ZYXEL
Your Networking Ally

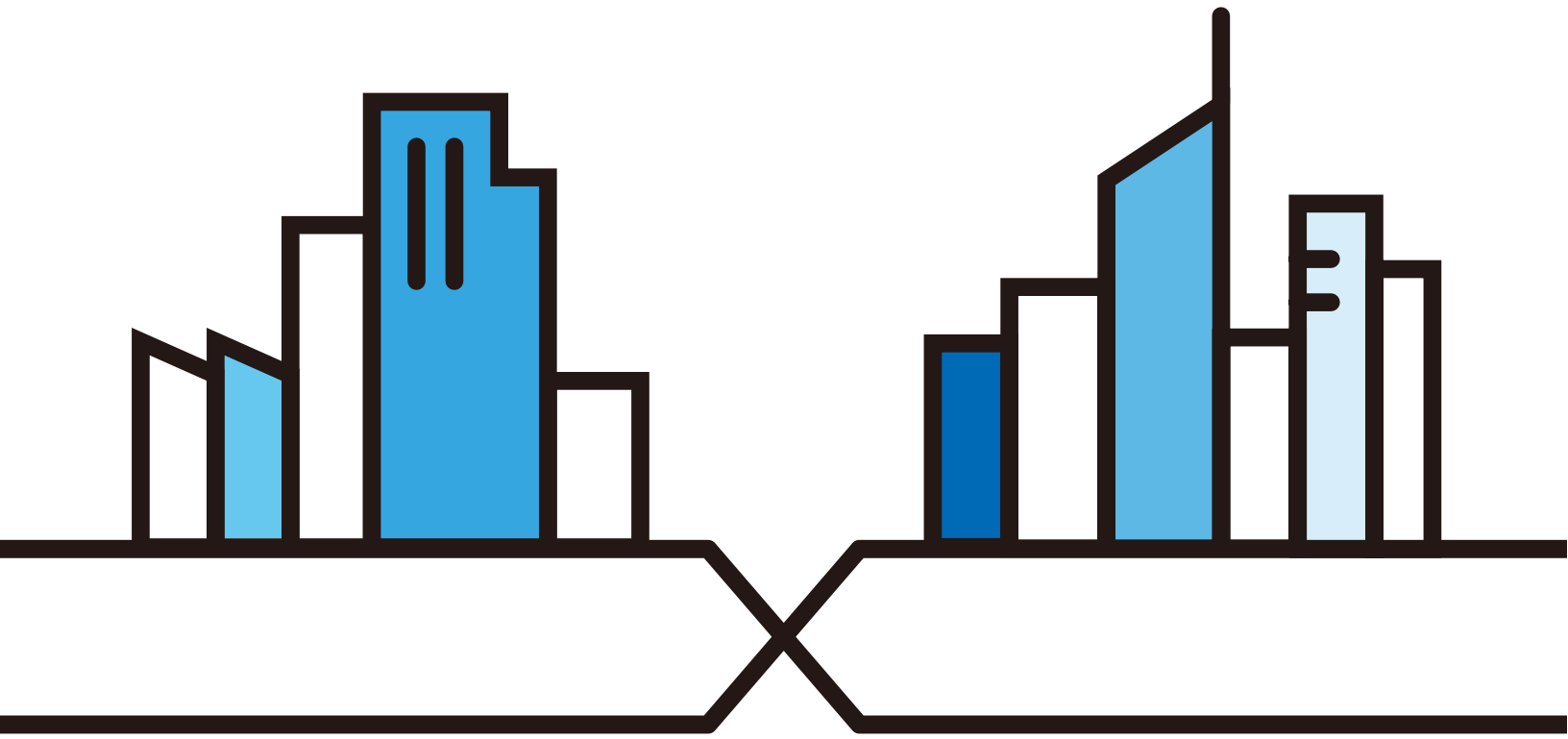
CLI Reference Guide

NXC Series

Wireless LAN Controller

Default Login Details	
IP Address	https://192.168.1.1
User Name	admin
Password	1234

Version 6.00 Edition 1, 1/2020



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 NXC 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 NXC. This guide applies to versions 4.20, 4.21, 4.22, 4.30, 5.00, 5.10, 5.20, 5.30, 5.40, and 6.00 at the time of writing.

How To Use This Guide

1 Read Chapter 1 on page 14 for how to access and use the CLI (Command Line Interface).

2 Read Chapter 2 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 NXC and access the Web Configurator.

- User's Guide

  The User's Guide explains how to use the Web Configurator to configure the NXC.

Note: It is recommended you use the Web Configurator to configure the NXC.

Icons Used in Figures

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

NXC 	Router 	Switch 	Internet 
Server 	Desktop 	Laptop 	AP 

Contents Overview

Table of Contents

CHAPTER 1
Command Line Interface

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

1.1 Overview

If you have problems with your NXC, 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 NXC and possibly render it unusable.

1.1.1 The Configuration File

When you configure the NXC 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 NXC. You can store more than one configuration file on the NXC. However, only one configuration file is used at a time.

You can perform the following with a configuration file:

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

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

1.2 Accessing the CLI

You can access the CLI using a terminal emulation program on a computer connected to the console port, from the web configurator or access the NXC using Telnet or SSH (Secure SHell).

Note: The NXC might force you to log out of your session if reauthentication time, lease time, or idle timeout is reached. See Chapter 23 on page 149 for more information about these settings.

1.2.1 Console Port

The default settings for the console port are as follows.

Table 1 Managing the NXC: Console Port

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

When you turn on your NXC, 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 NXC's.
- No text displays if the speed is set higher than the NXC's.
- If changing your terminal emulation program's speed does not get anything to display, restart the NXC.
- If restarting the NXC does not get anything to display, contact your local customer support.

Figure 1 Console Port Power-on Display

```
Flash: 8 MiB

BootModule Version: V0.9.1 | 2012-12-28 13:01:22
DRAM: Size = 1024 Mbytes



DRAM POST: Testing: 262144K
```

After the initialization, the login screen displays.

Figure 2 Login Screen

```
Welcome to NXC

Username:
```

Enter the user name and password at the prompts.

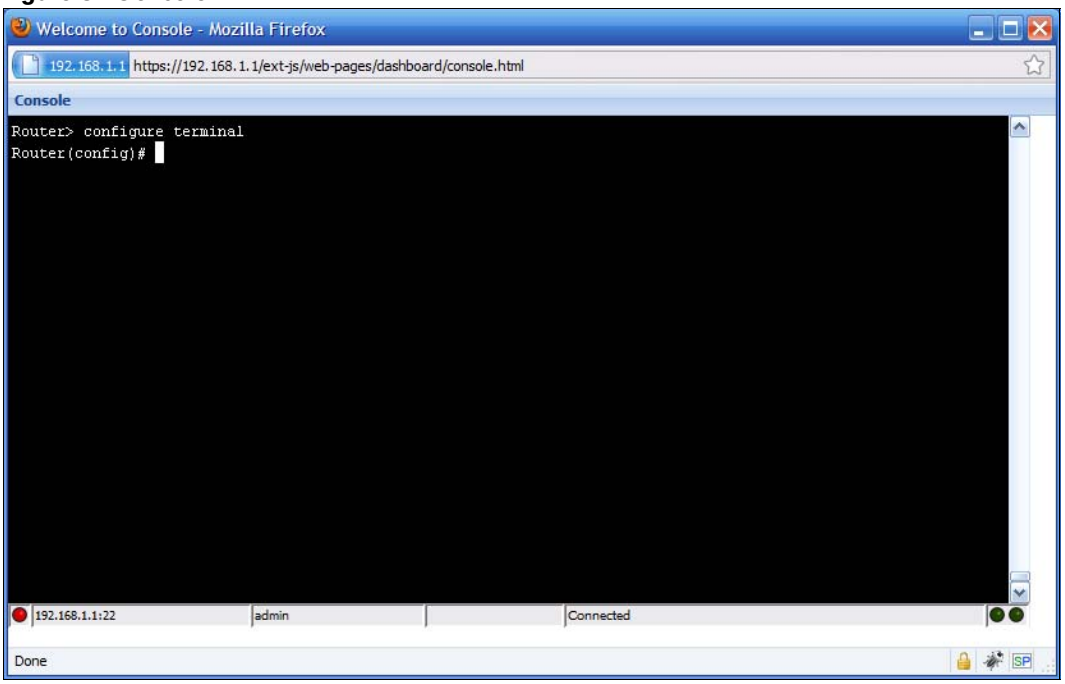
Note: The default login username is **admin** and password is **1234**. The username and password are case-sensitive.

1.2.2 Web Configurator Console

The Console allows you to use CLI commands from directly within the Web Configurator rather than having to use a separate terminal program. In addition to logging in directly to the NXC's CLI, you can also log into other devices on the network through this Console. It uses SSH to establish a connection.

Note: To view the functions in the Web Configurator user interface that correspond directly to specific NXC CLI commands, use the CLI Messages window (described in the User's Guide) in tandem with this one.

Figure 3 Console



The following table describes the elements in this screen.

Table 2 Console

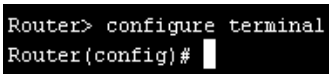
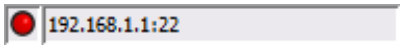
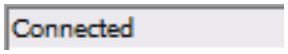
LABEL	DESCRIPTION
Command Line	 Enter commands for the device that you are currently logged into here. If you are logged into the NXC, see the CLI Reference Guide for details on using the command line to configure it.
Device IP Address	 This is the IP address of the device that you are currently logged into.
Logged-In User	 This displays the username of the account currently logged into the NXC through the Console Window. You can log into the Web Configurator with a different account than used to log into the NXC through the Console.

Table 2 Console (continued)

LABEL	DESCRIPTION
Connection Status	 This displays the connection status of the account currently logged in. If you are logged in and connected, then this displays 'Connected'. If you lose the connection, get disconnected, or logout, then this displays 'Not Connected'.
Tx/RX Activity Monitor	 This displays the current upload / download activity. The faster and more frequently an LED flashes, the faster the data connection.

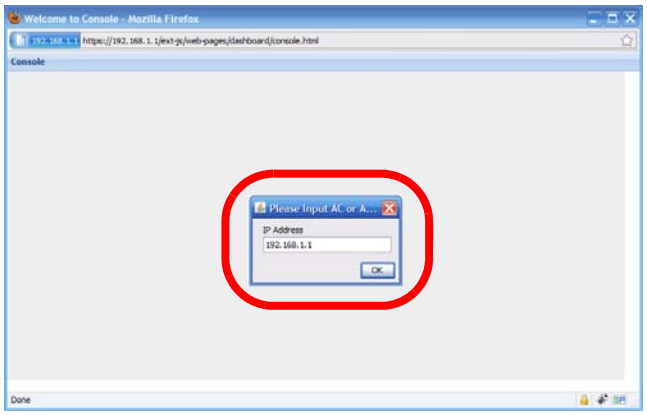
Before you use the Console, ensure that:

- Your web browser of choice allows pop-up windows from the IP address assigned to your NXC.
- Your web browser allows Java programs.
- You are using the latest version of the Java program (http://www.java.com).

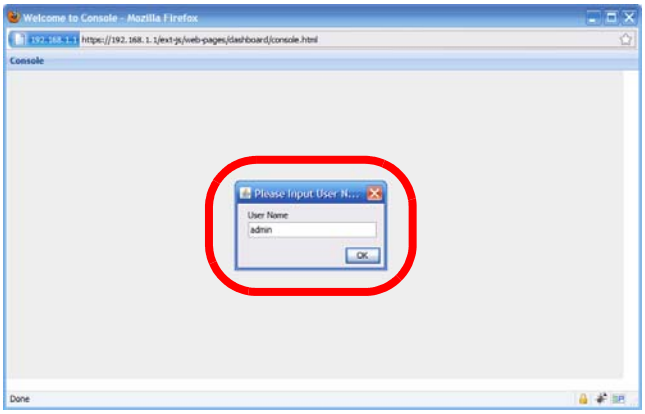
To login in through the Console:

1 Click the **Console** button on the Web Configurator title bar.

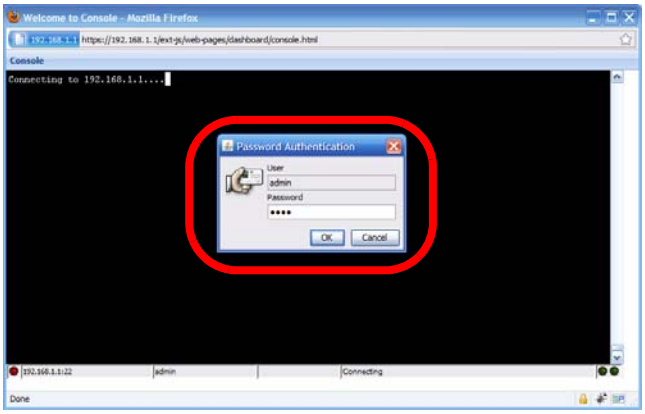
2 Enter the IP address of the NXC and click OK.



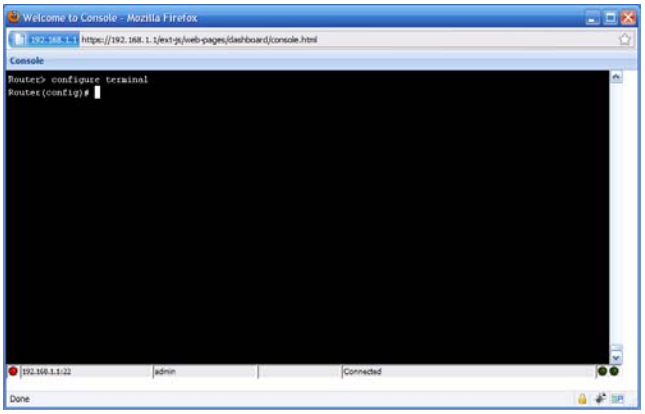
3 Next, enter the user name of the account being used to log into your target device and then click OK.



4 You may be prompted to authenticate your account password, depending on the type of device that you are logging into. Enter the password and click OK.



5 If your login is successful, the command line appears and the status bar at the bottom of the Console updates to reflect your connection state.



1.2.3 Telnet

Use the following steps to Telnet into your NXC.

1 If your computer is connected to the NXC over the Internet, skip to the next step. Make sure your computer IP address and the NXC 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 NXC's IP address. For example, enter `telnet 192.168.1.1` (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.

1.2.4 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 4 SSH Login Example

```
C:\>ssh2 admin@192.168.1.1
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_192.168.1.1.pub
host key for 192.168.1.1, accepted by user Tue Aug 09 2005 07:38:28
admin's password:
Authentication successful.
```

1.3 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 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.

1.4 How Commands Are Explained

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

1.4.1 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.

1.4.2 Command Input Values

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

1.4.3 Command Summary

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

1.4.4 Command Examples

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

1.4.5 Command Syntax

The following conventions are used in this 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.

For example, look at the following command to create a TCP/UDP service object.

`service-object` *`object-name`* `{tcp | udp} {eq <1..65535> | range <1..65535> <1..65535>}`

1. Enter `service-object` exactly as it appears.
2. Enter the name of the object where you see *`object-name`*.
3. Enter `tcp` or `udp`, depending on the service object you want to create.
4. Finally, do one of the following.
   - Enter `eq` exactly as it appears, followed by a number between 1 and 65535.

- Enter `range` exactly as it appears, followed by two numbers between 1 and 65535.

1.4.6 Changing the Password

It is highly recommended that you change the password for accessing the NXC. See Section 23.2 on page 150 for the appropriate commands.

1.5 CLI Modes

You run CLI commands in one of several modes.

Table 3 CLI Modes

	USER	PRIVILEGE	CONFIGURATION	SUB-COMMAND
What **Guest** users can do	Unable to access	Unable to access	Unable to access	Unable to access
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 NXC
How you enter it	Log in to the NXC	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(zone)#`
				`Router(config-if-ge)#`
				`...`

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

See Chapter 23 on page 149 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 NXC 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.

1.6 Shortcuts and Help

1.6.1 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 5 Help: Available Commands Example 1

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

Figure 6 Help: Available Command Example 2

```
Router> show ?
<wlan ap interface>
aaa
access-page
account
ad-server
address-object
------------------[Snip]--------------------
wlan
workspace
zone
Router> show
```

1.6.2 List of Sub-commands or Required User Input

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

Figure 7 Help: Sub-command Information Example

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

Figure 8 Help: Required User Input Example

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

1.6.3 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 NXC 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 NXC displays a list of commands that start with the partial command.

Figure 9 Non-Unique Partial Command Example

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

1.6.4 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 NXC treating it as a help query.

1.6.5 Command History

The NXC 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].

1.6.6 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.

1.6.7 Erase Current Command

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

1.6.8 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".

1.7 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 ge1
Router(config-if-ge)# description
<description>
```

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

Table 4 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 .@_-

Table 4 Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
e-mail	1-64	alphanumeric or .@_-
encryption key	16-64 8-32	"0x" or "0X" + 16-64 hexadecimal values alphanumeric or ;|`~!@#$%^&*()_+\\{}':,./<>=-
file name	0-31	alphanumeric or _-
filter extension	1-256	alphanumeric, spaces, or '()+,/:=?;!*#@$_%.-
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 `~!@#$%^&*()_\-+={}|\;:'<,>./
password: less than 8 chars	1-8	alphanumeric or ;/?:@&=+$\.-_!~*'()%,#$

Table 4 Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
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 ,+
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 (#)

Table 4 Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
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 _-
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

1.8 Saving Configuration Changes

Use the `write` command to save the current configuration to the NXC.

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

1.9 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 2
User and Privilege Modes

This chapter describes how to use these two modes.

2.1 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 NXC uses. See Chapter 23 on page 149 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 5 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.
`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 NXC create a new diagnostic file.
`dir`	P	Lists files in a directory.
`disable`	U/P	Goes from privilege mode to user mode
`enable`	U/P	Goes from user mode to privilege mode

Table 5 User (U) and Privilege (P) Mode Commands (continued)

COMMAND	MODE	DESCRIPTION
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 of 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 NXC. All unsaved changes are lost after the NXC 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.

2.1.1 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 6 Debug Commands

COMMAND SYNTAX	DESCRIPTION	LINUX COMMAND EQUIVALENT
debug alg	FTP/SIP ALG debug commands	
debug app	Application patrol debug command	
debug app show l7protocol (*)	Shows app patrol protocol list	> cat /etc/l7_protocols/protocol.list
debug ca (*)	Certificate debug commands	
debug force-auth (*)	Authentication policy debug commands	
debug gui (*)	Web Configurator related debug commands	
debug hardware (*)	Hardware debug commands	
debug interface	Interface debug commands	
debug interface ifconfig [interface]	Shows system interfaces detail	> ifconfig [interface]
debug ip dns	DNS debug commands	
debug ip virtual-server	Virtual Server (NAT) 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 no registration server (*)	Set the myZyxel.com registration/update server to the official site	
debug policy-route (*)	Policy route debug command	
debug service-register	Service registration debug command	
debug show ipset	Lists the NXC's received cards	
debug show registration-server status	myZyxel.com debug commands	
debug [cmdexec|corefile|ip|kernel|mac-id-rewrite|observer|switch|system|zyinetpkt|zysh-ipt-op] (*)	ZLD internal debug commands	
debug update server (*)	Update server debug command	

CHAPTER 3
Object Reference

This chapter describes how to use object reference commands.

3.1 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 7 `show reference` Commands

COMMAND	DESCRIPTION
`show reference object username [username]`	Displays which configuration settings reference the specified user object.
`show reference object address [profile]`	Displays which configuration settings reference the specified address object.
`show reference object service [profile]`	Displays which configuration settings reference the specified service object.
`show reference object schedule [profile]`	Displays which configuration settings reference the specified schedule object.
`show reference object aaa authentication [default | auth_method]`	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 zone [profile]`	Displays which configuration settings reference the specified zone object.
`show reference object-group username [username]`	Displays which configuration settings reference the specified user group object.
`show reference object-group address [profile]`	Displays which configuration settings reference the specified address group object.
`show reference object-group service [profile]`	Displays which configuration settings reference the specified service group object.
`show reference object-group interface [profile]`	Displays which configuration settings reference the specified trunk object.
`show reference object-group aaa ad [group_name]`	Displays which configuration settings reference the specified AAA AD group object.
`show reference object-group aaa ldap [group_name]`	Displays which configuration settings reference the specified AAA LDAP group object.
`show reference object-group aaa radius [group_name]`	Displays which configuration settings reference the specified AAA RADIUS group object.

Table 7 `show reference` Commands (continued)

COMMAND	DESCRIPTION
`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.

3.1.1 Object Reference Command Example

This example shows how to check which configuration is using an address object named LAN1_SUBNET. For the command output, firewall rule 3 named LAN1-to-NXC is using the address object.

