-), and you must use the @ character.

Use these commands to have the NWA/WAC e-mail you system statistics every day. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 79 Email Daily Report Commands

COMMAND	DESCRIPTION
`show daily-report status`	Displays the e-mail daily report settings.
`daily-report`	Enter the daily report sub-command mode.
`[no] activate`	Turns daily e-mail reports on or off.
`smtp-address {`*`ip`*` | `*`hostname`*`}`	Sets the SMTP mail server IP address or domain name.
`[no] smtp-auth activate`	Enables or disables SMTP authentication.
`smtp-auth username `*`username`*` password `*`password`*	Sets the username and password for SMTP authentication.

Table 79 Email Daily Report Commands (continued)

COMMAND	DESCRIPTION
no smtp-address	Resets the SMTP mail server configuration.
no smtp-auth username	Resets the authentication configuration.
mail-subject set *subject*	Configures the subject of the report e-mails.
no mail-subject set	Clears the configured subject for the report e-mails.
[no] mail-subject append system-name	Determines whether the system name will be appended to the subject of report mail.
[no] mail-subject append date-time	Determine whether the sending date-time will be appended at subject of the report e-mails.
mail-from *e_mail*	Sets the sender value of the report e-mails.
mail-to-1 *e_mail*	Sets to whom the NWA/WAC sends the report e-mails (up to five recipients).
mail-to-2 *e_mail*	See above.
mail-to-3 *e_mail*	See above.
mail-to-4 *e_mail*	See above.
mail-to-5 *e_mail*	See above.
[no] item ap-sta	This command is supported when the NWA/WAC is in standalone mode. Determines whether or not the AP station statistics will be included in the report e-mails.
[no] item ap-traffic	This command is supported when the NWA/WAC is in standalone mode. Determines whether or not the AP traffic statistics will be included in the report e-mails.
[no] item cpu-usage	Determines whether or not CPU usage statistics are included in the report e-mails.
[no] item mem-usage	Determines whether or not memory usage statistics are included in the report e-mails.
[no] item port-usage	Determines whether or not port usage statistics are included in the report e-mails.
[no] item station-count	This command is supported when the NWA/WAC is in standalone mode. Determines whether or not the station statistics are included in the report e-mails.
[no] item wtp-tx	This command is supported when the NWA/WAC is in standalone mode. Determines whether or not the NWA/WAC's outgoing traffic statistics are included in the report e-mails.
[no] item wtp-rx	This command is supported when the NWA/WAC is in standalone mode. Determines whether or not the NWA/WAC's incoming traffic statistics are included in the report e-mails.
smtp-port <1..65535>	Sets the SMTP service port.
no smtp-port	Resets the SMTP service port configuration.

Table 79 Email Daily Report Commands (continued)

COMMAND	DESCRIPTION
smtp-tls {tls|starttls}	Sets how you want communications between the SMTP mail server and the NWA/WAC to be encrypted. tls: to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS). starttls: to upgrade a plain text connection to a secure connection using SSL/TLS.
[no] smtp-tls activate	Encrypts the communications between the SMTP mail server and the NWA/WAC. The no command disables communication encryption.
schedule hour <0..23> minute <00..59>	Sets the time for sending out the report e-mails.
[no] reset-counter	Determines whether or not to clear the report statistics data after successfully sending out a report e-mail.
reset-counter-now	Discards all report data and starts all of the counters over at zero.
send-now	Sends the daily e-mail report immediately. let user actively send out the report e-mails.