```
Router(config)# show reference object address LAN1_SUBNET

LAN1_SUBNET References:
Category
Rule Priority        Rule Name
Description
================================================================================
Firewall
3                    N/A
LAN1-to-NXC
Router(config)#
```

CHAPTER 4
Status

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

4.1 Status Show Commands

The following table describes the commands available for NXC system status.

Table 8 Status Show Commands

COMMAND	DESCRIPTION
`show sta-info total usage` *timer*	Displays data usage of all connected wireless station(s). *timer*: a period of time (from 1 to 24 hours) over which the traffic flow occurred.
`show boot status`	Displays details about the NXC's startup state.
`show comport status`	Displays whether the console and auxiliary ports are on or off.
`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 fan-speed`	Displays the current fan speed.
`show led status`	Displays the status of each LED on the NXC.
`show mac`	Displays the NXC's MAC address.
`show mem status`	Displays what percentage of the NXC's memory is currently being used.
`show ram-size`	Displays the size of the NXC's on-board RAM.
`show serial-number`	Displays the serial number of this NXC.
`show socket listen`	Displays the NXC's listening ports.
`show socket open`	Displays the ports that are open on the NXC.
`show system uptime`	Displays how long the NXC has been running since it last restarted or was turned on.
`show version`	Displays the NXC's model, firmware and build information.
`show wizard status`	Displays whether the NXC is using the default settings. You can run the wizard only when you log into the Web Configurator for the first time or when you reset the NXC to its default configuration.

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

```
Router(config)# show cpu status
CPU utilization: 0 %
CPU utilization for 1 min: 0 %
CPU utilization for 5 min: 0 %
Router(config)# show disk
;      <cr>   |
Router(config)# show disk
No. Disk                Size(MB)        Usage
================================================================================
1   image               67              83%
2   onboard flash       163             15%
```

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

```
Router(config)# show fan-speed
FAN1(F00)(rpm): limit(hi)=6500, limit(lo)=1400, max=6650, min=6642, avg=6644
FAN2(F01)(rpm): limit(hi)=6500, limit(lo)=1400, max=6809, min=6783, avg=6795
FAN3(F02)(rpm): limit(hi)=6500, limit(lo)=1400, max=6683, min=6666, avg=6674
FAN4(F03)(rpm): limit(hi)=6500, limit(lo)=1400, max=6633, min=6617, avg=6627
Router(config)# show mac
MAC address: 28:61:32:89:37:61-28:61:32:89:37:67
Router(config)# show mem status
memory usage: 39%
Router(config)# show ram-size
ram size: 1024MB
Router(config)# show serial-number
serial number: S132L06160030
```

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   0.0.0.0:2601          0.0.0.0:0             LISTEN
2     tcp   0.0.0.0:2602          0.0.0.0:0             LISTEN
3     tcp   127.0.0.1:10443       0.0.0.0:0             LISTEN
4     tcp   0.0.0.0:2604          0.0.0.0:0             LISTEN
5     tcp   0.0.0.0:80            0.0.0.0:0             LISTEN
6     tcp   127.0.0.1:8085        0.0.0.0:0             LISTEN
7     tcp   1.1.1.1:53            0.0.0.0:0             LISTEN
8     tcp   172.16.13.205:53      0.0.0.0:0             LISTEN
9     tcp   10.0.0.8:53           0.0.0.0:0             LISTEN
10    tcp   172.16.13.240:53      0.0.0.0:0             LISTEN
11    tcp   192.168.1.1:53        0.0.0.0:0             LISTEN
12    tcp   127.0.0.1:53          0.0.0.0:0             LISTEN
13    tcp   0.0.0.0:21            0.0.0.0:0             LISTEN
14    tcp   0.0.0.0:22            0.0.0.0:0             LISTEN
15    tcp   127.0.0.1:953         0.0.0.0:0             LISTEN
16    tcp   0.0.0.0:443           0.0.0.0:0             LISTEN
17    tcp   127.0.0.1:1723        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     tcp   172.16.13.240:22      172.16.13.10:1179     ESTABLISHED
2     udp   127.0.0.1:64002       0.0.0.0:0
3     udp   0.0.0.0:520           0.0.0.0:0
4     udp   0.0.0.0:138           0.0.0.0:0
5     udp   0.0.0.0:138           0.0.0.0:0
6     udp   0.0.0.0:138           0.0.0.0:0
7     udp   0.0.0.0:138           0.0.0.0:0
8     udp   0.0.0.0:138           0.0.0.0:0
9     udp   0.0.0.0:138           0.0.0.0:0
10    udp   0.0.0.0:138           0.0.0.0:0
11    udp   0.0.0.0:32779         0.0.0.0:0
12    udp   192.168.1.1:4500      0.0.0.0:0
13    udp   1.1.1.1:4500          0.0.0.0:0
14    udp   10.0.0.8:4500         0.0.0.0:0
15    udp   172.16.13.205:4500    0.0.0.0:0
16    udp   172.16.13.240:4500    0.0.0.0:0
17    udp   127.0.0.1:4500        0.0.0.0:0
18    udp   127.0.0.1:63000       0.0.0.0:0
19    udp   127.0.0.1:63001       0.0.0.0:0
20    udp   127.0.0.1:63002       0.0.0.0:0
21    udp   0.0.0.0:161           0.0.0.0:0
22    udp   127.0.0.1:63009       0.0.0.0:0
23    udp   192.168.1.1:1701      0.0.0.0:0
24    udp   1.1.1.1:1701          0.0.0.0:0
25    udp   10.0.0.8:1701         0.0.0.0:0
26    udp   172.16.13.205:1701    0.0.0.0:0
27    udp   172.16.13.240:1701    0.0.0.0:0
28    udp   127.0.0.1:1701        0.0.0.0:0
29    udp   127.0.0.1:63024       0.0.0.0:0
30    udp   127.0.0.1:30000       0.0.0.0:0
31    udp   1.1.1.1:53            0.0.0.0:0
32    udp   172.16.13.205:53      0.0.0.0:0
33    udp   10.0.0.8:53           0.0.0.0:0
34    udp   172.16.13.240:53      0.0.0.0:0
35    udp   192.168.1.1:53        0.0.0.0:0
36    udp   127.0.0.1:53          0.0.0.0:0
37    udp   0.0.0.0:67            0.0.0.0:0
38    udp   127.0.0.1:63046       0.0.0.0:0
39    udp   127.0.0.1:65097       0.0.0.0:0
40    udp   0.0.0.0:65098         0.0.0.0:0
41    udp   192.168.1.1:500       0.0.0.0:0
42    udp   1.1.1.1:500           0.0.0.0:0
43    udp   10.0.0.8:500          0.0.0.0:0
44    udp   172.16.13.205:500     0.0.0.0:0
45    udp   172.16.13.240:500     0.0.0.0:0
46    udp   127.0.0.1:500         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           : NXC5200
firmware version: 2.20(AQQ.0)b3
BM version      : 1.08
build date      : 2009-11-21 01:18:06
```

This example shows the current LED states on the NXC. The **SYS** LED lights on and green.

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

CHAPTER 5
Registration

This chapter introduces myzyxel.com and shows you how to register the NXC for IDP/AppPatrol and anti-virus using commands.

5.1 myZyxel.com overview

myZyxel.com is Zyxel's online services center where you can register your NXC and manage subscription services available for the NXC.

Note: You need to create an account before you can register your device and activate the services at myZyxel.com.

You can directly create a myZyxel.com account, register your NXC and activate a service using the **Licensing > Registration** screens. Alternatively, go to http://www.myZyxel.com with the NXC's serial number and LAN MAC address to register it. Refer to the web site's on-line help for details.

Note: To activate a service on a NXC, you need to access myZyxel.com via that NXC.

5.1.1 Subscription Services Available on the NXC

Maximum Number of Managed APs

The NXC is configured to support a certain number of managed APs that can be increased by purchasing additional licenses. The number of APs that the NXC can support can be seen on the NXC User's Guide.

Note: To use a subscription service, you have to register the NXC and activate the corresponding service at myZyxel.com (through the NXC).

5.2 Registration Commands

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

Table 9 Input Values for General Registration Commands

LABEL	DESCRIPTION
user_name	The user name of your myZyxel.com account. You may use six to 20 alphanumeric characters (and the underscore). Spaces are not allowed.
password	The password for the myZyxel.com account. You may use six to 20 alphanumeric characters (and the underscore). Spaces are not allowed.

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

Table 10 Command Summary: Registration

COMMAND	DESCRIPTION
`device-register checkuser user_name`	Checks if the user name exists in the myZyxel.com database.
`device-register username user_name password password [e-mail user@domainname country-code country_code] [reseller-name reseller_name] [reseller-mail user@domainname] [reseller-phone reseller_phonenumber] [vat vat_number]`	Registers the device with an existing account or creates a new account and registers the device at one time. *country_code*: see Table 11 on page 39 *vat_number*: your seller's Value-Added Tax number, if you bought your NXC from Europe.
`service-register checkexpire`	Gets information of all service subscriptions from myZyxel.com and updates the status table.
`service-register service-type standard license-key key_value`	Activates a standard service subscription with the license key.
`show device-register status`	Displays whether the device is registered and account information.
`show service-register status {all|maps}`	Displays service license information.

5.2.1 Command Examples

The following commands allow you to register your device with an existing account or create a new account and register the device at one time, and activate a trial service subscription.

```
Router# configure terminal
Router(config)# device-register username alexctsui password 123456
Router(config)# service-register service-type trial service idp
```

The following command displays the account information and whether the device is registered.

```
Router# configure terminal
Router(config)# show device-register status
username               : alexctsui
password               : 123456
device register status : yes
expiration self check  : no
```

The following command displays the service registration status and type and how many days remain before the service expires.

```
Router# configure terminal
Router(config)# show service-register status all
Service              Status       Type            Count    Expiration
==============================================================================
IDP Signature        Licensed     Standard        N/A      698
Anti-Virus           Licensed     Standard        N/A      698
MAPS                 Licensed     Standard        240      N/A
```

5.3 Country Code

The following table displays the number for each country.

Table 11 Country Codes

COUNTRY CODE	COUNTRY NAME	COUNTRY CODE	COUNTRY NAME
001	Afghanistan	002	Albania
003	Algeria	004	American Samoa
005	Andorra	006	Angola
007	Anguilla	008	Antarctica
009	Antigua & Barbuda	010	Argentina
011	Armenia	012	Aruba
013	Ascension Island	014	Australia
015	Austria	016	Azerbaijan
017	Bahamas	018	Bahrain
019	Bangladesh	020	Barbados
021	Belarus	022	Belgium
023	Belize	024	Benin
025	Bermuda	026	Bhutan
027	Bolivia	028	Bosnia and Herzegovina
029	Botswana	030	Bouvet Island
031	Brazil	032	British Indian Ocean Territory
033	Brunei Darussalam	034	Bulgaria
035	Burkina Faso	036	Burundi
037	Cambodia	038	Cameroon
039	Canada	040	Cape Verde
041	Cayman Islands	042	Central African Republic
043	Chad	044	Chile
045	China	046	Christmas Island
047	Cocos (Keeling) Islands	048	Colombia
049	Comoros	050	Congo, Democratic Republic of the
051	Congo, Republic of	052	Cook Islands
053	Costa Rica	054	Cote d'Ivoire
055	Croatia/Hrvatska	056	Cyprus
057	Czech Republic	058	Denmark
059	Djibouti	060	Dominica
061	Dominican Republic	062	East Timor
063	Ecuador	064	Egypt
065	El Salvador	066	Equatorial Guinea
067	Eritrea	068	Estonia
069	Ethiopia	070	Falkland Islands (Malvina)
071	Faroe Islands	072	Fiji
073	Finland	074	France

Table 11 Country Codes (continued)

COUNTRY CODE	COUNTRY NAME	COUNTRY CODE	COUNTRY NAME
075	France (Metropolitan)	076	French Guiana
077	French Polynesia	078	French Southern Territories
079	Gabon	080	Gambia
081	Georgia	082	Germany
083	Ghana	084	Gibraltar
085	Great Britain	086	Greece
087	Greenland	088	Grenada
089	Guadeloupe	090	Guam
091	Guatemala	092	Guernsey
093	Guinea	094	Guinea-Bissau
095	Guyana	096	Haiti
097	Heard and McDonald Islands	098	Holy See (City Vatican State)
099	Honduras	100	Hong Kong
101	Hungary	102	Iceland
103	India	104	Indonesia
105	Ireland	106	Isle of Man
107	Italy	108	Jamaica
109	Japan	110	Jersey
111	Jordan	112	Kazakhstan
113	Kenya	114	Kiribati
115	Korea, Republic of	116	Kuwait
117	Kyrgyzstan	118	Lao People's Democratic Republic
119	Latvia	120	Lebanon
121	Lesotho	122	Liberia
123	Liechtenstein	124	Lithuania
125	Luxembourg	126	Macau
127	Macedonia, Former Yugoslav Republic	128	Madagascar
129	Malawi	130	Malaysia
131	Maldives	132	Mali
133	Malta	134	Marshall Islands
135	Martinique	136	Mauritania
137	Mauritius	138	Mayotte
139	Mexico	140	Micronesia, Federal State of
141	Moldova, Republic of	142	Monaco
143	Mongolia	144	Montserrat
145	Morocco	146	Mozambique
147	Namibia	148	Nauru
149	Nepal	150	Netherlands
151	Netherlands Antilles	152	New Caledonia
153	New Zealand	154	Nicaragua

Table 11 Country Codes (continued)

COUNTRY CODE	COUNTRY NAME	COUNTRY CODE	COUNTRY NAME
155	Niger	156	Nigeria
157	Niue	158	Norfolk Island
159	Northern Mariana Islands	160	Norway
161	Not Determined	162	Oman
163	Pakistan	164	Palau
165	Panama	166	Papua New Guinea
167	Paraguay	168	Peru
169	Philippines	170	Pitcairn Island
171	Poland	172	Portugal
173	Puerto Rico	174	Qatar
175	Reunion Island	176	Romania
177	Russian Federation	178	Rwanda
179	Saint Kitts and Nevis	180	Saint Lucia
181	Saint Vincent and the Grenadines	182	San Marino
183	Sao Tome and Principe	184	Saudi Arabia
185	Senegal	186	Seychelles
187	Sierra Leone	188	Singapore
189	Slovak Republic	190	Slovenia
191	Solomon Islands	192	Somalia
193	South Africa	194	South Georgia and the South Sandwich Islands
185	Spain	196	Sri Lanka
197	St Pierre and Miquelon	198	St. Helena
199	Suriname	200	Svalbard and Jan Mayen Islands
201	Swaziland	202	Sweden
203	Switzerland	204	Taiwan
205	Tajikistan	206	Tanzania
207	Thailand	208	Togo
209	Tokelau	210	Tonga
211	Trinidad and Tobago	212	Tunisia
213	Turkey	214	Turkmenistan
215	Turks and Caicos Islands	216	Tuvalu
217	US Minor Outlying Islands	218	Uganda
219	Ukraine	220	United Arab Emirates
221	United Kingdom	222	United States
223	Uruguay	224	Uzbekistan
225	Vanuatu	226	Venezuela
227	Vietnam	228	Virgin Islands (British)
229	Virgin Islands (USA)	230	Wallis And Futuna Islands
231	Western Sahara	232	Western Samoa

Table 11 Country Codes (continued)

COUNTRY CODE	COUNTRY NAME	COUNTRY CODE	COUNTRY NAME
233	Yemen	234	Yugoslavia
235	Zambia	236	Zimbabwe

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.
- An interface is bound to one zone at most.
- Many interface can belong to the same zone.
- Layer-3 virtualization (IP alias, for example) is a kind of interface.

Some characteristics do not apply to some types of interfaces.

6.1.1 Types of Interfaces

You can create several types of interfaces in the NXC:

- **Ethernet interfaces** are the foundation for defining other interfaces and network policies. RIP and OSPF are also configured in these interfaces.
- **VLAN interfaces** receive and send tagged frames. The NXC automatically adds or removes the tags as needed.
- **Link Aggregation Group (LAG) interfaces** combine multiple physical Ethernet interfaces into a single logical interface, thus increasing uplink bandwidth and availability in the event a link goes down.

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 NXC model. VLAN interface: vlan*x*, *x* = 0 - 4094
profile_name	The name of the DHCP pool. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
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
`show interface {ethernet | vlan | lag} status`	Displays the connection status of the specified type of interfaces.
`show interface {`*`interface_name`*` | ethernet | vlan | lag | 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 NXC 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.
`[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.

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

COMMAND	DESCRIPTION
[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.
ipv6 dhcp6 [client]	Sets the IPv6 interface to be a DHCPv6 client.
[no] ipv6 dhcp6 rapid-commit	Shortens the DHCPv6 message exchange process from four to two steps to help reduce network traffic. The no command sets the full four-step DHCPv6 message exchange process.
[no] ipv6 dhcp6 address-request	Get this interface's IPv6 address from the DHCPv6 server. The no command has the NXC not get this interface's IPv6 address from the DHCPv6 server.
[no] ipv6 dhcp6-request-object *dhcp6_profile*	For a DHCPv6 client interface, specify 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.
[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.
[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 NXC 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.
interface send statistics interval <15..3600>	Sets how often the NXC sends interface statistics to external servers. For example, a syslog server.

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

COMMAND	DESCRIPTION
`interface-name` *ethernet_interface user_defined_name*	Specifies a name for an Ethernet 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 an Ethernet 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".
`[no] ipv6 activate`	Sets the NXC to support IPv6. The `no` command disables IPv6 support and The NXC discards all IPv6 packets.
`show interface-name`	Displays all Ethernet interface system name and user-defined name mappings.
`show ipv6 interface {`*interface_name* `| all}`	Displays information about the specified IPv6 interface or all IPv6 interfaces.
`show ipv6 nd ra status` *config_interface*	Displays the specified IPv6 interface's IPv6 router advertisement configuration.
`show ipv6 static address` *interface*	Displays the static IPv6 addresses configured on the specified IPv6 interface.
`show ipv6 status`	Displays whether IPv6 support is enabled or disabled.

6.2.1.1 Basic Interface Properties Command Examples

The following commands make Ethernet interface ge1 a DHCP client.

```
Router# configure terminal
Router(config)# interface ge1
Router(config-if)# ip address dhcp
Router(config-if)# exit
```

This example shows how to modify the name of interface ge4 to "VIP". First you have to check the interface system name (ge4 in this example) on the NXC. Then change the name and display the result.

```
Router> show interface-name
No.  System Name     User Defined Name
================================================================================
1    ge1             ge1
2    ge2             ge2
3    ge3             ge3
4    ge4             ge4
5    ge5             ge5
Router> configure terminal
Router(config)# interface-name ge4 VIP
Router(config)# show interface-name
No.  System Name     User Defined Name
================================================================================
1    ge1             ge1
2    ge2             ge2
3    ge3             ge3
4    ge4             VIP
5    ge5             ge5
Router(config)#
```

This example shows how to restart an interface. You can check all interface names on the NXC. Then use either the system name or user-defined name of an interface (ge4 or Customer in this example) to restart it.

```
Router> show interface-name
No.  System Name     User Defined Name
================================================================================
1    ge1             ge1
2    ge2             ge2
3    ge3             ge3
4    ge4             Customer
5    ge5             ge5
Router> configure terminal
Router(config)# interface reset ge4
Router(config)# interface reset Customer
Router(config)#
```

6.2.2 DHCP Setting Commands

This table lists DHCP setting commands. DHCP is based on DHCP pools. Create a DHCP pool if you want to assign a static IP address to a MAC address or if you want to specify the starting IP address and pool size of a range of IP addresses that can be assigned to DHCP clients. There are different commands for each configuration. Afterwards, in either case, you have to bind the DHCP pool to the interface.

Table 14 interface Commands: DHCP Settings

COMMAND	DESCRIPTION
`show ip dhcp dhcp-options`	Shows the DHCP extended option settings.
`show ip dhcp pool [`*`profile_name`*`]`	Shows information about the specified DHCP pool or about all DHCP pools.

Table 14 interface Commands: DHCP Settings (continued)

COMMAND	DESCRIPTION
ip dhcp pool rename *profile_name profile_name*	Renames the specified DHCP pool from the first *profile_name* to the second *profile_name*.
[no] ip dhcp pool *profile_name*	Creates a DHCP pool if necessary and enters sub-command mode. You can use the DHCP pool to create a static entry or to set up a range of IP addresses to assign dynamically. About the sub-command settings: • If you use the host command, the NXC treats this DHCP pool as a static DHCP entry. • If you do not use the host command and use the network command, the NXC treats this DHCP pool as a pool of IP addresses. • If you do not use the host command or the network command, the DHCP pool is not properly configured and cannot be bound to any interface. The no command removes the specified DHCP pool.
show	Shows information about the specified DHCP pool.
	Use the following commands if you want to create a static DHCP entry. If you do not use the host command, the commands that are not in this section have no effect, but you can still set them.
[no] host *ip*	Specifies the static IP address the NXC should assign. Use this command, along with hardware-address, to create a static DHCP entry. Note: The IP address must be in the same subnet as the interface to which you plan to bind the DHCP pool. When this command is used, the NXC treats this DHCP pool like a static entry, regardless of the network setting. The no command clears this field.
[no] hardware-address *mac_address*	Reserves the DHCP pool for the specified MAC address. Use this command, along with host, to create a static DHCP entry. The no command clears this field.
[no] client-identifier *mac_address*	Specifies the MAC address that appears in the DHCP client list. The no command clears this field.
[no] client-name *host_name*	Specifies the host name that appears in the DHCP client list. The no command clears this field. *host_name*: You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Use the following commands if you want to create a pool of IP addresses. These commands have no effect if you use the host command. You can still set them, however.	

Table 14 interface Commands: DHCP Settings (continued)

COMMAND	DESCRIPTION
dhcp-option <1..254> *option_name* {boolean <0..1>| uint8 <0..255> | uint16 <0..65535> | uint32 <0..4294967295> | ip *ipv4* [*ipv4* [*ipv4*]] | fqdn *fqdn* [*fqdn* [*fqdn*]] | text *text* | hex *hex* | vivc *enterprise_id hex_s* [*enterprise_id hex_s*] | vivs *enterprise_id hex_s* [*enterprise_id hex_s*]	Adds or edits a DHCP extended option for the specified DHCP pool. *text*: String of up to 250 characters *hex*: String of up to 250 hexadecimal pairs. *vivc*: Vendor-Identifying Vendor Class option. A DHCP client may use this option to unambiguously identify the vendor that manufactured the hardware on which the client is running, the software in use, or an industry consortium to which the vendor belongs. *enterprise_id*: Number <0..4294967295>. *hex_s*: String of up to 120 hexadecimal pairs. *vivs*: Vendor-Identifying Vendor-Specific option. DHCP clients and servers may use this option to exchange vendor-specific information.
no dhcp-option <1..254>	Removes the DHCP extended option for the specified DHCP pool.
network IP/<1..32> network *ip mask* no network	Specifies the IP address and subnet mask of the specified DHCP pool. The subnet mask can be written in w.x.y.z format or in /<1..32> format. Note: The DHCP pool must have the same subnet as the interface to which you plan to bind it. The no command clears these fields.
[no] default-router *ip*	Specifies the default gateway DHCP clients should use. The no command clears this field.
[no] description *description*	Specifies a description for the DHCP pool for identification. The no command removes the description.
[no] domain-name *domain_name*	Specifies the domain name assigned to DHCP clients. The no command clears this field.
[no] starting-address *ip* pool-size <1..65535>	Sets the IP start address and maximum pool size of the specified DHCP pool. The final pool size is limited by the subnet mask. Note: You must specify the network number first, and the start address must be in the same subnet. The no command clears the IP start address and maximum pool size.
[no] first-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns} | EnterpriseWLAN}	Sets the first DNS server to the specified IP address, the specified interface's first, second, or third DNS server, or the NXC itself. The no command resets the setting to its default value.
[no] second-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns} | EnterpriseWLAN}	Sets the second DNS server to the specified IP address, the specified interface's first, second, or third DNS server, or the NXC itself. The no command resets the setting to its default value.

Table 14 interface Commands: DHCP Settings (continued)

COMMAND	DESCRIPTION
[no] third-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns} | EnterpriseWLAN}	Sets the third DNS server to the specified IP address, the specified interface's first, second, or third DNS server, or the NXC itself. The no command resets the setting to its default value.
[no] first-wins-server *ip*	Specifies the first WINS server IP address to assign to the remote users. The no command removes the setting.
[no] second-wins-server *ip*	Specifies the second WINS server IP address to assign to the remote users. The no command removes the setting.
[no] lease {<0..365> [<0..23> [<0..59>]] | infinite}	Sets the lease time to the specified number of days, hours, and minutes or makes the lease time infinite. The no command resets the first DNS server setting to its default value.
interface *interface_name*	Enters sub-command mode.
[no] ip dhcp-pool *profile_name*	Binds the specified interface to the specified DHCP pool. You have to remove any DHCP relays first. The no command removes the binding.
[no] ip helper-address *ip*	Creates the specified DHCP relay. You have to remove the DHCP pool first, if the DHCP pool is bound to the specified interface. The no command removes the specified DHCP relay.
release dhcp *interface-name*	Releases the TCP/IP configuration of the specified interface. The interface must be a DHCP client. This command is available in privilege mode, not configuration mode.
renew dhcp *interface-name*	Renews the TCP/IP configuration of the specified interface. The interface must be a DHCP client. This command is available in privilege mode, not configuration mode.
show ip dhcp binding [*ip* | *interface-name*]	Displays information about DHCP bindings for the specified IP address, IP addresses assigned by the specified interface or for all IP addresses.
clear ip dhcp binding {*ip* | *}	Removes the DHCP bindings for the specified IP address or for all IP addresses.

6.2.2.1 DHCP Setting Command Examples

The following example uses these commands to configure DHCP pool DHCP_TEST.

```
Router# configure terminal
Router(config)# ip dhcp pool DHCP_TEST
Router(config-ip-dhcp-pool)#  network 192.168.1.0 /24
Router(config-ip-dhcp-pool)#  domain-name zyxel.com
Router(config-ip-dhcp-pool)#  first-dns-server 10.1.5.1
Router(config-ip-dhcp-pool)#  second-dns-server ge1 1st-dns
Router(config-ip-dhcp-pool)#  third-dns-server 10.1.5.2
Router(config-ip-dhcp-pool)#  default-router 192.168.1.1
Router(config-ip-dhcp-pool)#  lease 0 1 30
Router(config-ip-dhcp-pool)#  starting-address 192.168.1.10 pool-size 30
Router(config-ip-dhcp-pool)#  hardware-address 00:0F:20:74:B8:18
Router(config-ip-dhcp-pool)#  client-identifier 00:0F:20:74:B8:18
Router(config-ip-dhcp-pool)#  client-name TWtester1
Router(config-ip-dhcp-pool)# exit
Router(config)#  interface ge1
Router(config-if)# ip dhcp-pool DHCP_TEST
Router(config-if)# exit
Router(config)# show ip dhcp server status
binding interface : ge1
  binding pool    : DHCP_TEST
```

6.2.3 Connectivity Check (Ping-check) Commands

Use these commands to have an interface regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the NXC stops routing to the gateway. The NXC resumes routing to the gateway the first time the gateway passes the connectivity check.

This table lists the `ping-check` commands

Table 15 interface Commands: Ping Check

COMMAND	DESCRIPTION
`show ping-check [interface_name | status]`	Displays information about ping check settings for the specified interface or for all interfaces. `status`: displays the current connectivity check status for any interfaces upon which it is activated.
`show ping-check [interface_name]`	Displays information about ping check settings for the specified interface or for all interfaces.
`[no] connectivity-check continuous-log activate`	Use this command to have the NXC logs connectivity check result continuously. The `no` command disables the setting.
`show connectivity-check continuous-log status`	Displays the continuous log setting about connectivity check.
`interface interface_name`	Enters sub-command mode.
`[no] ping-check activate`	Enables ping check for the specified interface. The `no` command disables ping check for the specified interface.
`ping-check {domain_name | ip | default-gateway}`	Specifies what the NXC pings for the ping check; you can specify a fully-qualified domain name, IP address, or the default gateway for the interface.
`ping-check {domain_name | ip | default-gateway} period <5..30>`	Specifies what the NXC pings for the ping check and sets the number of seconds between each ping check.
`ping-check {domain_name | ip | default-gateway} timeout <1..10>`	Specifies what the NXC pings for the ping check and sets the number of seconds the NXC waits for a response.
`ping-check {domain_name | ip | default-gateway} fail-tolerance <1..10>`	Specifies what the NXC pings for the ping check and sets the number of times the NXC times out before it stops routing through the specified interface.
`ping-check {domain_name | ip | default-gateway} method {icmp | tcp}`	Sets how the NXC checks the connection to the gateway. `icmp`: ping the gateway you specify to make sure it is still available. `tcp`: perform a TCP handshake with the gateway you specify to make sure it is still available.
`ping-check {domain_name | ip | default-gateway} port <1..65535>`	Specifies the port number to use for a TCP connectivity check.

6.2.3.1 Connectivity Check Command Example

The following commands show you how to set the WAN1 interface to use a TCP handshake on port 8080 to check the connection to IP address 1.1.1.2

```
Router# configure terminal
Router(config)# interface wan1
Router(config-if-wan1)# ping-check 1.1.1.2 method tcp port 8080
Router(config-if-wan1)# exit
Router(config)# show ping-check
Interface: wan1
Check Method: tcp
IP Address: 1.1.1.2
Period: 30
Timeout: 5
Fail Tolerance: 5
Activate: yes
Port: 8080
Router(config)#
```

6.3 Ethernet Interface Specific Commands

This section covers commands that are specific to Ethernet interfaces.

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

Table 16 Input Values for Ethernet Interface Commands

LABEL	DESCRIPTION
interface_name	The name of the interface. Ethernet interface: gex, x = 1 - N, where N equals the highest numbered Ethernet interface for your NXC model. VLAN interface: vlanx, x = 0 - 4094.

6.3.1 MAC Address Setting Commands

This table lists the commands you can use to set the MAC address of an interface..

Table 17 interface Commands: MAC Setting

COMMAND	DESCRIPTION
`interface` *interface_name*	Enters sub-command mode.
`no mac`	Has the interface use its default MAC address.
`mac` *mac*	Specifies the MAC address the interface is to use.

Table 17 interface Commands: MAC Setting (continued)

COMMAND	DESCRIPTION
type {internal|external|general}	Sets which type of network you will connect this interface. The NXC automatically adds default route and SNAT settings for traffic it routes from internal interfaces to external interfaces; for example LAN to WAN traffic. internal: Set this to connect to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The NXC automatically adds default SNAT settings for traffic flowing from this interface to an external interface. external: Set this to connect to an external network (like the Internet). The NXC automatically adds this interface to the default WAN trunk. general: Set this if you want to manually configure a policy route to add routing and SNAT settings for the interface.
no use-defined-mac	Has the interface use its default MAC address.
use-defined-mac	Has the interface use a MAC address that you specify.

6.4 Port Commands

This section covers commands that are specific to ports.

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

Table 18 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.

6.5 Port Role Commands

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

Table 19 Command Summary: Port Role

COMMAND	DESCRIPTION
`show port type`	Displays the type of cable connection for each physical interface on the device.
`show module type`	Display the type of module for each physical interface on the device.

6.5.1 Port Role Examples

The following are two port role examples..

```
Router(config)# show port type
Port Type
================================================================================
1    Copper
2    Down
3    Down
4    Down
5    Down
6    Down
7    Down
8    Down
Router(config)# show module type
Port Type
================================================================================
1    Copper
2    Copper
3    Copper
4    Copper
5    Fiber
6    Fiber
7    Fiber
8    Fiber
```

6.6 USB Storage Specific Commands

Use these commands to configure settings that apply to the USB storage device connected to the NXC.

Note: For the NXC which supports more than one USB ports, these commands only apply to the USB storage device that is first attached to the NXC.

Table 20 USB Storage General Commands

COMMAND	DESCRIPTION
show usb-storage	Displays the status of the connected USB storage device.
[no] usb-storage activate	Enables or disables the connected USB storage service.
usb-storage warn *number* <*percentage*|*megabyte*>	Sets a number and the unit (percentage or megabyte) to have the NXC send a warning message when the remaining USB storage space is less than the set value. *percentage*: 10 to 99 *megabyte*: 100 to 9999
usb-storage mount	Mounts the connected USB storage device.
usb-storage umount	Unmounts the connected USB storage device.
[no] logging usb-storage	Sets to have the NXC log or not log any information about the connected USB storage device(s) for the system log.
logging usb-storage category *category* level <all|normal>	Configures the logging settings for the specified category for the connected USB storage device.
logging usb-storage category *category* disable	Stops logging for the specified category to the connected USB storage device.
logging usb-storage flushThreshold <1..100>	Configures the maximum storage space (in percentage) for storing system logs on the connected USB storage device.
[no] diag-info copy usb-storage	Sets to have the NXC save or stop saving the current system diagnostics information to the connected USB storage device. You may need to send this file to customer support for troubleshooting.
[no] corefile copy usb-storage	Sets to have the NXC save or not save a process's core dump to the connected USB storage device if the process terminates abnormally (crashes). You may need to send this file to customer support for troubleshooting.
show corefile copy usb-storage	Displays whether (enable or disable) the NXC saves core dump files to the connected USB storage device.
show diag-info copy usb-storage	Displays whether (enable or disable) the NXC saves the current system diagnostics information to the connected USB storage device.
show logging status usb-storage	Displays the logging settings for the connected USB storage device.

6.6.1 USB Storage General Commands Example

This example shows how to display the status of the connected USB storage device.

```
Router> show usb-storage
USBStorage Configuration:
Activation: enable
Criterion Number: 100
Criterion Unit: megabyte
USB Storage Status:
Device description: N/A
Usage: N/A
Filesystem: N/A
Speed: N/A
Status: none
Detail: none
```

6.7 VLAN Interface Specific Commands

A Virtual Local Area Network (VLAN) divides a physical network into multiple logical networks. The standard is defined in IEEE 802.1q.

In the NXC, each VLAN is called a VLAN interface. As a router, the NXC routes traffic between VLAN interfaces, but it does not route traffic within a VLAN interface.

Note: vlan0 is the default VLAN interface. It cannot be deleted and its VID cannot changed.

Otherwise, VLAN interfaces are similar to other interfaces in many ways. They have an IP address, subnet mask, and gateway used to make routing decisions. They restrict bandwidth and packet size. They can provide DHCP services, and they can verify the gateway is available.

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 VLAN Interface Commands

LABEL	DESCRIPTION
virtual_interface	The VLAN interface name. You may use 0 - 511 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
gateway	The gateway IP address of the interface. Enter a standard IPv4 IP address (for example, 127.0.0.1).
ip_address	The network mask IP address. Enter a standard IPv4 IP address.
netmask	The network subnet mask. For example, 255.255.255.0.
description	Sets the description of the interface. You may use 0 - 511 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
profile_name	The DHCP pool name.

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

Table 22 Command Summary: VLAN Interface Profile

COMMAND	DESCRIPTION
[no] interface *virtual_interface*	Enters configuration mode for the specified interface. Use the *no* command to remove the specified VLAN interface.
vlanid <1..4094>	Sets the interface's VLAN identification number.
[no] ip address *ip_address netmask*	Sets the interface's IP address and netmask address. Use the no command to remove these values from this interface.
[no] ip address dhcp [metric <0..15>]	Sets the interface to use the DHCP to acquire an IP address. Enter the metric (priority) of the gateway (if any) on this interface. The NXC decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the NXC uses the one that was configured first.
mtu <576..1500>	Sets the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the NXC divides it into smaller fragments.
no mtu	Disables the mtu feature for this interface.
[no] ip gateway *gateway* [metric <0..15>]	Enter the IP address of the gateway. The NXC sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface. Also enter the metric (priority) of the gateway (if any) on this interface. The NXC decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the NXC uses the one that was configured first.
join <*interface_name*> <tag|untag>	Links the VLAN to the specified physical interface and also sets this interface to send packets with or without a VLAN tag.
no join <*interface_name*>	Disassociates the specified physical interface from the VLAN.
upstream <0..1048576>	Sets the maximum amount of traffic, in kilobits per second, the NXC can send through the interface to the network.
no upstream	Disables the upstream bandwidth limit.
downstream <0..1048576>	Sets the maximum amount of traffic, in kilobits per second, the NXC can receive from the network through the interface.
no downstream	Disables the downstream bandwidth limit.
description *description*	Sets the description of this interface. It is not used elsewhere. You can use alphanumeric and ()+/ :=?!*#@$_%- characters, and it can be up to 60 characters long.
no description	Removes the VLAN description.
[no] shutdown	Exits this sub-command mode, saving all changes but without enabling the VLAN.
[no] ip dhcp-pool *profile_name*	Sets the DHCP server pool. The no command removes the specified DHCP pool.

Table 22 Command Summary: VLAN Interface Profile (continued)

COMMAND	DESCRIPTION
[no] ip helper-address *ip_address*	Sets the IP helper address. The no command removes the IP address.
exit	Exits configuration mode for this interface.

6.7.1 VLAN Interface Examples

This example creates a VLAN interface called 'vlan0'..

```
Router(config)# interface vlan0
Router(config-if-vlan)# vlanid 100
Router(config-if-vlan)# join ge2 untag
Router(config-if-vlan)# ip address 1.2.3.4 255.255.255.0
Router(config-if-vlan)# ip gateway 2.2.2.2 metric 11
Router(config-if-vlan)# mtu 598
Router(config-if-vlan)# upstream 345
Router(config-if-vlan)# downstream 123
Router(config-if-vlan)# description I am vlan0
Router(config-if-vlan)# exit
Router(config)#
```

This example changes VLAN interface 'vlan0' to use DHCP..

```
Router(config)# interface vlan0
Router(config-if-vlan)# vlanid 100
Router(config-if-vlan)# join ge1 untag
Router(config-if-vlan)# ip address dhcp metric 4
Router(config-if-vlan)# exit
Router(config)#
```

6.8 LAG Commands

This section covers commands that are specific to Link Aggregation Group (LAG) interfaces. LAG is a way to combine multiple physical Ethernet interfaces into a single logical interface. This increases uplink bandwidth. It also increases availability as even if a member link goes down, LAG can continue to transmit and receive traffic over the remaining links.

To configure LAG, configure a link number and specify the member ports in the link. All ports must have the same speed and be in full-duplex mode. You must configure the LAG on both sides of the link and you must set the interfaces on either side of the link to be the same speed.

Note: At the time of writing, up to 4 ports can be grouped into a LAG and up to 3 LAGs can be configured on a NXC.

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

Table 23 Input Values for LAG Interface Commands

LABEL	DESCRIPTION
interface_name	The name of the interface. LAG interface: lagx, x = 0 - 2.

This table lists the LAG-specific interface commands. See Table 13 on page 44 for common `interface` commands.

Table 24 `interface` Commands: LAG Interfaces

COMMAND	DESCRIPTION
`interface` *interface_name*	Creates the specified LAG interface (`lag0` for example) and enters sub-command mode.
`mode {802_3ad | active-backup | balance-alb}`	Sets the LAG mode. Mode refers to whether the LAG is acting as follows: • **active-backup** where only one slave in the LAG interface is active and another slave becomes active only if the active slave fails. • **802.3ad** (IEEE 802.3ad Dynamic link aggregation) where Link Aggregation Control Protocol (LACP) negotiates automatic combining of links and balances the traffic load across the LAG link by sending LACP packets to the directly connected device that also implements LACP. The slaves must have the same speed and duplex settings. • **balance-alb** (adaptive load balancing) where traffic is distributed according to the current load on each slave by ARP negotiation. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave.
`[no] slave` *interface_name*	Specifies the member ports in the link. A slave is a physical Ethernet interface that is a member of a LAG. Slaves do not have an IP Address and in some cases share the same MAC address. The `no` command removed the member ports from the link.
`link-monitoring {arp | mii}`	Sets link monitoring to be `arp`, or `mii`. • `arp` monitoring sends ARP queries and uses the reply to know if the link is up and that traffic is flowing over the link. • `mii` monitoring monitors the state of the local interface; it can't tell if the link can transmit or receive packets.
`arp {arp-interval <1..1000> | arp-ip-target <W.X.Y.Z>}`	Configure for `arp` Link Monitoring. `arp-interval:` Specifies the frequency of ARP requests sent to confirm a that slave interface is up. `arp-ip-target <W.X.Y.Z>:` Specifies the IP address of the link to send ARP queries.
`miimon <1..1000>`	Configure for `mii` Link Monitoring. Specifies the link check interval in milliseconds that the system polls the Media Independent Interface (MII) to get status.
`lacp-rate {fast | slow}`	Configure for `802.3ad` Mode. Specifies the preferred LACPDU packet transmission rate (`fast | slow`) to request from 802.3ad partner.
`xmit-hash-policy {layer2 | layer2_3}`	Configure for `802.3ad` Mode. Specifies the algorithm for slave selection according to the selected TCP/IP layer.

Table 24 `interface` Commands: LAG Interfaces (continued)

COMMAND	DESCRIPTION
`updelay <0..1000>`	Configure for `mii` Link Monitoring. Specifies the waiting time in milliseconds to confirm the slave interface status is up.
`downdelay <0..1000>`	Configure for `mii` Link Monitoring. Specifies the waiting time in milliseconds to confirm the slave interface status is down.
`ping-check`	See Table 15 on page 52 for these command descriptions.
`type {external | general | internal}`	Specifies one of the following option depending on the type of network to which the NXC is connected or if you want to additionally manually configure some related settings. **`internal`** is for connecting to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The NXC automatically adds default SNAT settings for traffic flowing from this interface to an external interface. **`external`** is for connecting to an external network (like the Internet). The NXC automatically adds this interface to the default WAN trunk. For **`general`**, the rest of the screen's options do not automatically adjust and you must manually configure a policy route to add routing and SNAT settings for the interface.
`show lag available slaves`	Displays the available slaves that could be added to a LAG.
`show interface lag`	Displays interface details for all LAG interfaces.
`show interface lagx`	Displays interface details for the specified LAG interface.

6.8.1 LAG Interface Command Example

The following commands set up a LAG with slaves ge3, ge5 and ge6.

```
Router# configure terminal
Router(config)# interface lag1
Router(config-if-lag)# mode 802_3ad
Router(config-if-lag)# slave ge3
Router(config-if-lag)# slave ge5
Router(config-if-lag)# slave ge6
Router(config-if-lag)# link-monitoring mii
Router(config-if-lag)# miimon 1000
Router(config-if-lag)# xmit-hash-policy layer2
Router(config-if-lag)# lacp-rate fast
Router(config-if-lag)# updelay 500
Router(config-if-lag)# downdelay 500
Router(config-if-lag)# type external
Router(config-if-lag)# exit
```

CHAPTER 7
Route

This chapter shows you how to configure policies for IP routing and static routes on your NXC.

7.1 Policy Route

Traditionally, routing is based on the destination address only and the NXC takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

7.2 Policy Route Commands

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

Table 25 Input Values for General Policy Route 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 NXC model.
policy_number	The number of a policy route. 1 - *x* where *x* is the highest number of policy routes the NXC model supports. See the NXC's User's Guide for details.
schedule_object	The name of the schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
service_name	The name of the service (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
user_name	The name of a user (group). 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 policy route. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 26 Command Summary: Policy Route

COMMAND	DESCRIPTION
`[no] bwm activate`	Globally enables bandwidth management. You must globally activate bandwidth management to have individual policy routes or application patrol policies apply bandwidth management. The `no` command globally disables bandwidth management.
`policy {`*`policy_number`* `| append | insert` *`policy_number`*`}`	Enters the policy-route sub-command mode to configure, add or insert a policy.
`[no] auto-disable`	When you set `interface` as the next-hop type (using the `next-hop interface`) for this route, you can use this command to have the NXC automatically disable this policy route when the next-hop's connection is down. The `no` command disables the setting.
`[no] bandwidth <1..1048576> priority <1..1024> [maximize-bandwidth-usage]`	Sets the maximum bandwidth and priority for the policy. The `no` command removes bandwidth settings from the rule. You can also turn maximize bandwidth usage on or off.
`[no] deactivate`	Disables the specified policy. The `no` command enables the specified policy.
`[no] description` *`description`*	Sets a descriptive name for the policy. The `no` command removes the name for the policy.
`[no] destination {`*`address_object`*`|any}`	Sets the destination IP address the matched packets must have. The no command resets the destination IP address to the default (`any`). `any` means all IP addresses.
`[no] dscp {any | <0..63>}`	Sets a custom DSCP code point (0~63). This is the DSCP value of incoming packets to which this policy route applies. `any` means all DSCP value or no DSCP marker.
`[no] dscp class {default |` *`dscp_class`*`}`	Sets a DSCP class. Use `default` to apply this policy route to incoming packets that are marked with DSCP value 0. Use one of the pre-defined AF classes (including af11~af13, af21~af23, af31~af33, and af41~af43) to apply this policy route to incoming packets that are marked with the DSCP AF class. The "af" entries stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences.
`dscp-marking <0..63>`	Sets a DSCP value to have the NXC apply that DSCP value to the route's outgoing packets.
`dscp-marking class {default |` *`dscp_class`*`}`	Sets how the NXC handles the DSCP value of the outgoing packets that match this route. Set this to `default` to have the NXC set the DSCP value of the packets to 0. Set this to an "af" class (including af11~af13, af21~af23, af31~af33, and af41~af43) which stands for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences.
`no dscp-marking`	Use this command to have the NXC not modify the DSCP value of the route's outgoing packets.