23.2.1 Email Daily Report Example

This example sets the NWA/WAC to send a daily report e-mail.

```
Router(config)# daily-report
Router(config-daily-report)# no activate
Router(config-daily-report)# smtp-address example-SMTP-mail-server.com
Router(config-daily-report)# mail-subject set test subject
Router(config-daily-report)# no mail-subject append system-name
Router(config-daily-report)# mail-subject append date-time
Router(config-daily-report)# mail-from my-email@example.com
Router(config-daily-report)# no mail-to-2
Router(config-daily-report)# no mail-to-3
Router(config-daily-report)# mail-to-4 my-email@example.com
Router(config-daily-report)# no mail-to-5
Router(config-daily-report)# smtp-auth activate
Router(config-daily-report)# smtp-auth username 12345 password pass12345
Router(config-daily-report)# schedule hour 13 minutes 57
Router(config-daily-report)# no schedule reset-counter
Router(config-daily-report)# item cpu-usage
Router(config-daily-report)# item mem-usage
Router(config-daily-report)# item port-usage
Router(config-daily-report)# activate
Router(config-daily-report)# exit
Router(config)#
```

This displays the email daily report settings and has the NWA/WAC send the report now.

```
Router(config)# show daily-report  status
email daily report status
=========================
activate: no
scheduled time: 00:00
reset counter: no
smtp address:
smtp port: 25
smtp auth: no
smtp username:
smtp password:
mail subject:
append system name: no
append date time: no
mail from:
mail-to-1:
mail-to-2:
mail-to-3:
mail-to-4:
mail-to-5:
cpu-usage: yes
mem-usage: yes
port-usage: yes
ap-sta: no
ap-traffic: no
Router(config)#
```

23.3 Reboot

Use this to restart the device (for example, if the device begins behaving erratically).

If you made changes in the CLI, you have to use the `write` command to save the configuration before you reboot. Otherwise, the changes are lost when you reboot.

Use the `reboot` command to restart the device.

CHAPTER 24
Session Timeout

24.1 Session Timeout Commands

Use these commands to modify and display the session timeout values. You must use the configure terminal command before you can use these commands.

Table 80 Session Timeout Commands

COMMAND	DESCRIPTION
session timeout {udp-connect <1..300> | udp-deliver <1..300> | icmp <1..300>}	Sets the timeout for UDP sessions to connect or deliver and for ICMP sessions.
session timeout { tcp-close <1..300> | tcp-closewait <1..300> | tcp-established <1..432000> | tcp-finwait <1..300> | tcp-lastack <1..300> | tcp-synrecv <1..300> | tcp-synsent <1..300> | tcp-timewait <1..300> | udp-connect <1..300> | ucp-deliver <1..300> | icmp <1..300> }	Sets the timeout for TCP sessions in the ESTABLISHED, SYN_RECV, FIN_WAIT, SYN_SENT, CLOSE_WAIT, LAST_ACK, or TIME_WAIT state.
show session timeout {icmp | tcp-timewait | udp}	Displays ICMP, TCP, and UDP session timeouts.

24.1.1 Session Timeout Commands Example

The following example sets the UDP session connect timeout to 10 seconds, the UDP deliver session timeout to 15 seconds, and the ICMP timeout to 15 seconds.

```
Router(config)# session timeout udp-connect 10
Router(config)# session timeout udp-deliver 15
Router(config)# session timeout icmp 15
Router(config)# show session timeout udp
UDP session connect timeout: 10 seconds
UDP session deliver timeout: 15 seconds
Router(config)# show session timeout icmp
ICMP session timeout: 15 seconds
```

CHAPTER 25
LEDs

This chapter describes two features that controls the LEDs of your NWA/WAC - Locator and Suppression.

25.1 LED Suppression Mode

The LED Suppression feature allows you to control how the LEDs of your NWA/WAC behave after it's ready. The default LED suppression setting of your AP is different depending on your NWA/WAC model.

Note: When the NWA/WAC is booting or performing firmware upgrade, the LEDs will lit regardless of the setting in LED suppression.

25.2 LED Suppression Commands

Use these commands to set how you want the LEDs to behave after the device is ready. You must use the `configure terminal` command before you can use these commands.

Table 81 LED Suppression Commands

COMMAND	DESCRIPTION
`led_suppress enable`	Sets the LEDs of your NWA/WAC to turn off after it's ready.
`led_suppress disable`	Sets the LEDs to stay lit after the NWA/WAC is ready.
`show led_suppress status`	Displays whether LED suppression mode is enabled or disabled on the NWA/WAC.