Table 26 Command Summary: Policy Route (continued)

COMMAND	DESCRIPTION
[no] interface {*interface_name* | EnterpriseWLAN}	Sets the interface on which the incoming packets are received. The no command resets the incoming interface to the default (any). any means all interfaces. EnterpriseWLAN: the packets are coming from the NXC itself.
[no] next-hop {auto|gateway *address object* | interface *interface_name*}	Sets the next-hop to which the matched packets are routed. The no command resets next-hop settings to the default (auto).
[no] schedule *schedule_object*	Sets the schedule. The no command removes the schedule setting to the default (none). none means any time.
[no] service {*service_name*|any}	Sets the IP protocol. The no command resets service settings to the default (any). any means all services.
[no] snat {outgoing-interface|pool {*address_object*}}	Sets the source IP address of the matched packets that use SNAT. The no command removes source NAT settings from the rule.
[no] source {*address_object*|any}	Sets the source IP address that the matched packets must have. The no command resets the source IP address to the default (any). any means all IP addresses.
[no] trigger <1..8> incoming *service_name* trigger *service_name*	Sets a port triggering rule. The no command removes port trigger settings from the rule.
trigger append incoming *service_name* trigger *service_name*	Adds a new port triggering rule to the end of the list.
trigger delete <1..8>	Removes a port triggering rule.
trigger insert <1..8> incoming *service_name* trigger *service_name*	Adds a new port triggering rule before the specified number.
trigger move <1..8> to <1..8>	Moves a port triggering rule to the number that you specified.
[no] user *user_name*	Sets the user name. The no command resets the user name to the default (any). any means all users.
policy default-route	Enters the policy-route sub-command mode to set a route with the name “default-route”.
policy delete *policy_number*	Removes a routing policy.
policy flush	Clears the policy routing table.
policy list table	Displays all policy route settings.
policy move *policy_number* to *policy_number*	Moves a routing policy to the number that you specified.
[no] policy override-direct-route activate	Use this command to have the NXC forward packets that match a policy route according to the policy route instead of sending the packets to a directly connected network. Use the no command to disable it.
show policy-route [*policy_number*]	Displays all or specified policy route settings.
show policy-route begin *policy_number* end *policy_number*	Displays the specified range of policy route settings.

Table 26 Command Summary: Policy Route (continued)

COMMAND	DESCRIPTION
`show policy-route override-direct-route`	Displays whether or not the NXC forwards packets that match a policy route according to the policy route instead of sending the packets to a directly connected network.
`show policy-route rule_count`	Displays the number of policy routes that have been configured on the NXC.
`show policy-route underlayer-rules`	Displays all policy route rule details for advanced debugging.
`show bwm activation`	Displays whether or not the global setting for bandwidth management on the NXC is enabled.
`show bwm-usage < [policy-route` *`policy_number`*`] | [interface` *`interface_name`*`]`	Displays the specified policy route or interface's bandwidth allotment, current bandwidth usage, and bandwidth usage statistics.

7.2.1 Assured Forwarding (AF) PHB for DiffServ

Assured Forwarding (AF) behavior is defined in RFC 2597. The AF behavior group defines four AF classes. Inside each class, packets are given a high, medium or low drop precedence. The drop precedence determines the probability that routers in the network will drop packets when congestion occurs. If congestion occurs between classes, the traffic in the higher class (smaller numbered class) is generally given priority. Combining the classes and drop precedence produces the following twelve DSCP encodings from AF11 through AF43. The decimal equivalent is listed in brackets.

Table 27 Assured Forwarding (AF) Behavior Group

	CLASS 1	CLASS 2	CLASS 3	CLASS 4
Low Drop Precedence	AF11 (10)	AF21 (18)	AF31 (26)	AF41 (34)
Medium Drop Precedence	AF12 (12)	AF22 (20)	AF32 (28)	AF42 (36)
High Drop Precedence	AF13 (14)	AF23 (22)	AF33 (30)	AF43 (38)

7.2.2 Policy Route Command Example

The following commands create two address objects (TW_SUBNET and GW_1) and insert a policy that routes the packets (with the source IP address TW_SUBNET and any destination IP address) through the

interface ge1 to the next-hop router GW_1. This route uses the IP address of the outgoing interface as the matched packets' source IP address.

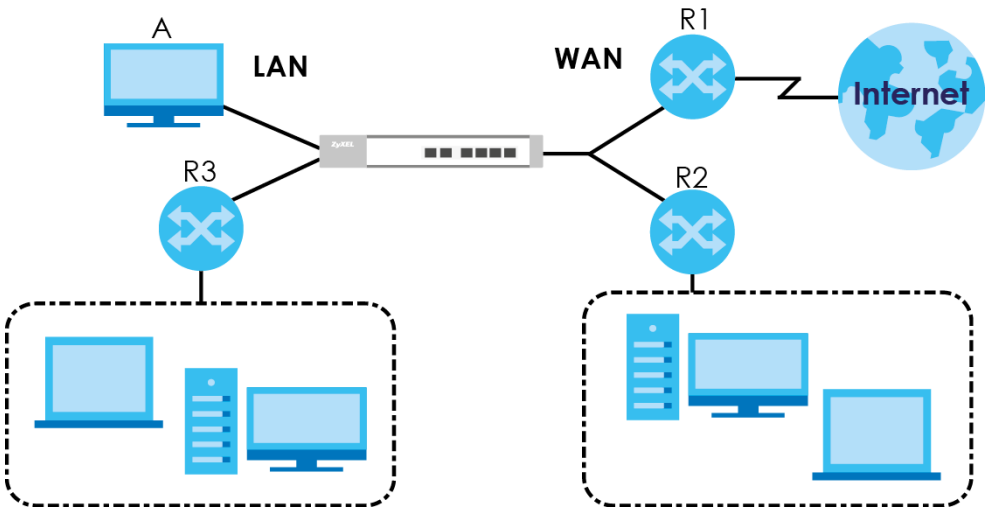
```
Router(config)# address-object TW_SUBNET 192.168.2.0 255.255.255.0
Router(config)# address-object GW_1 192.168.2.250
Router(config)# policy insert 1
Router(policy-route)# description example
Router(policy-route)# destination any
Router(policy-route)# interface ge1
Router(policy-route)# next-hop gateway GW_1
Router(policy-route)# snat outgoing-interface
Router(policy-route)# source TW_SUBNET
Router(policy-route)# exit
Router(config)# show policy-route 1
index: 1
  active: yes
  description: example
  user: any
  schedule: none
  interface: ge1
  tunnel: none
  sslvpn: none
  source: TW_SUBNET
  destination: any
  DSCP code: any
  service: any
  nexthop type: Gateway
  nexthop: GW_1
  nexthop state: Not support
  auto destination: no
  bandwidth: 0
  bandwidth priority: 0
  maximize bandwidth usage: no
  SNAT: outgoing-interface
  DSCP marking: preserve
  amount of port trigger: 0
Router(config)#
```

7.3 IP Static Route

The NXC usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the NXC send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the NXC's LAN interface. The NXC routes most traffic from **A** to the Internet through the NXC's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN..

Figure 10 Example of Static Routing Topology



7.4 Static Route Commands

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

Table 28 Command Summary: Static Route

COMMAND	DESCRIPTION
`[no] ip route {w.x.y.z} {w.x.y.z} {interface|w.x.y.z} [<0..127>]`	Sets a static route. The `no` command disables a static route.
`ip route replace {w.x.y.z} {w.x.y.z} {interface|w.x.y.z} [<0..127>] with {w.x.y.z} {w.x.y.z} {interface|w.x.y.z} [<0..127>]`	Changes an existing route's settings.
`show ip route-settings`	Displays static route information. Use `show ip route` to see learned route information.
`show ip route control-virtual-server-rules`	Displays whether or not static routes have priority over NAT virtual server rules (1-1 SNAT).

7.4.1 Static Route Commands Example

The following command sets a static route with IP address 10.10.10.0 and subnet mask 255.255.255.0 and with the next-hop interface ge1. Then use the `show` command to display the setting.

```
Router(config)# ip route 10.10.10.0 255.255.255.0 ge1
Router(config)#
Router(config)# show ip route-settings
Route           Netmask         Nexthop         Metric
================================================================================
10.10.10.0      255.255.255.0   ge1             0
```

7.5 Learned Routing Information Commands

This table lists the commands to look at learned routing information.

Table 29 ip route Commands: Learned Routing Information

COMMAND	DESCRIPTION
show ip route [kernel | connected | static]	Displays learned routing and other routing information.

7.5.1 show ip route Command Example

The following example shows learned routing information on the NXC.

```
Router> show ip route
Flags: A - Activated route, S - Static route, C - directly Connected
       O - OSPF derived, R - RIP derived, G - selected Gateway
       ! - reject, B - Black hole, L - Loop

IP Address/Netmask    Gateway          IFace           Metric    Flags
Persist
================================================================================
127.0.0.0/8           0.0.0.0          lo              0         ACG       -

192.168.1.0/24        0.0.0.0          vlan0           0         ACG       -

Router>
```

CHAPTER 8
AP Management

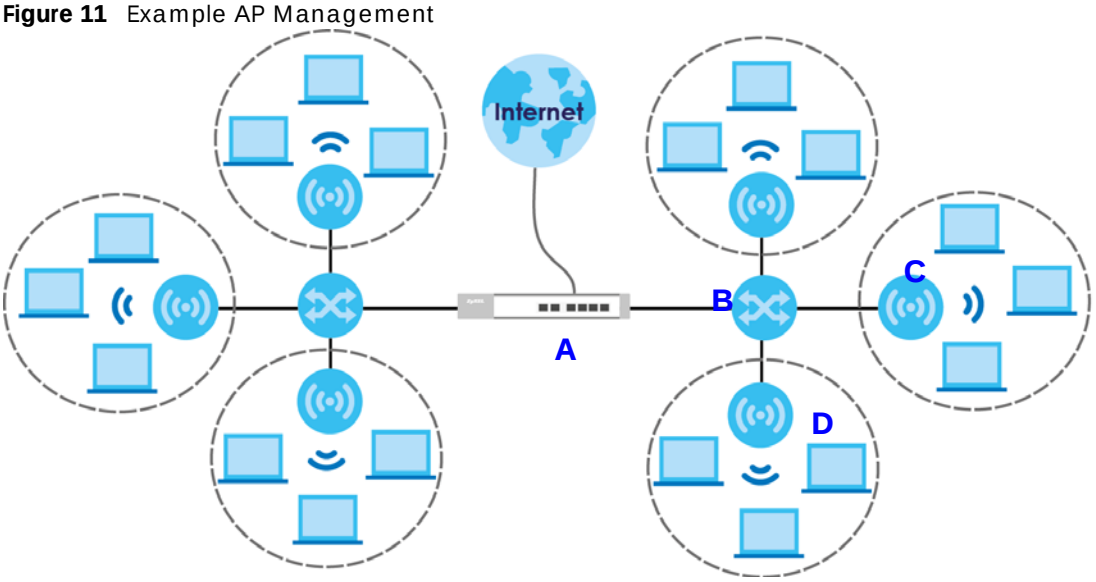
This chapter shows you how to configure wireless AP management options on your NXC.

8.1 AP Management Overview

The NXC allows you to remotely manage all of the Access Points (APs) on your network. You can manage a number of APs without having to configure them individually as the NXC automatically handles basic configuration for you.

The commands in this chapter allow you to add, delete, and edit the APs managed by the NXC by means of the CAPWAP protocol. An AP must be moved from the wait list to the management list before you can manage it. If you do not want to use this registration mechanism, you can disable it and then any newly connected AP is registered automatically.

Figure 11 Example AP Management



In this example, the NXC (**A**) connects up to a number of Power over Ethernet switches, such as the ES-2025 PWR (**B**). They connect to the NWA/WAC/WAX Access Points (**C**), which in turn provide access to the network for the wireless clients within their broadcast radius.

Let's say one AP (**D**) starts giving you trouble. You can log into the NXC via console or Telnet and troubleshoot, such as viewing its traffic statistics or reboot it or even remove it altogether from the list of viable APs that stations can use.

8.2 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 30 Input Values for General AP Management Commands

LABEL	DESCRIPTION
ap_mac	The Ethernet MAC address of the managed AP. Enter 6 hexidecimal pairs separated by colons. You can use 0-9, a-z and A-Z.
ap_model	The model name of the managed AP, such as WAC6303D-S or WAC6502D-S.
slot_name	The slot name for the AP's on-board wireless LAN card. Use either *slot1* or *slot2*.
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 MAC address of the wireless client. Enter 6 hexidecimal 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 31 Command Summary: AP Management

COMMAND	DESCRIPTION
`capwap ap` *ap_mac*	Enters the sub-command mode for the specified AP.
slot_name `ap-profile` *profile_name*	Sets the radio (*slot_name*) to AP mode and assigns a created AP profile to the radio.
`no` *slot_name* `ap-profile`	Removes the AP mode profile assignment for the specified radio (*slot_name*).
slot_name `monitor-profile` *profile_name*	Sets the specified radio (*slot_name*) to monitor mode and assigns a created monitor mode profile to the radio. Monitor mode APs act as wireless monitors, which can detect rogue APs and help you in building a list of friendly ones. See also Section 10.2 on page 87.
`no` *slot_name* `monitor-profile`	Removes the monitor mode profile assignment for the specified radio (*slot_name*).
slot_name `output-power <0dBm, 1dBm, ... 30dBm>`	Sets the maximum output power of the specified radio.
slot_name `{root-ap | repeater-ap}` *ap-profile_name*	Sets the specified radio (*slot_name*) to root AP or repeater mode and assigns a created AP profile to the radio.
slot_name `ssid-profile <1..8>` *ssid-profile_name*	Associates up to eight SSID profiles with the specified AP radio.

Table 31 Command Summary: AP Management (continued)

COMMAND	DESCRIPTION
slot_name wireless-bridge {enable | disable}	Enables or disables wireless bridging on the specified radio (*slot_name*). The managed AP 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 managed repeater AP can still transmit data through its Ethernet port(s) after the ZyMesh link is up. Be careful to avoid bridge loops. The managed APs in the same ZyMesh must use the same static VLAN ID.
slot_name zymesh-profile *profile_name*	Specifies the ZyMesh profile the radio uses to connect to a root AP or repeater. See also Section 10.7 on page 106 for more information about ZyMesh.
selectable-antenna config {ceiling | wall}	Adjust antenna orientation for all radios of an AP for better coverage. Select **Wall** if you mount the AP on a wall. Select **Ceiling** if the AP is mounted on a ceiling.
antenna config *slot_name* chain3 {ceiling | wall}	Adjust antenna orientation for a selected radio of an AP for better coverage. Select **Wall** if you mount the AP on a wall. Select **Ceiling** if the AP is mounted on a ceiling.
[no] antenna sw-control enable	Enables the adjustment of coverage depending on the orientation of the antenna for the AP radios using the web configurator or the command line interface (CLI). 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.
ap-group-profile *ap-group-profile_name*	Sets the AP group to which the AP belongs.
[no] ap-mode detection activate	Sets the AP to detect Rogue APs in the network. The no command disables rogue AP detection.
cloud interface ip address *ip netmask*	Manually sets an IP address for the AP in Nebula cloud management mode.
cloud interface ip address dhcp	Sets the AP in Nebula cloud management mode to act as a DHCP client.
cloud interface ip dns *ip*	Sets a DNS server address for the AP in Nebula cloud management mode.
cloud interface ip gateway *ip*	Sets a gateway address for the AP in Nebula cloud management mode.
cloud interface vlan <1..4094> {tag | untag}	Sets a management VLAN ID for the AP in Nebula cloud management mode and sets whether the AP adds the VLAN ID to outbound traffic transmitted through its Ethernet port.
cloud mode	Sets th e AP to work in Nebula cloud management mode and removes it from the managed AP list.
description *ap_description*	Sets the description for the specified AP.

Table 31 Command Summary: AP Management (continued)

COMMAND	DESCRIPTION
[no] force ip	Sets whether or not the NXC changes the AP's IP settings to match the ones you configure using the ip sub-command. This takes priority over the AP's CAPWAP client commands described in Chapter 42 on page 252.
[no] force vlan	Sets whether or not the NXC changes the AP's management VLAN to match the one you configure using the vlan sub-command. The management VLAN on the NXC and AP must match for the NXC to manage the AP. This takes priority over the AP's CAPWAP client commands described in Chapter 42 on page 252.
fw-updating	Updates the APs' firmware to the NXC's latest supported version.
ip address *ip*	Manually sets an IP address for the AP.
ip address dhcp	Sets the AP to act as a DHCP client.
ip dns *ip*	Sets a DNS server address for the AP.
ip gateway *ip*	Sets a gateway address for the AP.
ip no dns	Removes the specified DNS server address.
ip no gateway	Removes the specified gateway IP address.
lan-provision *lan_port* {activate | inactivate} pvid <1..4094>	Sets the NXC to enable or disable the specified LAN port on the AP and configures a PVID (Port VLAN ID) for this port. *lan_port*: the name of the AP's LAN port (lan1 for example).
lan-provision *vlan_interface* {activate | inactivate} vid <1..4094> join *lan_port* {tag | untag} [*lan_port* {tag | untag}] [*lan_port* {tag | untag}]	Sets the NXC to create a new VLAN or configure an existing VLAN. You can disable or enable the VLAN, set the VLAN ID, assign up to three ports to this VLAN as members and set whether the port is to tag outgoing traffic with the VLAN ID. *vlan_interface*: the name of the VLAN (vlan1 for example).
[no] override-full-power activate	Forces the AP to draw full power from the power sourcing equipment. This improves performance in cases when a PoE injector that does not support PoE negotiation is used. Use the no command to disable this feature.
[no] load-balancing <group1 | group2> *group_name*	Assigns a load balancing group to the AP. Use the no command to remove the group1 or group2 assignment of the AP.
[no] location *location*	Sets the name of the place where the AP is located. Use the no command to remove the specified settings.
[no] override *slot_name* {output-power | radio-setting | ssid-setting}	Sets the NXC to overwrite the AP's output power, radio or SSID profile settings for the specified radio. Use the no command to not overwrite the specified settings.

Table 31 Command Summary: AP Management (continued)

COMMAND	DESCRIPTION
[no] override ap-mode detection-setting	Sets the NXC to overwrite the AP's rogue AP detection settings. Use the no command to not overwrite the specified settings.
[no] override lan-provision	Sets the NXC to overwrite the AP's LAN port settings. Use the no command to not overwrite the specified settings.
[no] override vlan-setting	Sets the NXC to overwrite the AP's VLAN settings. Use the no command to not overwrite the specified settings.
[no] roaming group *roaminggroup*	Sets the name of the roaming group to which the AP belongs. The 802.11k neighbor list a client requests from the AP 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 AP's roaming group is not configured, any neighbor APs can be candidates for roaming. Use the no command to remove the specified settings.
[no] sysname *sysname*	Sets a name to identify the AP on a network. This is usually the AP's fully qualified domain name. Use the no command to remove the specified settings.
vlan <1..4094> {tag | untag}	Sets the VLAN ID for the specified AP as well as whether packets sent to and from that ID are tagged or untagged.
exit	Exits the sub-command mode for the specified AP.
capwap ap ac-ip *{primary_ac_ip} {secondary_ac_ip}*	Specifies the primary and secondary IP address or domain name of the AP controller (the NXC) to which the AP connects.
capwap ap ac-ip auto	Sets the AP to use DHCP to get the address of the AP controller (the NXC).
capwap ap add *ap_mac* [*ap_model*]	Adds the specified AP to the NXC for management. If manual add is disabled, this command can still be used; if you add an AP before it connects to the network, then this command simply preconfigures the management list with that AP's information.
capwap ap factory default *ap_mac*	Resets the specified AP to its factory default settings.
capwap ap fallback disable	Sets the managed AP(s) to not change back to associate with the primary AP controller when the primary AP controller is available.
capwap ap fallback enable	Sets the managed AP(s) to change back to associate with the primary AP controller as soon as the primary AP controller is available.

Table 31 Command Summary: AP Management (continued)

COMMAND	DESCRIPTION
capwap ap fallback interval <30..86400>	Sets how often (in seconds) the managed AP(s) check whether the primary AP controller is available.
capwap ap kick {all | *ap_mac*}	Removes the specified AP (*ap_mac*) or all connected APs (*all*) from the management list. Doing this removes the AP(s) from the management list. If the NXC is set to automatically add new APs to the AP management list, then any kicked APs are added back to the management list as soon as they reconnect.
capwap ap led-off *ap_mac*	Sets the LEDs of the specified AP to turn off after it's ready.
capwap ap led-on *ap_mac*	Sets the LEDs of the specified AP to stay lit after the NXC is ready.
capwap ap reboot *ap_mac*	Forces the specified AP (*ap_mac*) to restart. Doing this severs the connections of all associated stations.
capwap ap-group *ap_group_profile_name* fw-updating	Upgrades the firmware of the APs in the specified AP group to the NXC's latest supported version.
capwap firmware-update apply	Sets the NXC to download the latest AP firmware from the firmware server.
capwap firmware-update check	Checks the firmware server to see if there is any new AP firmware available.
capwap fw-updating method {capwap | ftp}	Sets how you want the NXC to upgrade AP firmware. capwap: have the NXC use CAPWAP to automatically update firmware on the managed APs. ftp: allow the managed APs to download the latest firmware from the NXC using FTP.
capwap fw-updating mode {auto | manual}	Sets whether a managed AP's firmware is updated automatically. auto: the NXC checks the AP's firmware version and updates it automatically to the NXC's latest supported version. manual: you use the commands or web configurator to update the AP firmware manually.
capwap manual-add {enable | disable}	Allows the NXC to either automatically add new APs to the network (*disable*) or wait until you manually confirm them (*enable*).
capwap station kick *sta_mac*	Forcibly disconnects the specified station from the network.
show capwap ap {all | *ap_mac*}	Displays information of all managed APs (*all*) or information of an AP on the Specified MAC address (*ap_mac*).
show capwap ap {all | ap_mac} config status	Displays whether or not any AP's configuration or the specified AP's configuration is in conflict with the NXC's settings for the AP and displays the settings in conflict if there are any.
show capwap ap *ap_mac slot_name* detail	Displays details for the specified radio (*slot_name*) on the specified AP (*ap_mac*).
show capwap ap ac-ip	Displays the address of the NXC or auto if the AP finds the NXC through broadcast packets.

Table 31 Command Summary: AP Management (continued)

COMMAND	DESCRIPTION
show capwap ap all statistics	Displays radio statistics for all APs on the management list.
show capwap ap fallback	Displays whether the managed AP(s) will change back to associate with the primary AP controller when the primary AP controller is available.
show capwap ap fallback interval	Displays the interval for how often the managed AP(s) check whether the primary AP controller is available.
show capwap ap firmware	Displays the firmware version of the managed AP the NXC currently has.
show capwap ap info	Displays the number of managed APs which are currently connected to the NXC or go offline and the number of wireless clients.
show capwap ap wait-list	Displays a list of connected but as-of-yet unmanaged APs. This is known as the 'wait list'.
show capwap fw-updating info	Displays the number of APs doing firmware update, their method and mode used to update firmware. This also displays the latest AP firmware version currently on the NXC and the status of the last firmware check.
show capwap manual-add	Displays the current manual add option.
show capwap station all	Displays information for all stations connected to the APs on the management list.
show country-code list	Displays a reference list of two-letter country codes.
show default country-code	Displays the default country code configured on the NXC.
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 lan-provision ap *ap_mac* interface {*lan_port* | *vlan_interface* | all| ethernet | uplink | vlan}	Displays the port and/or VLAN settings for the specified AP. You can also set to display settings for a specified port, a specified VLAN, all physical Ethernet ports, the uplink port or all VLANs on the AP.

8.2.1 AP Management Commands Example

The following example shows you how to add an AP to the management list, and then edit it.

```
Router# show capwap ap wait-list
index: 1
  IP: 192.168.1.35, MAC: 00:11:11:11:11:FE
  Model: NWA5160N, Description: AP-00:11:11:11:11:FE
index: 2
  IP: 192.168.1.36, MAC: 00:19:CB:00:BB:03
  Model: NWA5160N, Description: AP-00:19:CB:00:BB:03
Router# configure terminal
Router(config)# capwap ap add 00:19:CB:00:BB:03
Router(config)# capwap ap 00:19:CB:00:BB:03
Router(AP 00:19:CB:00:BB:03)# slot1 ap-profile approf01
Router(AP 00:19:CB:00:BB:03)# exit
```

The following example shows you part of the information that the command `show capwap ap all` will show.

```
Router> show capwap ap all
index: 1
  Status: RUN
  IP: 10.253.41.39, MAC: 4C:9E:FF:90:B1:C0
  Description: Mark_Test
  Model: WAC6502D-S
  CPU Usage: 5 %
  R1 mode: AP, R1Prof: Mark_24G_US
  R2 mode: AP, R2Prof: Mark_5G_US
  AP Group Profile: Mark_test
  Override Slot1 Radio Profile: disable
  Override Slot1 SSID Profile: disable
  slot1-SSID Profile 1:
  slot1-SSID Profile 2:
  slot1-SSID Profile 3:
  slot1-SSID Profile 4:
  slot1-SSID Profile 5:
  slot1-SSID Profile 6:
  slot1-SSID Profile 7:
  slot1-SSID Profile 8:
  Override Slot1 Output Power: disable
  Slot1 Output Power: 10dBm
  Override Slot2 Radio Profile: disable
  Override Slot2 SSID Profile: disable
  slot2-SSID Profile 1: Mark_Test
  slot2-SSID Profile 2: Mark_Test_Local
  slot2-SSID Profile 3:
  slot2-SSID Profile 4:
  slot2-SSID Profile 5:
```

The following example shows you part of the information that the command `show capwap ap_mac` will show.

```
Router> show capwap ap BC:CF:4F:56:BD:DF
index: 1
  Status: RUN
  IP: 10.50.40.5, MAC: BC:CF:4F:56:BD:DF
  Description: WAX650S-LOC-RDFT
  Model: WAX650S
  CPU Usage: 22 %
  R1 mode: AP, R1Prof: RADIO_24G_Taiwan
  R2 mode: AP, R2Prof: RADIO_5G_Taiwan
  AP Group Profile: RDFT_LOC
  Override Slot1 Radio Profile: disable
  Override Slot1 SSID Profile: disable
  slot1-SSID Profile 1: LOC-24G-CP3
  slot1-SSID Profile 2: virtual_ssid-loc24_2
  slot1-SSID Profile 3: virtual_ssid-loc24_3
  slot1-SSID Profile 4: virtual_ssid-loc24_4
  slot1-SSID Profile 5: virtual_ssid-loc24_5
  slot1-SSID Profile 6: virtual_ssid-loc24_6
  slot1-SSID Profile 7: virtual_ssid-loc24_7
  slot1-SSID Profile 8: virtual_ssid-loc24_8
  Override Slot1 Output Power: disable
  Slot1 Output Power: 17dBm
  Override Slot2 Radio Profile: disable
  Override Slot2 SSID Profile: disable
  slot2-SSID Profile 1: virtual_ssid-loc5_1
  slot2-SSID Profile 2: LOC-5G-CP1
  slot2-SSID Profile 3: LOC-5G-CP2
  slot2-SSID Profile 4: virtual_ssid-loc5_4
  slot2-SSID Profile 5: virtual_ssid-loc5_5
  slot2-SSID Profile 6: virtual_ssid-loc5_6
  slot2-SSID Profile 7: virtual_ssid-loc5_7
  slot2-SSID Profile 8: virtual_ssid-loc5_8
  Override Slot2 Output Power: disable
  Slot2 Output Power: 17dBm
  Station: 5, RadioNum: 2
  Override VLAN Setting: disable
  Mgmt. VLAN ID: 1, Tag: no
  WTP VLAN ID: 1, WTP Tag: no
  Force VLAN: disable
  Support Lan-provision: yes
  Override LAN Provision: disable
  Firmware Version: 6.00(ABRM.5)b3
```

The following example displays the management list and radio statistics for the specified AP.

```
Router(config)# show capwap ap all
index: 1
  Status: RUN
  IP: 192.168.1.37, MAC: 60:31:97:82:F5:AF
  Description: AP-60319782F5AF
  Model: WAC5302D-S
  CPU Usage: 12 %
  R1 mode: AP, R1Prof: default
  R2 mode: AP, R2Prof: default2
  AP Group Profile: default
  Override Slot1 Radio Profile: disable
  Override Slot1 SSID Profile: disable
  slot1-SSID Profile 1: default
  slot1-SSID Profile 2:
  slot1-SSID Profile 3:
  slot1-SSID Profile 4:
  slot1-SSID Profile 5:
  slot1-SSID Profile 6:
  slot1-SSID Profile 7:
  slot1-SSID Profile 8:
  Override Slot1 Output Power: disable
  Slot1 Output Power: 30dBm
  Override Slot2 Radio Profile: disable
  Override Slot2 SSID Profile: disable
  slot2-SSID Profile 1: default
  slot2-SSID Profile 2:
  slot2-SSID Profile 3:
  slot2-SSID Profile 4:
  slot2-SSID Profile 5:
  slot2-SSID Profile 6:
  slot2-SSID Profile 7:
  slot2-SSID Profile 8:
  Override Slot2 Output Power: disable
  Slot2 Output Power: 30dBm
  Station: 2, RadioNum: 2
  Override VLAN Setting: disable
  Mgnt. VLAN ID: 1, Tag: no
  WTP VLAN ID: 1, WTP Tag: no
  Force VLAN: disable
  Support Lan-provision: yes
  Override LAN Provision: disable
  Firmware Version: 5.30(AASE.0)b6
  Primary AC IP: broadcast
  Secondary AC IP: N/A
  Recent On-line Time: 2018/06/26 04:08:16
  Last Off-line Time: 2018/06/26 04:08:16
  Loop State: N/A
  LED Status: N/A
  Suppress Mode Status: Enable
  Locator LED Status: N/A
  Locator LED Time: 0
  Locator LED Time Lease: 0
  Power Mode: Full
  Antenna Switch SW-Control: N/A
  Antenna Switch Radio 1: N/A
  Antenna Switch Radio 2: N/A
```

```
  Compatible: No
  Capability: 582
  Port Number: 2
  Conflict: n/a
  Non-support: n/a
  Slot1-BLE-status: N/A
  Override AP-mode Detection: enable
  AP-mode Detection: no
  Ethernet Uplink: N/A
  System Name: ZyxelTW
  Location: Zyxel 1F
  S/N: S162L31240135
  Roaming Group:
  Load-Balancing Group1:
  Load-Balancing Group2:
  NebulaFlex PRO: No
  Support Factory Default: No
  Packet Capture Capability: No
  Force IP: disable
  Config IP Status: dhcp
  Config IP Address: n/a
  Config IP Mask: n/a
  Config IP Gateway: n/a
  Config IP DNS: n/a
  Storming: N/A
  Override full power: N/A
Router(config)# show capwap ap 60:31:97:82:F5:AF slot1 detail
index: 1
  SSID: Zyxel
  BSSID: 60:31:97:82:F5:B0
  SecMode: NONE, Forward Mode: Local Bridge, Vlan: 1
Router(config)# show capwap ap all statistics
index: 1
  Status: RUN, Loading: -
  AP MAC: 60:31:97:82:F5:AF
  Radio: 1, OP Mode: AP
  Profile: default, MAC: F0:FD:F0:FD:F0:FD
  Description: AP-60319782F5AF
  Model: WAC5302D-S
  Band: 2.4GHz, Channel: 6
  Station: 0
  Rx: 101395, Tx: 866288
  RxFCS: 42803, TxRetry: 897
  TxPower: 15 dBm
  Antenna Type: N/A

index: 2
  Status: RUN, Loading: -
  AP MAC: 60:31:97:82:F5:AF
  Radio: 2, OP Mode: AP
  Profile: default2, MAC: F0:FD:F0:FD:F0:FD
  Description: AP-60319782F5AF
  Model: WAC5302D-S
  Band: 5GHz, Channel: 36/40
  Station: 2
  Rx: 864251, Tx: 1076862
  RxFCS: 169608, TxRetry: 2816
  TxPower: 16 dBm
  Antenna Type: N/A

Router(config)#
```

CHAPTER 9
AP Group

This chapter shows you how to configure AP groups, which define the radio, port, VLAN and load balancing settings and apply the settings to all APs in the group. An AP can belong to one AP group at a time.

9.1 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.

9.2 AP Group 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 AP Management Commands

LABEL	DESCRIPTION
ap_group_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.
slot	The slot name for the AP's on-board wireless LAN card. Use either *slot1* or *slot2*.

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

Table 33 Command Summary: AP Group

COMMAND	DESCRIPTION
`ap-group first-priority` *ap_group_profile_name*	Sets an AP group file that is used as the default group file. Any AP that is not configured to associate with a specific AP group belongs to the default group automatically.
`ap-group flush wtp-setting` *ap_group_profile_name*	Sets the NXC to overwrite the settings of all managed APs in the specified group with the group profile settings.

Table 33 Command Summary: AP Group (continued)

COMMAND	DESCRIPTION
ap-group-member *ap_group_profile_name* [no] member *mac_address*	Specifies the MAC address of the AP that you want to apply the specified AP group profile and add to the group. Use the no command to remove the specified AP from this group.
[no] ap-group-profile *ap_group_profile_name*	Enters configuration mode for the specified AP group profile. Use the no command to remove the specified profile.
[no] *slot* ap-profile *radio_profile_name*	Sets the specified radio to work as an AP and specifies the radio profile the radio is to use. Use the no command to remove the specified profile.
[no] *slot* monitor-profile *monitor_profile_name*	Sets the specified radio to work in monitor mode and specifies the monitor profile the radio is to use. Use the no command to remove the specified profile.
[no] *slot* output-power *wlan_power*	Sets the output power (between 0 to 30 dBm) for the radio on the AP that belongs to this group. Use the no command to remove the output power setting.
[no] *slot* repeater-ap *radio_profile_name*	Sets the specified AP radio to work as a repeater and specifies the radio profile the radio is to use. Use the no command to remove the specified profile.
[no] *slot* root-ap *radio_profile_name*	Sets the specified radio to work as a root AP and specifies the radio profile the radio is to use. A root AP supports the wireless connections with other APs (in repeater mode) to form a ZyMesh to extend its wireless network. Use the no command to remove the specified profile.
[no] *slot* ssid-profile <1..8> *ssid_profile_name*	Sets the SSID profile that is associated with this profile. You can associate up to eight SSID profiles with an AP radio. Use the no command to remove the specified profile.
[no] *slot* zymesh-profile *zymesh_profile_name*	Sets the ZyMesh profile the radio (in root AP or repeater mode) uses to connect to a root AP or repeater. Use the no command to remove the specified profile.
description *description*	Sets a description for this group. You can use up to 31 characters, spaces and underscores allowed. Use the no command to remove the specified description.
exit	Exits configuration mode for this profile.
[no] force vlan	Sets the NXC to change the AP's management VLAN to match the configuration in this profile. Use the no command to not change the AP's management VLAN setting.

Table 33 Command Summary: AP Group (continued)

COMMAND	DESCRIPTION
[no] lan-provision model *ap_model ap_lan_port* activate pvid <1..4094>	Sets the model of the managed AP and enable the model-specific LAN port and configure the port VLAN ID. Use the no command to remove the specified port and VLAN settings. *ap_lan_port*: the Ethernet LAN port on the managed AP, such as lan1 or lan2. *ap_model*: the model name you want to configure. Use "-" instead of spaces. Examples are: nwa5123-achd, wac6503d-s, and wac6552d-s.
[no] lan-provision model *ap_model ap_lan_port* inactivate pvid <1..4094>	Sets the model of the managed AP and disable the model-specific LAN port and configure the port VLAN ID. Use the no command to remove the specified port and VLAN settings. *ap_lan_port*: the Ethernet LAN port on the managed AP, such as lan1 or lan2. *ap_model*: the model name you want to configure. Use "-" instead of spaces. Examples are: nwa5123-ac-hd, wac6503d-s, and wac6552d-s.
[no] lan-provision model *ap_model vlan_interface* activate vid <1..4094> join *ap_lan_port* {tag | untag} [*ap_lan_port* {tag | untag}] [*ap_lan_port* {tag | untag}]	Sets the model of the managed AP, enable a VLAN and configure the VLAN ID. It also sets the Ethernet port(s) on the managed AP to be a member of the VLAN, and sets the port(s) to send packets with or without a VLAN tag. Use the no command to remove the specified port and VLAN settings. *vlan_interface*: the name of the VLAN, such as vlan0. *ap_lan_port*: the Ethernet LAN port on the managed AP, such as lan1 or lan2. *ap_model*: the model name you want to configure. Use "-" instead of spaces. Examples are: nwa5123-ac-hd, wac6503d-s, and wac6552d-s.
[no] lan-provision model *ap_model vlan_interface* inactivate vid <1..4094> join *ap_lan_port* {tag | untag} [*ap_lan_port* {tag | untag}] [*ap_lan_port* {tag | untag}]	Sets the model of the managed AP, disable a VLAN and configure the VLAN ID. It also sets the Ethernet port(s) on the managed AP to be a member of the VLAN, and sets the port(s) to send packets with or without a VLAN tag. Use the no command to remove the specified port and VLAN settings. *vlan_interface*: the name of the VLAN, such as vlan0. *ap_lan_port*: the Ethernet LAN port on the managed AP, such as lan1 or lan2. *ap_model*: the model name you want to configure. Use "-" instead of spaces. Examples are: nwa5123-ac-hd, wac6503d-s, and wac6552d-s.
[no] load-balancing [slot1 | slot2] activate	Enables load balancing. Use the no parameter to disable it. Optionally specify a radio slot.

Table 33 Command Summary: AP Group (continued)

COMMAND	DESCRIPTION
load-balancing [slot1 | slot2] 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 NXC and should not be changed unless you have been specifically directed to do so by Zyxel support.
load-balancing [slot1 | slot2] 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 NXC and should not be changed unless you have been specifically directed to do so by Zyxel support.
load-balancing [slot1 | slot2] 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.
[no] load-balancing [slot1 | slot2] kickout	Enables an overloaded AP to disconnect ("kick") idle clients or clients with noticeably weak connections.
load-balancing [slot1 | slot2] 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 NXC and should not be changed unless you have been specifically directed to do so by Zyxel support.
load-balancing [slot1 | slot2] 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 [slot1 | slot2] 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 AP delays association request and authentication request packets from any new station that attempts to make a connection. smart-classroom: the AP ignores association request and authentication request packets from any new station when the maximum number of stations is reached.

Table 33 Command Summary: AP Group (continued)

COMMAND	DESCRIPTION
load-balancing [slot1 | slot2] 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 NXC and should not be changed unless you have been specifically directed to do so by Zyxel support.
load-balancing [slot1 | slot2] 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 [slot1 | slot2] traffic level {high | low | medium}	If load balancing by traffic threshold, this sets the traffic threshold level.
[no] location *location*	Sets the name of the place where the AP group is located. Use the no command to remove the location setting.
vlan <1..4094> {tag | untag}	Sets the management VLAN ID for the AP(s) in this group as well as whether packets sent to and from that VLAN ID are tagged or untagged.
show ap-group first-priority	Displays the name of the default AP group profile.
show ap-group-profile {all | *ap_group_profile_name*}	Displays the settings of the AP group profile(s). *all*: Displays all profiles. *ap_group_profile_name*: Displays the specified profile.
show ap-group-profile *ap_group_profile_name* ap-mode detection config	Displays the AP-mode rogue AP detection configuration of the specified AP group profile.
show ap-group-profile *ap_group_profile_name* load-balancing config	Displays the load balancing configuration of the specified AP group profile.
show ap-group-profile *ap_group_profile_name* lan-provision model ap_*model* interface {all | vlan | ethernet | *ap_lan_port* | *vlan_interface*}	Displays the LAN port and/or VLAN settings on the managed AP which is in the specified AP group and of the specified model. *vlan_interface*: the name of the VLAN, such as vlan0. *ap_lan_port*: the Ethernet LAN port on the managed AP, such as lan1 or lan2. *ap_model*: the model name you want to configure. Use "-" instead of spaces. Examples are: nwa5123-ac-hd, wac6503d-s, and wac6552d-s.
show ap-group-profile *ap_group_profile_name* lan-provision model	Shows the model name of the managed AP which belongs to the specified AP group.
show ap-group-profile rule_count	Displays how many AP group profiles have been configured on the NXC.
capwap ap-group *ap_group_profile_name* fw-updating	Forces the APs in a specified AP group (*ap_group_profile_name*) to upgrade their firmware.

Table 33 Command Summary: AP Group (continued)

COMMAND	DESCRIPTION
capwap ap-group reboot *ap_group_profile_name*	Forces the APs in a specified AP group (*ap_group_profile_name*) to restart. Doing this severs the connections of all associated stations.
ap-group-profile rename *ap_group_profile_name1* *ap_group_profile_name2*	Gives an existing AP group profile (*ap_group_profile_name1*) a new name (*ap_group_profile_name2*).

9.2.1 AP Group Examples

The following example shows you how to create an AP group profile (named "TEST") and configure the AP's first radio to work in repeater mode using the "default" radio profile and the "ZyMesh_TEST" ZyMesh profile. It also adds the AP with the MAC address 00:a0:c5:01:23:45 to this AP group.

```
Router(config)# ap-group-profile TEST
Router(config-ap-group TEST)# slot1 repeater-ap default
Router(config-ap-group TEST)# slot1 zymesh-profile ZyMesh_TEST
Router(config-ap-group TEST)# exit
Router(config)# ap-group-member TEST member 00:a0:c5:01:23:45
Router(config)#
```

The following example shows you how to create an AP group profile (named GP1) and configure AP load balancing in "by station" mode. The maximum number of stations is set to 1.

```
Router(config)# ap-group-profile GP1
Router(config-ap-group GP1)# load-balancing mode station
Router(config-ap-group GP1)# load-balancing max sta 1
Router(config-ap-group GP1)# exit
Router(config)# show ap-group-profile GP1 load-balancing config
AP Group Profile:GP1
load balancing config slot1:
Activate: no
Kickout: no
Mode: station
Max-sta: 1
Traffic-level: high
Alpha: 5
Beta: 10
Sigma: 60
Timeout: 20
LIInterval: 10
KickoutInterval: 10
load balancing config slot2:
Activate: no
Kickout: no
Mode: station
Max-sta: 1
Traffic-level: high
Alpha: 5
Beta: 10
Sigma: 60
Timeout: 20
LIInterval: 10
KickoutInterval: 10
Router(config)#
```

The following example shows you how to create an AP group profile (named GP2) and configure AP load balancing in "by traffic" mode. The traffic level is set to low, and "disassociate station" is enabled.

```
Router(config)# ap-group-profile GP2
Router(config-ap-group GP2)# load-balancing mode traffic
Router(config-ap-group GP2)# load-balancing traffic level low
Router(config-ap-group GP2)# load-balancing kickout
Router(config-ap-group GP2)# exit
Router(config)# show ap-group-profile GP2 load-balancing config
AP Group Profile:GP2
load balancing config slot1:
Activate: no
Kickout: yes
Mode: traffic
Max-sta: 127
Traffic-level: low
Alpha: 5
Beta: 10
Sigma: 60
Timeout: 20
LIInterval: 10
KickoutInterval: 10
load balancing config slot2:
Activate: no
Kickout: yes
Mode: traffic
Max-sta: 127
Traffic-level: low
Alpha: 5
Beta: 10
Sigma: 60
Timeout: 20
LIInterval: 10
KickoutInterval: 10
Router(config)#
```

CHAPTER 10
Wireless LAN Profiles

This chapter shows you how to configure wireless LAN profiles on your NXC.

10.1 Wireless LAN Profiles Overview

The managed Access Points designed to work explicitly with your NXC 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, MAC Filter profiles, and Layer-2 isolation 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 34 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.
interval	Enters the dynamic channel selection interval time. The range is 10 ~ 1440 minutes.
wlan_role	Sets the wireless LAN radio operating mode. At the time of writing, you can use `ap` for Access Point.
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_htcw	Sets the HT channel width. Select either `20`, `20/40` or `20/40/80`.

Table 34 Input Values for General Radio and Monitor Profile Commands (continued)

LABEL	DESCRIPTION
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`.
wlan_power	Sets the radio output power.
scan_method	Sets the radio's scan method while in Monitor mode. Select `manual` or `auto`.
wlan_interface_index	Sets the radio interface index number. The range is `1 ~ 8`.
ssid_profile	Sets the associated SSID profile name. This name must be an existing 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.