25.2.1 LED Suppression Commands Example

The following example activates LED suppression mode and displays the settings..

```
Router(config)# led_suppress enable
Router(config)# show led_suppress status
suppress mode status: Enable
```

25.3 LED Locator

The LED locator feature identifies the location of your WAC among several devices in the network. You can run this feature and set a timer.

25.4 LED Locator Commands

Use these commands to run the LED locator feature. You must use the `configure terminal` command before you can use these commands.

Table 82 LED Locator Commands

COMMAND	DESCRIPTION
`led_locator on`	Enables the LED locator function. It will show the actual location of the WAC between several devices in the network.
`led_locator off`	Disables the LED locator function.
`led_locator blink-timer <1..60>`	Sets a time interval between 1 and 60 minutes to stop the locator LED from blinking.
`show led_locator status`	Displays whether LED locator function is enabled and the timer setting.

25.4.1 LED Locator Commands Example

The following example turns on the LED locator feature and displays the settings.

```
Router(config)# led_locator on
Router(config)# show led_locator status
Locator LED Status : ON
Locator LED Time : 10
```

CHAPTER 26
Antenna Switch

This chapter shows you how to adjust coverage depending on the orientation of the antenna.

26.1 Antenna Switch Overview

On the NWA/WAC that comes with internal antennas and also has an antenna switch, you can adjust coverage depending on the orientation of the antenna for the NWA/WAC radios using the web configurator, the command line interface (CLI) or a physical switch.

Note: With the physical antenna switch, you apply the same antenna orientation settings to both radios. You can set the radios to have different settings while using the web configurator or the command line interface.

Note: The antenna switch is not available in every model. Please check the User's Guide or datasheet, or refer to the product page at www.zyxel.com to see if your NWA/WAC has an antenna switch.

26.2 Antenna Switch Commands

The following table describes the commands available for the antenna switch function. You must use the `configure terminal` command before you can use these commands.

Table 83 Antenna Switch Commands

COMMAND	DESCRIPTION
`antenna config` *`slot_name`* `chain3 {ceiling | wall}`	Adjusts coverage depending on each radio's antenna orientation for better coverage.
`[no] antenna sw-control enable`	Enables the adjustment of coverage depending on the orientation of the antenna for the NWA/WAC radios using the web configurator or the command line interface (CLI). Note: The antenna switch in the web configurator or CLI has priority over the physical antenna switch if you enable software control. The no command disables adjustment through the web configurator or the command line interface (CLI). You can still adjust coverage using a physical antenna switch.
`show antenna status`	Displays whether software control of the antenna switch is enabled and the antenna orientation.
`show wlan all`	Displays the antenna settings for all radios on the NWA/WAC.

26.2.1 Antenna Switch Commands Example

The following example enables software control of the antenna switch and displays the settings.

```
Router(config)# antenna sw-control enable
Router(config)# show antenna status
SW-Control: Enable
Radio 1: Ceiling
Radio 2: Ceiling

Router(config)#
```

CHAPTER 27
Diagnostics

This chapter covers how to use the diagnostics feature.

27.1 Diagnostics Overview

The diagnostics feature provides an easy way for you to generate a file containing the NWA/WAC's configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting.

27.2 Diagnosis Commands

The following table lists the commands that you can use to have the NWA/WAC collect diagnostics information. Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

Table 84 diagnosis Commands

COMMAND	DESCRIPTION
`diag-info collect`	Has the NWA/WAC create a new diagnostic file.
`show diag-info`	Displays the name, size, and creation date (in yyyy-mm-dd hh:mm:ss format) of the diagnostic file.

27.2.1 Diagnosis Commands Example

The following example creates a diagnostic file and displays its name, size, and creation date.

```
Router# configure terminal
Router(config)# diag-info collect
Please wait, collecting information
Router(config)# show diag-info
Filename  : diaginfo-20070423.tar.bz2
File size : 1259 KB
Date      : 2007-04-23 09:55:09
```

CHAPTER 28
Maintenance Tools

Use the maintenance tool commands to check the conditions of other devices through the NWA/WAC. The maintenance tools can help you to troubleshoot network problems.