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 35 Command Summary: Radio Profile

COMMAND	DESCRIPTION
`show wlan-radio-profile {all | radio_profile_name}`	Displays the radio profile(s). *all*: Displays all profiles. *radio_profile_name*: Displays the specified profile.
`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.
`2g-channel wireless_channel_2g`	Sets the broadcast band for this profile in the 2.4 GHz frequency range. The default is 6.
`5g-channel wireless_channel_5g`	Sets the broadcast band for this profile in the 5 GHz frequency range. The default is 36.
`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-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] activate`	Makes this profile active or inactive.

Table 35 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
band {2.4G |5G} band-mode {bg | bgn | a | ac | an | bgnax | anacax}	Sets the radio band (2.4 GHz or 5 GHz) and band mode for this profile. Band mode details: For 2.4 GHz, bg lets IEEE 802.11b and IEEE 802.11g clients associate with the AP. For 2.4 GHz, bgn lets IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n clients associate with the AP. For 2.4 GHz, bgnax lets IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, and IEEE802.11ax clients associate with the AP. For 5 GHz, a lets only IEEE 802.11a clients associate with the AP. For 5 GHz, ac lets IEEE 802.11a, IEEE 802.11n, and IEEE 802.11ac clients associate with the AP. For 5 GHz, an lets IEEE 802.11a and IEEE 802.11n clients associate with the AP. For 5 GHz, anacax lets IEEE 802.11a, IEEE 802.11n, IEEE 802.11ac, and IEEE802.11ax clients associate with the AP.
bss-color <0~63>	Sets the BSS color of the AP, which distinguishes it from other nearby APs when they transmit over the same channel. Set it to 0 to automatically assign a BSS color.
[no] disable-bss-color	Disables BSS coloring. Use the no command to enable BSS coloring.
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.
country-code *country_code*	Sets the country where the NXC is located/installed. The available channels vary depending on the country you selected. Be sure to select the correct/same country for both radios on an AP and all connected APs, in order to prevent roaming failure and interference to other systems. *country_code*: 2-letter country-codes, such as TW, DE, or FR.
[no] dcs activate	Starts dynamic channel selection to automatically find a less-used channel in an environment where there are many APs and there may be interference. Use the no parameter to turn it off.
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 an AP 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 an AP can use.

Table 35 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
dcs dcs-2g-method {auto|manual}	Sets the AP to automatically search for available channels or manually configure the channels the AP uses in the 2.4 GHz band.
dcs dcs-5g-method {auto|manual}	Sets the AP to automatically search for available channels or manually configure the channels the AP uses in the 5 GHz band.
dcs client-aware {enable|disable}	When enabled, this ensures that an AP will not change channels as long as a client is connected to it. If disabled, the AP may change channels regardless of whether it has clients connected to it or not.
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). Sets the option that is applicable to your region. (Channel deployment may be regulated differently between countries and locales.)
dcs dfs-aware {enable|disable}	Enables this to allow an AP to avoid phase DFS channels below the 5 GHz spectrum.
dcs mode {interval|schedule}	Sets the AP 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 AP starts to use DCS on the specified day(s) of the week.
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 time-interval *interval*	Sets the interval that specifies how often DCS should run.
[no] nol-channel-block	Enables or disables temporary DFS channel blacklisting. If enabled, the AP will block a DFS channel if it detects a radar signal within that range.
[no] disable-dfs-switch	Makes the DFS switch active or inactive. By default this is inactive.
[no] dot11n-disable-coexistence	Fixes the channel bandwidth as 40 MHz. The no command has the AP automatically choose 40 MHz if all the clients support it or 20 MHz if some clients only support 20 MHz.

Table 35 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
[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] 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.
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.
[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.
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.
[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.

Table 35 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
limit-amsdu *<2290..4096>*	Sets the maximum frame size to be aggregated. The default is 4096.
[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.
[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.
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.
output-power *wlan_power*	Sets the output power (between 0 to 30 dBm) for the radio in this profile.
role *wlan_role*	Sets the profile's wireless LAN radio operating mode.
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~-105>	Sets a minimum kick-off signal strength. When a wireless client's signal strength is lower than the specified threshold, the NXC disconnects the wireless client from the AP. -20 dBm is the strongest signal you can require and -105 is the weakest.
[no] rssi-retry	Allows a wireless client to try to associate with the AP 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 AP.
[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 AP.
[no] ssid-profile *wlan_interface_index ssid_profile*	Assigns an SSID profile to this radio profile. Requires an existing SSID profile. Use the *no* parameter to disable it.
tx-mask *chain_mask*	Sets the outgoing chain mask rate.

Table 35 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
rx-mask *chain_mask*	Sets the incoming chain mask rate.
exit	Exits configuration mode for this profile.
storm-control ethernet ap *mac address*	Enters the storm control sub-command mode for the specified AP.
[no] broadcast	Enables or disables broadcast storm control, which drops broadcast packets from ingress traffic if the traffic rate exceeds the configured maximum rate.
broadcast pps <1~10000>	Sets the maximum rate for broadcast traffic before storm control starts dropping broadcast packets.
[no] multicast	Enables or disables multicast storm control, which drops multicast packets from ingress traffic if the traffic rate exceeds the configured maximum rate.
multicast pps <1~10000>	Sets the maximum rate for multicast traffic before storm control starts dropping multicast packets.
wlan-radio-profile RADIO_PROFILE_NAME rssi-dbm <signal strength (dBm)>	Sets a minimum client signal strength. A wireless client is allowed to connect to the AP only when its signal strength is stronger than the specified threshold. -20 dBm is the strongest signal you can set and -105 is the weakest.
wlan-radio-profile RADIO_PROFILE_NAME rssi-kickout <signal strength (dBm)>	Sets a minimum kick-off signal strength. When a wireless client's signal strength is lower than the specified threshold, the AP disconnects the wireless client from it. -20 dBm is the strongest signal you can set and -105 is the weakest.
show storm-control ethernet ap *mac address*	Displays broadcast/multicast storm control settings on the specified AP.
show wlan-monitor-profile {all | *monitor_profile_name*}	Displays all monitor profiles or just the specified one.
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.
country-code *country_code*	Sets the country where the NXC is located/installed. The available channels vary depending on the country you selected. Be sure to select the correct/same country for both radios on an AP and all connected APs, in order to prevent roaming failure and interference to other systems. *country_code*: 2-letter country-codes, such as TW, DE, or FR.
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.

Table 35 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
[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 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
- an output power of 100%

It will also assign the SSID profile labeled 'default' in order to create WLAN VAP (wlan-1-1) functionality within the radio profile.

```
Router(config)# wlan-radio-profile RADIO01
Router(config-profile-radio)# activate
Router(config-profile-radio)# band 2.4G band-mode bgn
Router(config-profile-radio)# 2g-channel 6
Router(config-profile-radio)# ch-width 20/40
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
Router(config-profile-radio)# output-power 21dBm
Router(config-profile-radio)# ssid-profile 1 default
```

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 36 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.
vlan_iface	The VLAN interface name of the controller (in this case, it is NXC5200). The maximum VLAN interface number is product-specific; for the NXC, the number is 512.
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 37 Command Summary: SSID Profile

COMMAND	DESCRIPTION
`show wlan-ssid-profile {all | ssid_profile_name}`	Displays the SSID profile(s). *all*: Displays all profiles for the selected operating mode. *ssid_profile_name*: Displays the specified profile for the selected operating mode.
`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 37 Command Summary: SSID Profile (continued)

COMMAND	DESCRIPTION
[no] bandselect balance-ratio <1..8>	Sets a ratio of the wireless clients using the 5 GHz band to the wireless clients using the 2.4 GHz band. Use the *no* parameter to turn off this feature.
bandselect check-sta-interval <1..60000>	Sets how often (in seconds) the AP checks and deletes old wireless client data. Note: This command is not applicable to the managed APs running with firmware version 5.30 or later.
bandselect drop-authentication <1..16>	Sets how many authentication request from a client to a 2.4GHz WiFi network is ignored during the specified timeout period. Note: This command is not applicable to the managed APs running with firmware version 5.30 or later.
bandselect drop-probe-request <1..32>	Sets how many probe request from a client to a 2.4GHz WiFi network is ignored during the specified timeout period. Note: This command is not applicable to the managed APs running with firmware version 5.30 or later.
bandselect min-sort-interval <1..60000>	Sets the minimum interval (in seconds) at which the AP sorts the wireless client data when the client queue is full. Note: This command is not applicable to the managed APs running with firmware version 5.30 or later.
bandselect mode {disable | force | standard}	To improve network performance and avoid interference in the 2.4 GHz frequency band, you can enable this feature to use the 5 GHz band first. You should set 2.4GHz and 5 GHz radio profiles to use the same SSID and security settings. Note: The managed APs must be dual-band capable. disable: to turn off this feature. force: to have the wireless clients always connect to an SSID using the 5 GHZ band. Connections to an SSID using the 2.4GHz band are not allowed. It is recommended you select this option when the AP and wireless clients can function in either frequency band. standard: to have the AP try to connect the wireless clients to the same SSID using the 5 GHZ band. Connections to an SSID using the 2.4GHz band are still allowed. Note: This command is not applicable to the managed APs running with firmware version 5.30 or later.

Table 37 Command Summary: SSID Profile (continued)

COMMAND	DESCRIPTION
bandselect mode {disable | standard}	To improve network performance and avoid interference in the 2.4 GHz frequency band, you can enable this feature to use the 5 GHz band first. You should set 2.4GHz and 5 GHz radio profiles to use the same SSID and security settings. Note: The managed APs must be dual-band capable. disable: to turn off this feature. standard: to turn on the band select feature. Connections to an SSID using the 2.4GHz band are still allowed. If you enable IEEE 802.11k/v assisted roaming on the AP, • when a client connecting to the 2.4 GHz WiFi network can also function in the 5 GHz band and supports 802.11v, and its 5 GHz WiFi signal strength is good, the AP sends 802.11v messages to suggest preferred 5 GHz SSIDs to the client. • when a client connecting to the 2.4 GHz WiFi network can also function in the 5 GHz band but doesn't support 802.11v, the AP disconnects the client after it has been idle longer than 5 seconds. The client then can change to connect to a 5 GHz WiFi network.
[no] bandselect stop-threshold <10..20>	Sets the threshold number of the connected wireless clients at which the AP disables the band select feature. Use the *no* parameter to turn off this feature.
bandselect time-out-force <1..255>	Sets the timeout period (in seconds) within which the AP accepts probe or authentication requests to a 2.4GHz WiFi network when the band select mode is set to force. Note: This command is not applicable to the managed APs running with firmware version 5.30 or later.
bandselect time-out-period <1..255>	Sets the timeout period (in seconds) within which the AP drops the specified number of probe or authentication requests to a 2.4GHz WiFi network. Note: This command is not applicable to the managed APs running with firmware version 5.30 or later.
bandselect time-out-standard <1..255>	Sets the timeout period (in seconds) within which the AP accepts probe or authentication requests to a 2.4GHz WiFi network when the band select mode is set to standard. Note: This command is not applicable to the managed APs running with firmware version 5.30 or later.
[no] block-intra	Enables intra-BSSID traffic blocking. Use the no parameter to disable it in this profile. By default this is disabled.

Table 37 Command Summary: SSID Profile (continued)

COMMAND	DESCRIPTION
[no] controller-offline-policy {standard | fallback}	Enables the policy and sets the action the AP takes when the AP controller (the NXC) is not reachable. standard: the AP hides the SSID when the AP fails to connect to the NXC. The SSID stays up when the NXC is reachable. fallback: the SSID appears only when the NXC is not reachable and is hidden when the AP can connect to the NXC. Use the no parameter to disable the controller offline policy.
data-forward {localbridge | tunnel *vlan_iface*}	Sets the data forwarding mode used by this SSID. The default is localbridge.
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] dot11k-v activate	Enables IEEE 802.11k/v assisted roaming on the AP. When the connected clients request 802.11k neighbor lists, the AP will response with a list of neighbor APs that can be candidates for roaming. When the 802.11v capable clients are using the 2.4 GHz band, the AP can send 802.11v messages to steer clients to the 5 GHz band. Use the no parameter to disable EEE 802.11k/v assisted roaming.
downlink-rate-limit *data_rate*	Sets the maximum incoming transmission data rate (either in mbps or kbps) on a per-station basis.
[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 *l2isolationprofile*	Assigns the specified layer-2 isolation profile to this SSID profile. Use the no parameter to remove it.
[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.
{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] proxy-arp	Sets the AP 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.

Table 37 Command Summary: SSID Profile (continued)

COMMAND	DESCRIPTION
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. The default SSID is 'Zyxel'.
[no] ssid-schedule	Enables the SSID schedule. Use the no parameter to disable the SSID schedule.
[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 AP using this SSID profile. Use the no parameter to disable the U-APSD feature.
uplink-rate-limit *data_rate*	Sets the maximum outgoing transmission data rate (either in mbps or kbps) on a per-station basis.
vlan-id *<1..4094>*	Applies to each SSID profile that uses localbridge. 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.
exit	Exits configuration mode for this profile.

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)# data-forward localbridge
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 38 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*.

Table 38 Input Values for General Security Profile Commands (continued)

LABEL	DESCRIPTION
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 39 Command Summary: Security Profile

COMMAND	DESCRIPTION
`show wlan-security-profile {all | security_profile_name}`	Displays the security profile(s). *all*: Displays all profiles for the selected operating mode. *security_profile_name*: Displays the specified profile for the selected operating mode.
`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 AP 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 AP 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] dot11r activate`	Turns on IEEE 802.11r fast roaming on the AP. Use the `no` parameter to turn it off.
`[no] dot11r ft-over-ds activate`	Sets the clients to communicate with the target AP through the current AP. The communication between the client and the target AP is carried in frames between the client and the current AP, and is then sent to the target AP through the wired Ethernet connection. Use the `no` parameter to have the clients communicate directly with the target AP. Note: This command is applicable to the managed APs running with firmware version 5.30 or later.

Table 39 Command Summary: Security Profile (continued)

COMMAND	DESCRIPTION
[no] dot11r over-the-ds activate	Sets the clients to communicate with the target AP through the current AP. The communication between the client and the target AP is carried in frames between the client and the current AP, and is then sent to the target AP through the wired Ethernet connection. Use the no parameter to have the clients communicate directly with the target AP. Note: This command is applicable to the managed APs running with firmware version older than v5.30.
[no] dot1x-eap	Enables 802.1x secure authentication. Use the no parameter to disable it.
[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 AP's wireless network.
eap {external | internal *auth_method*}	Sets the 802.1x authentication method.
[no] fallback	Allows the client to change to authenticate his/her connection via the captive portal login page when MAC authentication fails and captive portal is enabled. The no parameter disables it. If MAC authentication fails and captive portal is disabled, the client can log into the network without authentication.
group-key <30..30000>	Sets the interval (in seconds) at which the AP updates the group WPA/WPA2 encryption key. The default is 3000.
idle <30..30000>	Sets the idle interval (in seconds) that a client can be idle before authentication is discontinued. The default is 300.
[no] internal-eap-proxy activate	Allows the NXC to act as a proxy server and forward the authentication packets to the connected RADIUS server. Use the no parameter to disable it.

Table 39 Command Summary: Security Profile (continued)

COMMAND	DESCRIPTION
[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. See Section 23.2.4.1 on page 153 for a MAC authentication example.
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 | enhanced-open | wep | wpa2 | wpa2-mix | wpa3}	Sets the security mode for this profile.
[no] reauth <30..30000>	Sets the interval (in seconds) between authentication requests. The default is 0.
[no] server-acct <1..2> activate	Enables user accounting through an external server. Use the no parameter to disable.
server-acct <1..2> ip address *ipv4_address* port <1..65535> secret *secret*	Sets the IPv4 address, port number and shared secret of the external accounting server.
[no] server-acct <1..2>	Clears the user accounting setting.
[no] server-auth <1..2> activate	Activates server authentication. Use the no parameter to deactivate.
server-auth <1..2> ip address *ipv4_address* port <1..65535> secret *secret*	Sets the IPv4 address, port number and shared secret of the RADIUS server to be used for authentication.
[no] server-auth <1..2>	Clears the server authentication setting.
[no] transition-mode	Enables backward compatibility when used with WPA3 or Enhanced Open security mode. WPA3 falls back to WPA2, while Enhanced Open falls back to open (none).

Table 39 Command Summary: Security Profile (continued)

COMMAND	DESCRIPTION
wep <64 | 128> default-key <1..4>	Sets the WEP encryption strength (*64 or 128*) and the default key value (*1 ~ 4*). 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.
wep-auth-type {open | share}	Sets the authentication key type to either *open* or *share*.
wpa-encrypt {tkip | 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. tkip: This is the Temporal Key Integrity Protocol encryption method added later to the WEP encryption protocol to further secure. Not all wireless clients may support this. 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 40 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.
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 security profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 41 Command Summary: MAC Filter Profile

COMMAND	DESCRIPTION
`show wlan-macfilter-profile {all | macfilter_profile_name}`	Displays the security profile(s). *all*: Displays all profiles for the selected operating mode. *macfilter_profile_name*: Displays the specified profile for the selected operating mode.
`wlan-macfilter-profile rename macfilter_profile_name1 macfilter_profile_name2`	Gives an existing security 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 description description2`	Sets the description of this profile. 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)# MAC 01:02:03:04:05:06 description MAC01
Router(config-macfilter-profile)# MAC 01:02:03:04:05:07 description MAC02
Router(config-macfilter-profile)# MAC 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 42 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	The Ethernet MAC address of the device that you want to allow to be accessed by other devices in the SSID to which the layer-2 isolation profile is applied. Enter 6 hexidecimal pairs separated by colons. You can use 0-9, a-z and A-Z.
description	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 layer-2 isolation profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 43 Command Summary: Layer-2 Isolation Profile

COMMAND	DESCRIPTION
`show wlan-l2isolation-profile {all | l2isolation_profile_name}`	Displays the layer-2 isolation profile(s). *all*: Displays all profiles. *l2isolation_profile_name*: Displays the specified profile.
`wlan-l2isolation-profile rename l2isolation_profile_name1 l2isolation_profile_name2`	Gives an 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 description description`	Sets a MAC address associated with this profile and the profile description. Use the `no` parameter to clear the settings. Note: If a device's MAC addresses is NOT listed in a layer-2 isolation profile, it is blocked from communicating with other devices in an SSID on which layer-2 isolation is enabled.
`description description`	Sets the description for the 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 'L2-Isolate-example'. In this profile, you allow the device with the MAC address of 00:a0:c5:01:23:45 to be accessed by other devices in the SSID to which the layer-2 isolation profile is applied. It also displays the profile settings.

```
Router(config)# wlan-l2isolation-profile L2-Isolate-example
Router(config-wlan-l2isolation L2-Isolate-example)# 00:a0:c5:01:23:45
description printer
Router(config-wlan-l2isolation L2-Isolate-example)# exit
Router(config)# show wlan-l2isolation-profile all
l2isolation profile: L2-Isolate-example
  reference: 0
  ProfileDescription:
  entry: 0
    MAC: 00:A0:C5:01:23:45
    Description: printer
Router(config)#
```

10.7 ZyMesh Profile Commands

ZyMesh is a Zyxel proprietary protocol that creates wireless mesh links between managed APs to expand the wireless network. Managed APs can provide services or forward traffic between the NXC and wireless clients. ZyMesh also allows the NXC to use CAPWAP to automatically update the configuration settings on the managed APs (in repeater mode) through wireless connections. The managed APs (in repeater mode) are provisioned hop by hop.

The managed APs in a ZyMesh must use the same SSID, channel number and pre-shared key. A manged AP can be either a root AP or repeater in a ZyMesh.

Note: All managed APs should be connected to the NXC directly to get the configuration file before being deployed to build a ZyMesh. Ensure you restart the managed AP after you change its operating mode using the `wlan-radio-profile` *`radio_profile_name`* `role` commands.

- Root AP: a managed AP that can transmit and receive data from the NXC via a wired Ethernet connection.
- Repeater: a managed AP that transmit and/or receive data from the NXC via a wireless connection through a root AP.

Note: When managed APs are deployed to form a ZyMesh for the first time, the root AP must be connected to an AP controller (the NXC).

The maximum number of hops (the repeaters between a wireless client and the root AP) you can have in a ZyMesh varies according to how many wireless clients a managed AP can support.

Note: A ZyMesh link with more hops has lower throughput.

Note: When the wireless connection between the root AP and the repeater is up, in order to prevent bridge loops, the repeater would not be able to transmit data through its Ethernet port(s). The repeater then could only receive power from a PoE device if you use PoE to provide power to the managed AP via an 8-ping Ethernet cable.

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

Table 44 Input Values for General ZyMesh Profile Commands

LABEL	DESCRIPTION
zymesh_profile_name	The ZyMesh 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 ZyMesh profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 45 Command Summary: ZyMesh Profile

COMMAND	DESCRIPTION
`show zymesh ap info`	Displays the number of currently connected/offline ZyMesh APs.
`show zymesh link info {repeater-ap | root-ap}`	Displays the ZyMesh traffic statistics between the managed APs. `repeater-a`: the managed AP is acting as a repeater in a ZyMesh. `root-ap`: the managed AP is acting as a root AP in a ZyMesh.
`show zymesh provision-group`	Displays the current ZyMesh Provision Group MAC address in the NXC.
`show zymesh-profile {all | zymesh_profile_name}`	Displays the ZyMesh profile settings. *all*: Displays all profiles. *zymesh_profile_name*: Displays the specified profile.
`zymesh-profile rename zymesh_profile_name1 zymesh_profile_name2`	Gives an existing radio profile (*zymesh_profile_name1*) a new name (*zymesh_profile_name2*).
`[no] zymesh-profile zymesh_profile_name`	Enters configuration mode for the specified ZyMesh profile. Use the *no* parameter to remove the specified 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 wireless traffic between the APs.
`ssid ssid`	Sets the SSID with which you want the managed AP to connect to a root AP or repeater to build a ZyMesh link. Note: The ZyMesh SSID is hidden in the outgoing beacon frame so a wireless device cannot obtain the SSID through scanning using a site survey tool.
`exit`	Exits configuration mode for this profile.
`zymesh provision-group ac_mac`	Enters the ZyMesh Provision Group MAC address of the primary AP controller in your network to use this NXC to replace the primary AP controller.

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 NXC network administrator regards as non-threatening. This does not necessarily mean the friendly AP must belong to the network managed by the NXC; rather, it is any unmanaged AP within range of the NXC'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 46 Input Values for Rogue AP Detection Commands

LABEL	DESCRIPTION
ap_mac	Specifies the MAC address (in 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 47 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.

Table 47 Command Summary: Rogue AP Detection (continued)

COMMAND	DESCRIPTION
[no] ap-mode detection activate	Sets the AP to detect Rogue APs in the network. Use the no parameter to disable rogue AP detection.
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.
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.
[no] rogue-rule {hidden-ssid |ssid-keyword |weak-security |unmanaged-ap} activate	Specifies the characteristic(s) a device should have for the AP 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.
detect now	Allows the managed APs to scan for APs in the network.
show rogue-ap detection keyword list	Displays the SSID keyword(s) a device should have for the AP 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 48 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 49 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 config`	Displays whether rogue AP containment is enabled or not.
`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 Bluetooth

This chapter shows you how to configure the Bluetooth advertising settings for the APs that support 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.

12.1 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

12.2 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 50 Bluetooth Commands

COMMAND	DESCRIPTION
`ble ap` *ap_mac*	Enters the Bluetooth sub-command mode for the specified bluetooth radio on the AP.
`slot1 ibeacon index <1..5> activate`	Enables the specified iBeacon ID.
`slot1 ibeacon index <1..5> no activate`	Disables the specified iBeacon ID.
`slot1 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 ap` *ap_mac* `advertising all`	Displays the Bluetooth advertising settings (beacon IDs) of the AP.
`show ble uuid-gen`	Automatically generates a UUID and displays.

12.3 Bluetooth Commands Example

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

```
Router# show ble uuid-gen
UUID: EBAECFAF-DFE0-4039-BE5A-F030EED4303C
Router# configure terminal
Router(config)# ble ap 00:00:00:61:03:01
Router(AP 00:00:00:61:03:01)# slot1 ibeacon index 1 no activate
Router(AP 00:00:00:61:03:01)# slot1 ibeacon index 1 activate
Router(AP 00:00:00:61:03:01)# slot1 ibeacon index 1 uuid EBAECFAF-DFE0-4039-
BE5A-F030EED4303C major 10 minor 1
Router(AP 00:00:00:61:03:01)# slot1 ibeacon index 2 no activate
Router(AP 00:00:00:61:03:01)# slot1 ibeacon index 2 activate
Router(AP 00:00:00:61:03:01)# slot1 ibeacon index 2 uuid EBAECFAF-DFE0-4039-
BE5A-F030EED4303C major 10 minor 2
Router(AP 00:00:00:61:03:01)# slot1 ibeacon index 3 no activate
Router(AP 00:00:00:61:03:01)# slot1 ibeacon index 3 activate
Router(AP 00:00:00:61:03:01)# slot1 ibeacon index 3 uuid EBAECFAF-DFE0-4039-
BE5A-F030EED4303C major 20 minor 1
Router(AP 00:00:00:61:03:01)# exit

Router(config)# show ble ap 00:00:00:61:03:01 advertising all

Slot   Index   Activate    UUID                            Major    Minor

==========================================================================
====

1     1     1        EBAECFAF-DFE0-4039-BE5A-F030EED4303C    10       1

1     2     1        EBAECFAF-DFE0-4039-BE5A-F030EED4303C    10       2

1     3     1        EBAECFAF-DFE0-4039-BE5A-F030EED4303C    20       1

1     4     0                                                0        0

1     5     0                                                0        0

Router(config)# exit
Router#
```

CHAPTER 13
Wireless Frame Capture

This chapter shows you how to configure and use wireless frame capture on the NXC.

13.1 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 NXC 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.

13.2 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 51 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_dir_size	The total combined size (in kbytes) of all files to be captured. The maximum you can set is 50 megabtyes (52428800 bytes.)
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 52 Command Summary: Wireless Frame Capture

COMMAND	DESCRIPTION
`frame-capture configure`	Enters sub-command mode for wireless frame capture.
`src-ip {add|del} {ipv4_address | local}`	Sets or removes the IPv4 address of an AP controlled by the NXC 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_dir_size`	Sets the total combined size (in kbytes) of all 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.

13.2.1 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 14
Dynamic Channel Selection

This chapter shows you how to configure and use dynamic channel selection on the NXC.

14.1 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.

14.2 DCS Commands

See Section 10.2 on page 87 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 53 Command Summary: DCS

COMMAND	DESCRIPTION
`dcs now`	Sets the managed APs to scan for and select an available channel immediately.

CHAPTER 15
Auto-Healing

This chapter shows you how to configure auto-healing settings.

15.1 Auto-Healing Overview

Auto-healing allows you to extend the wireless service coverage area of the managed APs when one of the managed APs fails.

15.2 Auto-Healing Commands

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

Table 54 Input Values for Auto-Healing Commands

LABEL	DESCRIPTION
interval	Enters the auto-healing interval time. The range is 5 ~ 30 minutes.

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

Table 55 Command Summary: Auto-Healing

COMMAND	DESCRIPTION
`[no] auto-healing activate`	Turns on the auto-healing feature. Use the `no` parameter to turn it off.
`auto-healing healing-interval` *interval*	Sets the interval that specifies how often the managed APs scan their neighborhoods and report the status of neighbor APs to the AP controller (NXC). An AP is considered "failed" if the AP controller obtains the same scan result that the AP is missing from the neighbor list of other APs three times.
`auto-healing healing-threshold`	Sets a minimum signal strength. A managed AP is added to the neighbor lists only when the signal strength of the AP is stronger than the specified threshold.
`auto-healing power-threshold <-50~-80>`	Sets a power threshold (in dBm). This value is used to calculate the power level (`power-threshold` + `margin`) to which the neighbor APs of the failed AP increase their output power in order to extend their wireless service coverage areas. When the failed AP is working again, its neighbor APs return their output power to the original level.

Table 55 Command Summary: Auto-Healing (continued)

COMMAND	DESCRIPTION
auto-healing margin	Enters a number from 0 to 9. This value is used to calculate the power level (power-threshold + margin) to which the neighbor APs of the failed AP increase their output power in order to extend their wireless service coverage areas.
auto-healing update	Sets all manged APs to immediately scan their neighborhoods three times in a row and update their neighbor lists to the AP controller (NXC).
show auto-healing config	Displays the current auto-healing configuration.

15.2.1 Auto-Healing Examples

This example enables auto-healing and sets the power level (in dBm) to which the neighbor APs of the failed AP increase their output power.

```
Router(config)# auto-healing activate
Router(config)# auto-healing power-threshold -70
Router(config)# show auto-healing config
auto-healing activate: yes
auto-healing interval: 10
auto-healing power threshold: -70 dBm
auto-healing healing threshold: -85 dBm
auto-healing margin: 0
Router(config)#
```

CHAPTER 16
Dynamic Guest

This chapter shows you how to configure dynamic guest accounts.

16.1 Dynamic Guest Overview

Dynamic guest accounts are guest accounts, but are created dynamically with the guest manager account and stored in the NXC's local user database. A dynamic guest account user can access the NXC's services only within a given period of time and will become invalid after the expiration date/time. A dynamic guest account has a dynamically-created user name and password. You cannot modify or edit a dynamic guest account.

16.2 Dynamic Guest Commands

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

Table 56 Command Summary: Dynamic Guest

COMMAND	DESCRIPTION
`username` *`username`* `password` *`password`* `user-type guest-manager`	Creates a guest-manager user account to generate dynamic guest accounts.
`users default-setting [no] user-type dynamic-guest logon-lease-time <0~1440>`	Sets the default lease time for the dynamic guests. Set it to zero to set unlimited lease time. The `no` command sets the lease time to five minutes.
`users default-setting [no] user-type dynamic-guest logon-re-auth-time <0~1440>`	Sets the default reauthorization time for the dynamic guests. Set it to zero to set unlimited reauthorization time. The `no` command sets the reauthorization time to thirty minutes.
`users default-setting user-type guest-manager logon-lease-time <0~1440>`	Sets the default lease time for the guest-manager user. Set it to zero to set unlimited lease time. The `no` command sets the lease time to five minutes.
`users default-setting user-type guest-manager logon-re-auth-time <0~1440>`	Sets the default reauthorization time for the guest-manager user. Set it to zero to set unlimited reauthorization time. The `no` command sets the reauthorization time to thirty minutes.
`[no] groupname` *`groupname`*	Creates the specified user group if necessary and enters sub-command mode. The `no` command deletes the specified user group.

Table 56 Command Summary: Dynamic Guest (continued)

COMMAND	DESCRIPTION
[no] description *description*	Sets the description for the specified user group. The no command clears the description for the specified user group.
dynamic-guest group	Sets this group as a dynamic guest group.
dynamic-guest enable expired-account deleted	Sets the NXC to remove the dynamic guest accounts from the NXC's local database when they expire.
dynamic-guest generate [username *user_name*]	Creates one dynamic guest user. Alternatively, you can enter a user name to create one dynamic guest user with the specified user name. Note: You must configure an expiration date and a dynamic guest group in order to generate dynamic guest users.
address *address*	Sets the geographic address for the dynamic guest user.
company *company*	Sets the company name for the dynamic guest user.
e-mail *mail*	Sets the E-mail address for the dynamic guest user.
encrypted-password *password*	Turns on data encryption. Data transmitted between the NXC and the user will be encrypted with a password.
expire-time *yyyy-mm-dd hh:mm*	Sets the date and time when the dynamic guest user account becomes invalid.
group *groupname*	Sets the name of the dynamic guest group with which the dynamic guest user is associated.
name *real-name*	Sets the name for the dynamic guest user.
others *description*	Sets the additional information for the dynamic guest user.
password *password*	Sets the password for the dynamic guest user.
phone *phone-number*	Sets the telephone number for the dynamic guest user.
dynamic-guest generate <2~32>	Creates multiple dynamic guest users at a time. Note: You must configure an expiration date and a dynamic guest group in order to generate dynamic guest users.
address *address*	Sets the geographic address for the dynamic guest user.
company *company*	Sets the company name for the dynamic guest user.
expire-time *yyyy-mm-dd hh:mm*	Sets the date and time when the dynamic guest user account becomes invalid.
group *groupname*	Sets the name of the dynamic guest group with which the dynamic guest user is associated.
others *description*	Sets the additional information for the dynamic guest user.
[no] dynamic-guest message-text *note*	Sets the notes that display in the paper along with the account information you print out for dynamic guest users. The no command removes the notes that you configure.
dynamic-guest username-password-length {4|5|6}	Sets the length of a user name and password for dynamic guest user accounts.
no dynamic-guest *username*	Deletes the specified guest-manager user account.

Table 56 Command Summary: Dynamic Guest (continued)

COMMAND	DESCRIPTION
no dynamic-guest expired-account deleted	Sets the NXC to not remove the dynamic guest accounts when they expire.
show dynamic-guest status	Displays dynamic guest general settings.
show dynamic-guest	Displays information about the dynamic guests.

16.2.1 Dynamic Guest Examples

This example creates a guest-manager user account and a dynamic-guest user group, then sets the NXC to generate two dynamic-guest accounts automatically. This also shows the dynamic guest users information.

```
Router(config)# username GuestMaster password 4321 user-type guest-manager
Router(config)# groupname dynamic-guest
Router(group-user)# dynamic-guest group
Router(group-user)# exit
Router(config)# dynamic-guest generate 2
Router(config-dynamic-guest)# company example
Router(config-dynamic-guest)# group dynamic-guest
Router(config-dynamic-guest)# expire-time 2018-06-16 14:00
Router(config-dynamic-guest)# exit
[dynamic guest] username:N84AVAJN, password:QAA3KJ63
[dynamic guest] username:S6F8PZ3N, password:66DA3BCX
Router(config)# show dynamic-guest
Client: N84AVAJN
  guest name:
  phone:
  e-mail:
  address:
  company: example
  expire time: 2018-06-16 14:00
  group: dynamic-guest
  others:
  expire: no
Client: S6F8PZ3N
  guest name:
  phone:
  e-mail:
  address:
  company: example
  expire time: 2018-06-16 14:00
  group: dynamic-guest
  others:
  expire: no
Router(config)#
```

CHAPTER 17
LEDs

This chapter describes two features that controls the LEDs of the managed APs connected to your NXC - Locator and Suppression.

17.1 LED Suppression Mode

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

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

17.2 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 57 LED Suppression Commands

COMMAND	DESCRIPTION
`led_suppress` *ap_mac_address* `enable`	Sets the LEDs of the specified AP to turn off after it's ready.
`led_suppress` *ap_mac_address* `disable`	Sets the LEDs of the specified AP to stay lit after the NXC is ready.
`show led_suppress` *ap_mac_address* `status`	Displays whether LED suppression mode is enabled or disabled on the specified AP.

17.2.1 LED Suppression Commands Example

The following example activates LED suppression mode on the AP with the MAC address 00:a0:c5:01:23:45 and displays the settings.

```
Router(config)# led_suppress 00:a0:c5:01:23:45 enable
Router(config)# show led_suppress 00:a0:c5:01:23:45 status
Suppress Mode Status : Enable
Router(config)#
```

17.3 LED Locator

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

17.4 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 58 LED Locator Commands

COMMAND	DESCRIPTION
`led_locator` *ap_mac_address* `on`	Enables the LED locator function on the specified AP. It will show the actual location of the AP between several devices in the network.
`led_locator` *ap_mac_address* `off`	Disables the LED locator function on the specified AP.
`led_locator` *ap_mac_address* `blink-timer <1..60>`	Sets a time interval between 1 and 60 minutes to stop the locator LED from blinking on the specified AP. Note: You should run this command before enabling the LED locator function.
`show led_locator` *ap_mac_address* `status`	Displays whether LED locator function is enabled on the specified AP and the timer setting.

17.4.1 LED Locator Commands Example

The following example turns on the LED locator feature on the AP with the MAC address 00:a0:c5:01:23:45, sets how long the locator LED stays blinking, and also displays the settings.

```
Router(config)# led_locator 00:a0:c5:01:23:45 blink-timer 5
Router(config)# led_locator 00:a0:c5:01:23:45 on
Router(config)# show led_locator 00:a0:c5:01:23:45 status
Locator LED Status : ON
Locator LED Time : 5
Router(config)#
```

CHAPTER 18
Zones

Set up zones to configure network security and network policies in the NXC.

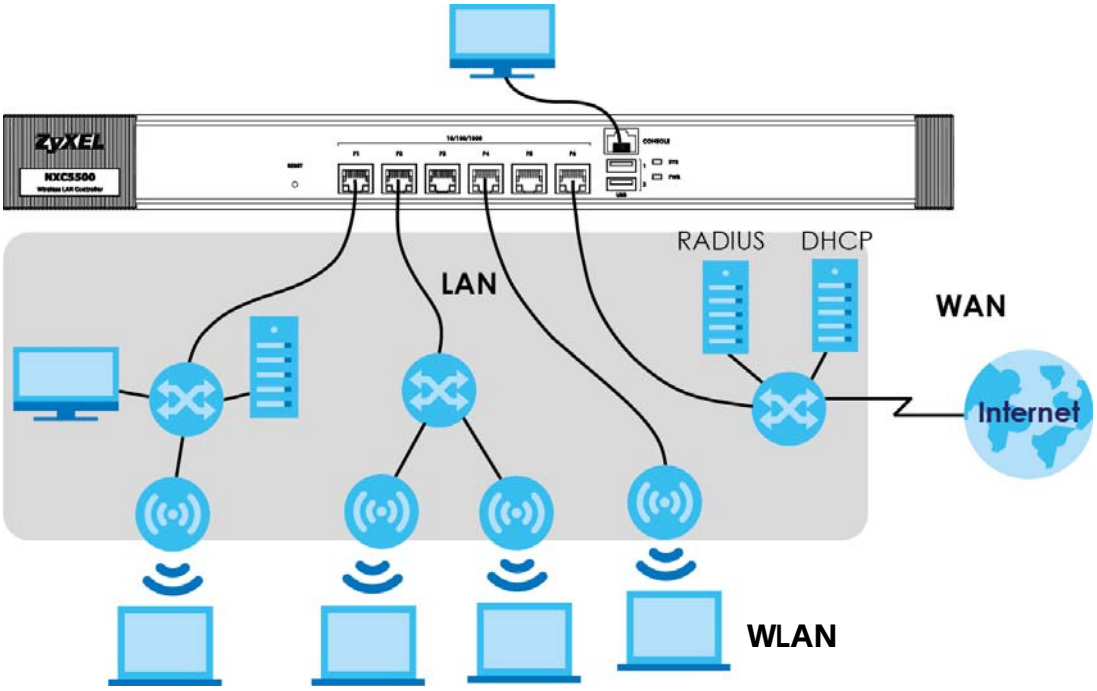
Note: Use the `configure terminal` command to enter Configuration mode in order to use the commands described in this chapter.

18.1 Zones Overview

A zone is a group of interfaces. The NXC uses zones, not interfaces, in many security and policy settings, such as firewall rules and remote management.

Zones cannot overlap. Each Ethernet interface or VLAN interface can be assigned to at most one zone.

Figure 12 Example: Zones



18.2 Zone Commands Summary

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

Table 59 Input Values for Zone Commands

LABEL	DESCRIPTION
profile_name	The name of a zone. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.

This table lists the zone commands.

Table 60 zone Commands

COMMAND	DESCRIPTION
show zone [*profile_name*]	Displays information about the specified zone or about all zones.
show zone binding-iface	Displays each interface and zone mappings.
show zone none-binding	Displays the interfaces that are not associated with a zone yet.
show zone user-define	Displays all customized zones.
[no] zone *profile_name*	Creates the zone if necessary and enters sub-command mode. The no command deletes the zone.
zone *profile_name*	Enter the sub-command mode.
[no] block	Blocks intra-zone traffic. The no command allows intra-zone traffic.
[no] interface *interface_name*	Adds the specified interface to the specified zone. The no command removes the specified interface from the specified zone.
exit	Exits the sub-command mode for this zone.

18.2.1 Zone Command Examples

The following commands add Ethernet interfaces ge1 and ge2 to zone A and block intra-zone traffic.

```
Router# configure terminal
Router(config)# zone A
Router(zone)# interface ge1
Router(zone)# interface ge2
Router(zone)# block
Router(zone)# exit
Router(config)# show zone
No. Name                            Block  Member
==============================================================================
1   A                                 yes    ge1,ge2
Router(config)# show zone A
blocking intra-zone traffic: yes
No. Type                            Member
==============================================================================
1   interface                       ge1
2   interface                       ge2
```

CHAPTER 19
ALG

This chapter covers how to use the NXC's ALG feature to allow certain applications to pass through the NXC.

19.1 ALG Introduction

The NXC can function as an Application Layer Gateway (ALG) to allow certain NAT un-friendly applications (such as SIP) to operate properly through the NXC's NAT.

Some applications cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload. The NXC examines and uses IP address and port number information embedded in the VoIP traffic's data stream. When a device behind the NXC uses an application for which the NXC has VoIP pass through enabled, the NXC translates the device's private IP address inside the data stream to a public IP address. It also records session port numbers and allows the related sessions to go through the firewall so the application's traffic can come in from the WAN to the LAN.

The NXC only needs to use the ALG feature for traffic that goes through the NXC's NAT. The firewall allows related sessions for VoIP applications that register with a server. The firewall allows or blocks peer to peer VoIP traffic based on the firewall rules.

You do not need to use a TURN (Traversal Using Relay NAT) server for VoIP devices behind the NXC when you enable the SIP ALG.

19.2 ALG Commands

The following table lists the `alg` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 61 alg Commands

COMMAND	DESCRIPTION
`[no] alg sip [inactivity-timeout | signal-port <1025..65535> | signal-extra-port <1025..65535> | media-timeout <1..86400> | signal-timeout <1..86400> | transformation]`	Turns on or configures the ALG. Use `inactivity-timeout` to have the NXC apply SIP media and signaling inactivity time out limits. Use `signal-port` with a listening port number (1025 to 65535) if you are using SIP on a port other than UDP 5060. Use `signal-extra-port` with a listening port number (1025 to 65535) if you are also using SIP on an additional UDP port number, enter it here. Use `media-timeout` and a number of seconds (1~86400) for how long to allow a voice session to remain idle (without voice traffic) before dropping it. Use `signal-timeout` and a number of seconds (1~86400) for how long to allow a SIP signaling session to remain idle (without SIP packets) before dropping it. Use `transformation` to have the NXC modify IP addresses and port numbers embedded in the SIP data payload. You do not need to use this if you have a SIP device or server that will modify IP addresses and port numbers embedded in the SIP data payload. The `no` command turns off the SIP ALG or removes the settings that you specify.
`[no] alg <h323 | ftp> [signal-port <1025..65535> | signal-extra-port <1025..65535> | transformation]`	Turns on or configures the H.323 or FTP ALG. Use `signal-port` with a listening port number (1025 to 65535) if you are using H.323 on a TCP port other than 1720 or FTP on a TCP port other than 21. Use `signal-extra-port` with a listening port number (1025 to 65535) if you are also using H.323 or FTP on an additional TCP port number, enter it here. Use `transformation` to have the NXC modify IP addresses and port numbers embedded in the H.323 or FTP data payload. You do not need to use this if you have an H.323 or FTP device or server that will modify IP addresses and port numbers embedded in the H.323 or FTP data payload. The `no` command turns off the H.323 or FTP ALG or removes the settings that you specify.
`[no] alg sip defaultport <1..65535>`	Adds (or removes) a custom UDP port number for SIP traffic.
`show alg <sip | h323 | ftp>`	Displays the specified ALG's configuration.

19.3 ALG Commands Example

The following example turns on pass through for SIP and turns it off for H.323.

```
Router# configure terminal
Router(config)# alg sip
Router(config)# no alg h323
```

CHAPTER 20
Captive Portal

This chapter describes how to configure which HTTP-based network services default to the captive portal page when client makes an initial network connection.

20.1 Captive Portal Overview

A captive portal can intercept all network traffic, regardless of address or port, until the user authenticates his or her connection, usually through a specifically designated login Web page.

20.1.1 Web Authentication Policy Commands

Use these commands to use a custom login page from an external web portal instead of the default one built into the NXC. You can configure the look and feel of the web portal page.

Note: It is recommended to have the external web server on the same subnet as the login users.