Here are maintenance tool commands that you can use in privilege mode.

Table 85 Maintenance Tools Commands in Privilege Mode

COMMAND	DESCRIPTION
packet-trace [interface *interface_name*] [ip-proto {<0..255> | *protocol_name* | any}] [src-host {*ip* | *hostname* | any}] [dst-host {*ip* | *hostname* | any}] [port {<1..65535> | any}] [file] [duration <1..3600>] [extension-filter *filter_extension*] traceroute {*ip* | *hostname*}	Sends traffic through the specified interface with the specified protocol, source address, destination address, and/or port number. If you specify file, the NWA/WAC dumps the traffic to /packet_trace/packet_trace_interface. Use FTP to retrieve the files (see Section 21.6 on page 110). If you do not assign the duration, the NWA/WAC keeps dumping traffic until you use Ctrl-C. Use the extension filter to extend the use of this command. *protocol_name*: You can use the name, instead of the number, for some IP protocols, such as tcp, udp, icmp, and so on. The names consist of 1-16 alphanumeric characters, underscores (_), or dashes (-). The first character cannot be a number. *hostname*: You can use up to 252 alphanumeric characters, dashes (-), or periods (.). The first character cannot be a period. *filter_extension*: You can use 1-256 alphanumeric characters, spaces, or '()+,/:=?;!*#@$_%.- characters.
traceroute {*ip* | *hostname*}	Displays the route taken by packets to the specified destination. Use Ctrl+c when you want to return to the prompt.
[no] packet-capture activate	Performs a packet capture that captures network traffic going through the set NWA/WAC's interface(s). Studying these packet captures may help you identify network problems. The no command stops the running packet capture on the NWA/WAC. Note: Use the packet-capture configure command to configure the packet-capture settings before using this command.
packet-capture configure	Enters the sub-command mode.
duration <0..300>	Sets a time limit in seconds for the capture. The NWA/WAC stops the capture and generates the capture file when either this period of time has passed or the file reaches the size specified using the files-size command below. 0 means there is no time limit.

Table 85 Maintenance Tools Commands in Privilege Mode (continued)

COMMAND	DESCRIPTION
file-suffix <*profile_name*>	Specifies text to add to the end of the file name (before the dot and filename extension) to help you identify the packet capture files. Modifying the file suffix also avoids making new capture files that overwrite existing files of the same name. The file name format is "interface name-file suffix.cap", for example "vlan2-packet-capture.cap".
files-size <1..10000>	Specify a maximum size limit in kilobytes for the total combined size of all the capture files on the NWA/WAC, including any existing capture files and any new capture files you generate. The NWA/WAC stops the capture and generates the capture file when either the file reaches this size or the time period specified (using the duration command above) expires. Note: If you have existing capture files you may need to set this size larger or delete existing capture files.
host-ip {*ip-address* | *profile_name* | any>	Sets a host IP address or a host IP address object for which to capture packets. any means to capture packets for all hosts.
host-port <0..65535>	If you set the IP Type to any, tcp, or udp using the ip-type command below, you can specify the port number of traffic to capture.
iface {add | del} {*interface_name* | *virtual_interface_name*}	Adds or deletes an interface or a virtual interface for which to capture packets to the capture interfaces list.
ip-type {icmp | igmp | igrp | pim | ah | esp | vrrp | udp | tcp | any}	Sets the protocol of traffic for which to capture packets. any means to capture packets for all types of traffic.
snaplen <68..1512>	Specifies the maximum number of bytes to capture per packet. The NWA/WAC automatically truncates packets that exceed this size. As a result, when you view the packet capture files in a packet analyzer, the actual size of the packets may be larger than the size of captured packets.
show packet-capture status	Displays whether a packet capture is ongoing.
show packet-capture config	Displays current packet capture settings.

28.0.1 Command Examples

Some packet-trace command examples are shown below.

```
Router# packet-trace duration 3
tcpdump: listening on eth0
19:24:43.239798 192.168.1.10 > 192.168.1.1: icmp: echo request
19:24:43.240199 192.168.1.1 > 192.168.1.10: icmp: echo reply
19:24:44.258823 192.168.1.10 > 192.168.1.1: icmp: echo request
19:24:44.259219 192.168.1.1 > 192.168.1.10: icmp: echo reply
19:24:45.268839 192.168.1.10 > 192.168.1.1: icmp: echo request
19:24:45.269238 192.168.1.1 > 192.168.1.10: icmp: echo reply

6 packets received by filter
0 packets dropped by kernel
```

```
Router# packet-trace interface br0 ip-proto icmp file extension-filter and
src h
ost 192.168.105.133 and dst host 192.168.105.40 -s 500 -n
tcpdump: listening on br0
07:26:51.731558 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:26:52.742666 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:26:53.752774 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:26:54.762887 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)

8 packets received by filter
0 packets dropped by kernel
```

```
Router# packet-trace interface br0 ip-proto icmp file extension-filter -s
500 -n
tcpdump: listening on br0
07:24:07.898639 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:24:07.900450 192.168.105.40 > 192.168.105.133: icmp: echo reply
07:24:08.908749 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:24:08.910606 192.168.105.40 > 192.168.105.133: icmp: echo reply

8 packets received by filter
0 packets dropped by kernel
```

```
Router# traceroute www.zyxel.com
traceroute to www.zyxel.com (203.160.232.7), 30 hops max, 38 byte packets
 1  172.23.37.254  3.049 ms  1.947 ms  1.979 ms
 2  172.23.6.253  2.983 ms  2.961 ms  2.980 ms
 3  172.23.6.1  5.991 ms  5.968 ms  6.984 ms
 4  * * *
```

Here are maintenance tool commands that you can use in configure mode.

Table 86 Maintenance Tools Commands in Configuration Mode

COMMAND	DESCRIPTION
show arp-table	Displays the current Address Resolution Protocol table.
arp IP *mac_address*	Edits or creates an ARP table entry.
no arp *ip*	Removes an ARP table entry.

The following example creates an ARP table entry for IP address 192.168.1.10 and MAC address 01:02:03:04:05:06. Then it shows the ARP table and finally removes the new entry.

```
Router# arp 192.168.1.10 01:02:03:04:05:06
Router# show arp-table
Address                HWtype  HWaddress          Flags Mask           Iface
192.168.1.10            ether   01:02:03:04:05:06   CM                    lan
192.168.1.254           ether   00:04:80:9B:78:00   C                     lan
Router# no arp 192.168.1.10
Router# show arp-table
Address                HWtype  HWaddress          Flags Mask           Iface
192.168.1.10                    (incomplete)                             lan
192.168.1.254           ether   00:04:80:9B:78:00   C                     lan
```

28.0.1.1 Packet Capture Command Example

The following examples show how to configure packet capture settings and perform a packet capture. First you have to check whether a packet capture is running. This example shows no other packet capture is running. Then you can also check the current packet capture settings.

```
Router(config)# show packet-capture status
capture status: off
Router(config)#
Router(config)# show packet-capture config
iface: lan
ip-version: any
proto-type: any
host-port: 0
host-ip: any
file-suffix: lan-packet-capture
snaplen: 1500
duration: 0
file-size: 1000
```

Exit the sub-command mode and have the NWA/WAC capture packets according to the settings you just configured.

```
Router(packet-capture)# exit
Router(config)# packet-capture activate
Router(config)#
```

Manually stop the running packet capturing.

```
Router(config)# no packet-capture activate
Router(config)#
```

Check current packet capture status and list all packet captures the NWA/WAC has performed.

```
Router(config)# show packet-capture status
capture status: off
Router(config)# dir /packet_trace
File Name                                          Size     Modified Time
==========================================================================
lan-packet-capture.cap                           575160   2009-11-24 09:06:59
Router(config)#
```

You can use FTP to download a capture file. Open and study it using a packet analyzer tool (for example, Ethereal or Wireshark).

CHAPTER 29
Watchdog Timer

This chapter provides information about the NWA/WAC's watchdog timers.

29.1 Hardware Watchdog Timer

The hardware watchdog has the system restart if the hardware fails.

The `hardware-watchdog-timer` commands are for support engineers. It is recommended that you not modify the hardware watchdog timer settings.

Table 87 hardware-watchdog-timer Commands

COMMAND	DESCRIPTION
`[no] hardware-watchdog-timer <4..37>`	Sets how long the system's hardware can be unresponsive before resetting. The no command turns the timer off.
`show hardware-watchdog-timer status`	Displays the settings of the hardware watchdog timer.

29.2 Software Watchdog Timer

The software watchdog has the system restart if the core firmware fails.

The `software-watchdog-timer` commands are for support engineers. It is recommended that you not modify the software watchdog timer settings.

Table 88 software-watchdog-timer Commands

COMMAND	DESCRIPTION
`[no] software-watchdog-timer <10..600>`	Sets how long the system's core firmware can be unresponsive before resetting. The no command turns the timer off.
`show software-watchdog-timer status`	Displays the settings of the software watchdog timer.
`show software-watchdog-timer log`	Displays a log of when the software watchdog timer took effect.

29.3 Application Watchdog

The application watchdog has the system restart a process that fails. These are the `app-watchdog` commands.Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

Table 89 app-watchdog Commands

COMMAND	DESCRIPTION
`[no] app-watch-dog activate`	Turns the application watchdog timer on or off.
`[no] app-watch-dog console-print {always|once}`	Display debug messages on the console (every time they occur or once). The no command changes the setting back to the default.
`[no] app-watch-dog interval <5..60>`	Sets how frequently (in seconds) the NWA/WAC checks the system processes. The no command changes the setting back to the default.
`[no] app-watch-dog retry-count <1..5>`	Set how many times the NWA/WAC is to re-check a process before considering it failed. The no command changes the setting back to the default.
`[no] app-watch-dog alert`	Has the NWA/WAC send an alert the user when the system is out of memory or disk space.
`[no] app-watch-dog disk-threshold min <1..100> max <1..100>`	Sets the percentage thresholds for sending a disk usage alert. The NWA/WAC starts sending alerts when disk usage exceeds the maximum (the second threshold you enter). The NWA/WAC stops sending alerts when the disk usage drops back below the minimum threshold (the first threshold you enter). The no command changes the setting back to the default.
`[no] app-watch-dog mem-threshold min` *`threshold_min`* `max` *`threshold_max`*	Sets the percentage thresholds for sending a memory usage alert. The NWA/WAC starts sending alerts when memory usage exceeds the maximum (the second threshold you enter). The NWA/WAC stops sending alerts when the memory usage drops back below the minimum threshold (the first threshold you enter). The no command changes the setting back to the default.
`show app-watch-dog config`	Displays the application watchdog timer settings.
`show app-watch-dog monitor-list`	Display the list of applications that the application watchdog is monitoring.

29.3.1 Application Watchdog Commands Example

The following example displays the application watchdog configuration and lists the processes that the application watchdog is monitoring.

```
Router(config)# show app-watch-dog monitor-list
#app_name       min_process_count       max_process_count(negative integer
means unlimited)
uamd                    1                           -1
policyd                 1                           -1
classify                1                           -1
resd                    1                           -1
zyshd_wd                1                           -1
zylogd                  1                           -1
syslog-ng               1                           -1
zylogger                1                           -1
ddns_had                1                           -1
wdtd                    1                           -1
link_updown             1                           -1
fauthd                  1                           -1
signal_wrapper          1                           -1
capwap_srv      1                       1
capwap_client           1                           -1
Router(config)#
```

List of Commands (Alphabetical)

This section lists the commands and sub-commands in alphabetical order. Commands and subcommands appear at the same level.