Table 62 Web Authentication Policy Commands

COMMAND	DESCRIPTION
`[no] web-auth activate`	Turns on the captive portal feature. This blocks all network traffic until the client authenticates with the NXC through the external web portal page. The `no` command turns off the external web portal feature.
`web-auth ap-auth-policy-group` *`ap_auth_policy_group_name`*	Adds an authentication policy group for a group of managed APs. See Table 63 on page 132 for the sub-commands.
`web-auth ap-auth-policy-group` *`rename ap_auth_policy_group_name1 ap_auth_policy_group_name2`*	Gives an existing AP authentication policy group (*`ap_auth_policy_group_name1`*) a new name (*`ap_auth_policy_group_name2`*).
`web-auth ap-policy-rule` *`ap_auth_policy_name`*	Adds an authentication policy for a policy group or individual managed AP. See Table 64 on page 132 for the sub-commands.
`web-auth ap-policy-rule rename` *`ap_auth_policy_name1 ap_auth_policy_name2`*	Gives an existing AP authentication policy rule (*`ap_auth_policy_name1`*) a new name (*`ap_auth_policy_name2`*).

Table 62 Web Authentication Policy Commands (continued)

COMMAND	DESCRIPTION
`web-auth default-rule authentication {required | unnecessary} {no log | log [alert]}`	Sets the default authentication policy the NXC uses on traffic not matching any exceptional service or other authentication policy. `required`: Users need to be authenticated. Users must manually go to the NXC's login screen (the NXC does not redirect them to it). `unnecessary`: Users do not need to be authenticated. `no log | log [alert]`: Select whether to have the NXC generate a log (`log`), log and alert (`log alert`) or not (`no log`) for packets that match this default policy.
`web-auth [no] exceptional-service` *`service_name`*	Lets users access a service without user authentication. The `no` command removes the specified service from the exception list. *`service_name`*: the name of network service, such as AH or DNS.
`web-auth local-mac-db` *`ssid_profile_name`* `<1..168>`	Sets the MAC caching time (in hours) for an SSID profile. The wireless client that connects to the specified SSID has to log into the network via captive portal after the seesion times out.
`web-auth no local-mac-db-cache` *`mac_address ssid_profile_name`*	Disconnect a MAC address from the specified SSID. The client device of the MAC address needs to log in via the captive portal page next time he/she wants to connect to the same SSID.
`web-auth logout-ip` *`ip`*	Sets an IP address that users can use to terminate their sessions manually by entering the IP address in the address bar of the web browser. Note: The manual logout IP will not work if web authentication is disabled using the `portal-type 3` sub-command.
`web-auth logout-ip none`	Removes the specified logout IP address.
`web-auth policy <1..1024>`	Creates the specified condition for forcing user authentication, if necessary, and enters sub-command mode. The NXC checks the conditions in sequence, starting at 1. See Table 65 on page 134 for the sub-commands.
`web-auth policy append`	Creates a new condition for forcing user authentication at the end of the current list and enters sub-command mode. See Table 65 on page 134 for the sub-commands.
`web-auth policy delete <1..1024>`	Deletes the specified condition.
`web-auth policy flush`	Deletes all the conditions for forcing user authentication.
`web-auth policy insert <1..1024>`	Creates a new condition for forcing user authentication at the specified location, renumbers the other conditions accordingly, and enters sub-command mode. See Table 65 on page 134 for the sub-commands.
`web-auth policy move <1..1024> to <1..1024>`	Moves the specified condition to the specified location and renumbers the other conditions accordingly.
`show web-auth activation`	Displays whether forcing user authentication is enabled or not.
`show web-auth ap-auth-policy-group {all |` *`ap_auth_policy_group_name`*`}`	Displays details about all AP authentication policy groups or the specified policy group.
`show web-auth ap-policy-rule {all |` *`ap_auth_policy_name`*`}`	Displays details about all AP authentication policies or the specified policy.
`show web-auth authentication`	Displays the name of authentication method used for the captive portal page.

Table 62 Web Authentication Policy Commands (continued)

COMMAND	DESCRIPTION
show web-auth default-rule	Displays the default captive portal authentication settings the NXC uses on traffic not matching any exceptional service or other authentication policy.
show web-auth exceptional-service	Displays services that users can access without user authentication.
show web-auth local-mac-db	Displays the SSID profile's MAC caching time,
show web-auth local-mac-db-cache	Displays a list of MAC addresses, which are authenticated and allowed to access the network.
show web-auth logout-ip	Displays the IP address that users can use to terminate their sessions manually.
show web-auth policy {<1..1024> | all}	Displays details about the policies for forcing user authentication.

20.1.1.1 web-auth ap-auth-policy-group Sub-commands

The following table describes the sub-commands for the `web-auth ap-auth-policy-group` command.

Table 63 web-auth ap-auth-policy-group Sub-commands

COMMAND	DESCRIPTION
[no] description *description*	Sets the description for the policy group. The no command clears the description. *description*: You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 61 characters long.
[no] web-auth-policy <1..8> *ap_policy_rule_name*	Adds the specified AP authentication policy to the policy group. The no command removes the AP authentication policy.

20.1.1.2 web-auth ap-policy-rule Sub-commands

The following table describes the sub-commands for the `web-auth ap-policy-rule` command.

Table 64 web-auth ap-policy-rule Sub-commands

COMMAND	DESCRIPTION
[no] activate	Activates the policy. The no command deactivates the policy.
[no] authentication {force | required}	Selects the authentication requirement for users with traffic matching this policy. The no command requires no user authentication. force: Users need to be authenticated. The NXC automatically displays the login screen if unauthenticated users try to send HTTP traffic. required: Users need to be authenticated. They must manually go to the login screen. The NXC does not redirect them to the login screen.
authentication-method *auth_method*	Sets the authentication method for the captive portal.

Table 64 web-auth ap-policy-rule Sub-commands (continued)

COMMAND	DESCRIPTION
[no] description *description*	Sets the description for the policy. The no command clears the description. *description*: You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 61 characters long.
[no] destination *address_object*	Sets the destination criteria for the specified policy. The no command removes the destination criteria, making the condition effective for all destinations.
[no] external error-url <*url*>	Sets the error page's URL; for example: http://192.168.1.1/error.html. 192.168.1.1 is the web server on which the web portal files are installed. Use the no command to remove the specified URL.
[no] external login-url <*url*>	Sets the login page's URL; for example: http://192.168.1.1/login.html. 192.168.1.1 is the web server on which the web portal files are installed. Use the no command to remove the specified URL.
[no] external logout-url <*url*>	Sets the logout page's URL; for example: http://192.168.1.1/logout.html. 192.168.1.1 is the web server on which the web portal files are installed. Use the no command to remove the specified URL.
[no] external session-url <*url*>	Sets the session page's URL; for example: http://192.168.1.1/session.html. 192.168.1.1 is the web server on which the web portal files are installed. Use the no command to remove the specified URL.
[no] external userlogout-url <*url*>	Sets the URL of the page from which users can terminate their sessions; for example, http://192.168.1.1/userlogout.html. 192.168.1.1 is the web server on which the web portal files are installed. Use the no command to remove the specified URL.
[no] external welcome-url <*url*>	Sets the welcome page's URL; for example: http://192.168.1.1/welcome.html. 192.168.1.1 is the web server on which the web portal files are installed. Use the no command to remove the specified URL.
internal-portal-page *theme_name*	Sets the internal portal-page theme from default, customized or uploaded theme.
portal-type {0 | 1 | 2}	Sets which login page appears whenever the web portal intercepts network traffic, preventing unauthorized users from gaining access to the network. **0 -** internal: Use the default login page built into the NXC. **1-** external: Use a custom login page from an external web portal. You can configure the look and feel of the web portal page. **2-** no authentication: Disable web authentication. Note: If setting portal-type to 2, you must use the promotion-url command to configure a web site address, to which the users will be redirected.

Table 64 web-auth ap-policy-rule Sub-commands (continued)

COMMAND	DESCRIPTION
[no] promotion-url <*url*>	Sets the URL or IP address of the web page, that displays as the first web page when the user connects to the Internet. Use "http://" followed by up to 262 characters (0-9a-zA-Z;/ ?:@&=+$\.-_!~*'()%). For example, http://www.example.com or http://172.16.1.35. Use the no command to remove the specified web site address.
[no] schedule *schedule_name*	Sets the time criteria for the specified policy. The no command removes the time criteria, making the condition effective all the time.
[no] source *address_object*	Sets the source criteria for the specified policy. The no command removes the source criteria, so all sources match the condition.
[no] ssid_profile {*ssid_profile*}	Sets the SSID profile criteria for the specified condition. The no command removes the SSID profile criteria.

20.1.1.3 web-auth policy Sub-commands

The following table describes the sub-commands for several web-auth policy commands. Note that not all rule commands use all the sub-commands listed here.

Table 65 web-auth policy Sub-commands

COMMAND	DESCRIPTION
[no] activate	Activates the specified condition. The no command deactivates the specified condition.
[no] authentication {force | required}	Selects the authentication requirement for users with traffic matching this policy. The no command requires no user authentication. force: Users need to be authenticated. The NXC automatically displays the login screen if unauthenticated users try to send HTTP traffic. required: Users need to be authenticated. They must manually go to the login screen. The NXC does not redirect them to the login screen.
authentication-method *auth_method*	Sets the authentication method for the captive portal.
[no] description *description*	Sets the description for the specified condition. The no command clears the description. *description*: You can use alphanumeric and ()+/ :=?!*#@$_%- characters, and it can be up to 61 characters long.
[no] destination *address_object*	Sets the destination criteria for the specified condition. The no command removes the destination criteria, making the condition effective for all destinations.
[no] external error-url <*url*>	Sets the error page's URL; for example: http://192.168.1.1/error.html. 192.168.1.1 is the web server on which the web portal files are installed. Use the no command to remove the specified URL.

Table 65 web-auth policy Sub-commands (continued)

COMMAND	DESCRIPTION
[no] external login-url <*url*>	Sets the login page's URL; for example: http://192.168.1.1/login.html. 192.168.1.1 is the web server on which the web portal files are installed. Use the no command to remove the specified URL.
[no] external logout-url <*url*>	Sets the logout page's URL; for example: http://192.168.1.1/logout.html. 192.168.1.1 is the web server on which the web portal files are installed. Use the no command to remove the specified URL.
[no] external session-url <*url*>	Sets the session page's URL; for example: http://192.168.1.1/session.html. 192.168.1.1 is the web server on which the web portal files are installed. Use the no command to remove the specified URL.
[no] external userlogout-url <*url*>	Sets the URL of the page from which users can terminate their sessions; for example, http://192.168.1.1/userlogout.html. 192.168.1.1 is the web server on which the web portal files are installed. Use the no command to remove the specified URL.
[no] external welcome-url <*url*>	Sets the welcome page's URL; for example: http://192.168.1.1/welcome.html. 192.168.1.1 is the web server on which the web portal files are installed. Use the no command to remove the specified URL.
[no] force	Forces users that match the specified condition to log into the NXC. The no command means users matching the specified condition do not have to log into the NXC.
internal-portal-page *theme_name*	Sets the internal portal-page theme from default, customized or uploaded theme.
[no] internal-redirect-fqdn <*redirect_fqdn*>	Sets the Fully-Qualified Domain Name (FQDN) of the NXC interface to which the clients connect. This is the internal login page's URL. Use the no command to remove the specified FQDN.
portal-type {0 | 1 | 2}	Sets which login page appears whenever the web portal intercepts network traffic, preventing unauthorized users from gaining access to the network. **0 -** internal: Use the default login page built into the NXC. **1-** external: Use a custom login page from an external web portal. You can configure the look and feel of the web portal page. **2-** no authentication: Disable web authentication. Note: If setting portal-type to 2, you must use the promotion-url command to configure a web site address, to which the users will be redirected.
[no] promotion-url <*url*>	Sets the URL or IP address of the web page, that displays as the first web page when the user connects to the Internet. Use "http://" followed by up to 262 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%). For example, http://www.example.com or http://172.16.1.35. Use the no command to remove the specified web site address.

Table 65 web-auth policy Sub-commands (continued)

COMMAND	DESCRIPTION
[no] qrcode auth-assisted-authenticator *user_name*	Sets the user account or user group that acts as an authenticator. The authenticator assists clients in authentication with a QR code. The authenticator must be able to access the IP address of the specified VLAN interface. Use the no command to remove the specified authenticator.
[no] qrcode auth-assisted-vlan *vlan_iface*	Sets the VLAN interface on the NXC, through which the client is allowed to access the NXC. Use the no command to remove the specified VLAN interface.
[no] qrcode auth-type {all | auth-assisted | self-assisted}	Sets how the clients authenticate with a QR code to log into the web site. auth-assisted: display the QR code on the captive portal login page. Clients can log in by entering the guest account information. They can also have the specified authenticator help to scan the QR code to authenticate. self-assisted: allow clients themselves to scan the QR code (printed out by the administrator) to log into the web site. all: clients can use either way to log in. Use the no command to reset the setting to its default value (no).
[no] qrcode guest-account *user_name*	Sets a user or guest account. Clients that authenticate with a QR code are represented by this account name in the user list. Use the no command to remove the specified account.
[no] qrcode qrcode-activate	Makes this profile active or inactive.
[no] qrcode self-assisted-message <*message*>	Sets the notes you want to display along with the QR code. Use the no command to remove the specified notes.
[no] qrcode self-assisted-vlan *vlan_iface*	Sets a VLAN interface on the NXC, through which the client is allowed to access the NXC. Use the no command to remove the specified VLAN interface.
[no] schedule *schedule_name*	Sets the time criteria for the specified condition. The no command removes the time criteria, making the condition effective all the time.
[no] source *address_object*	Sets the source criteria for the specified condition. The no command removes the source criteria, so all sources match the condition.
show	Displays information about the specified condition.

20.1.1.4 Web Authentication Policy Insert Command Example

Here is an example of using a custom login page from an external web portal for web authentication. The following commands:

- Turn on web authentication
- Set the NXC to use the authentication profile named AuthProfile1
- Set www.login.com as the login web page through which users authenticate their connections
- Have the NXC use a custom login page from an external web portal instead of the default one built into the NXC
- Create web-auth policy 1

- Set web-auth policy 1 to use the SSID profile named SSIDprofile1
- Set web-auth policy 1 to require user authentication
- Have the NXC automatically display the login screen when unauthenticated users try to send HTTP traffic
- Turn on web-auth policy 1

```
Router(config)# web-auth activate
Router(config)# web-auth policy insert 1
Router(config-web-auth-1)# authentication force
Router(config-web-auth-1)# activate
Router(config-web-auth-1)# authentication-method default
Router(config-web-auth-1)# portal-type 0
Router(config-web-auth-1)# exit
```

20.1.2 Customizing the WWW Login Page

Use these commands to customize the Web Configurator login screen. You can also customize the page that displays after an access user logs into the Web Configurator to access network services like the Internet.

The following figures identify the parts you can customize in the login, access, and user-logout pages.

Figure 13 Login Page Customization

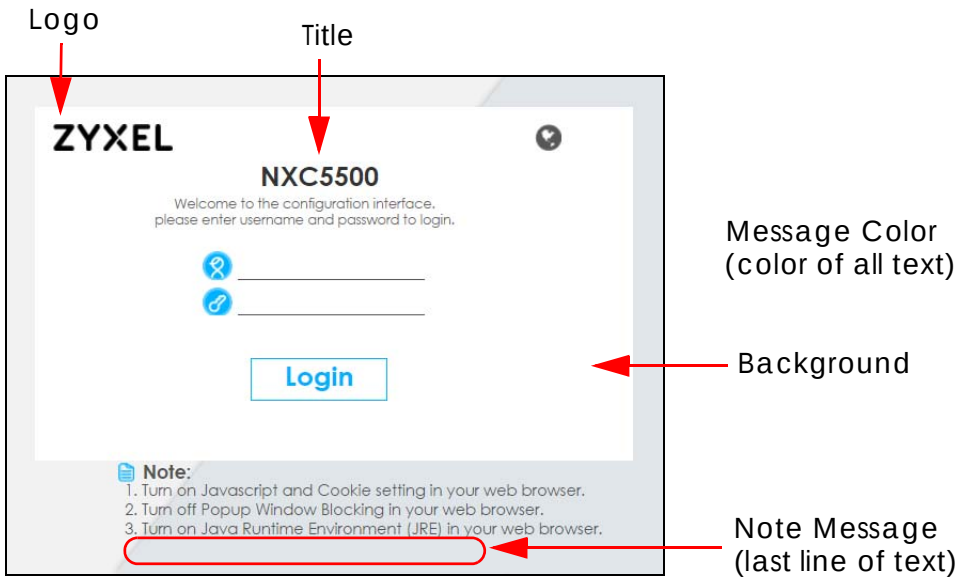


Figure 14 Access Page Customization

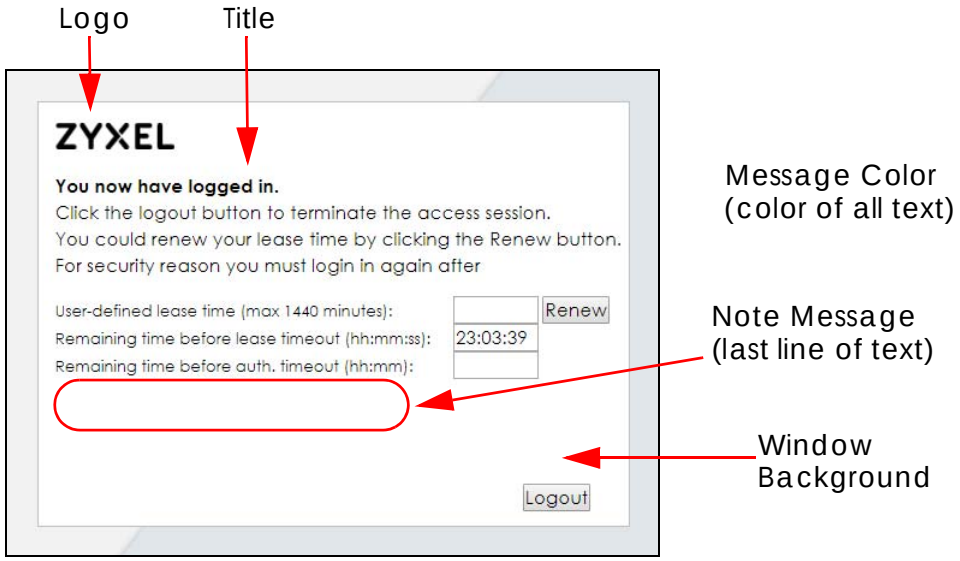
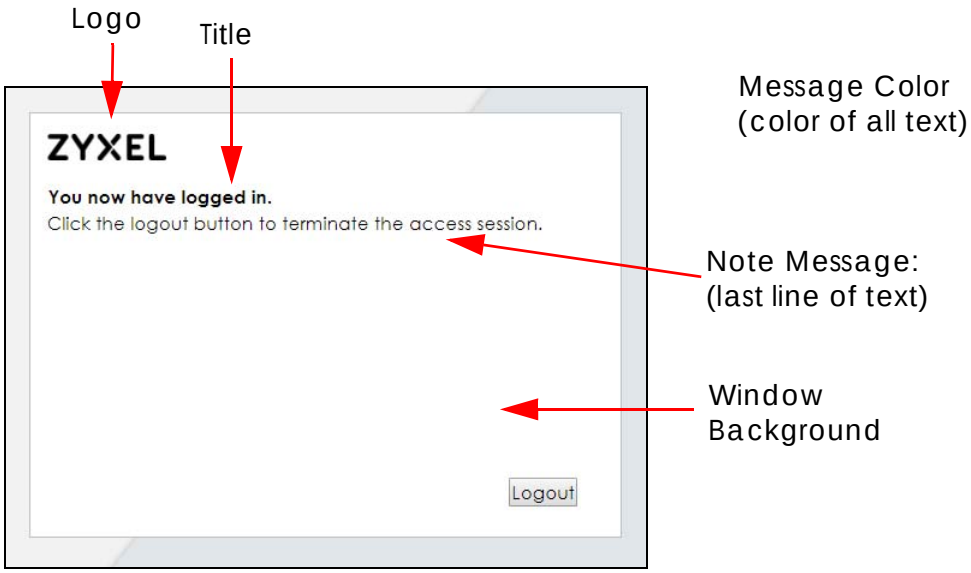


Figure 15 User Logout Customization



You can specify colors in one of the following ways:

- *color-rgb*: Enter red, green, and blue values in parenthesis and separate by commas. For example, use “rgb(0,0,0)” for black.
- *color-name*: Enter the name of the desired color.
- *color-number*: Enter a pound sign (#) followed by the six-digit hexadecimal number that represents the desired color. For example, use “#000000” for black.

The following table describes the commands available for customizing the Web Configurator login screen, user logout screen and the page that displays after an access user logs into the Web

Configurator to access network services like the Internet. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 66 Command Summary: Customization

COMMAND	DESCRIPTION
customized-page *theme_name*	Enters the sub-command mode for page customization.
access-page color-window-background {yes | no}	Sets whether or not the access page uses a colored background.
access-page-message-color {*color-rgb* | *color-name* | *color-number*}	Sets the color of the message text on the access page.
[no] access-page message-text *message*	Sets a note to display below the access page's title. Use up to 64 printable ASCII characters. Spaces are allowed.
access-page-title <title>	Sets the title for the top of the access page. Use up to 64 printable ASCII characters. Spaces are allowed.
access-page-window-color {*color-rgb* | *color-name* | *color-number*}	Sets the color of the access page's colored background.
login-page-background-color {*color-rgb* | *color-name* | *color-number*}	Sets the color of the login page's background.
login-page-color-background {yes | no}	Sets the login page to use a solid colored background.
login-page-message-color {*color-rgb* | *color-name* | *color-number*}	Sets the color of the message text on the login page.
[no] login-page-message-text *message*	Sets a note to display at the bottom of the login screen. Use up to 64 printable ASCII characters. Spaces are allowed.
login-page-title *title*	Sets the title for the top of the login screen. Use up to 64 printable ASCII characters. Spaces are allowed.
login-page-title-color {*color-rgb* | *color-name* | *color-number*}	Sets the title text color of the login page.
userlogout-page-color-window-background {*yes* | *no*}	Sets whether or not the user logout page uses a colored background.
userlogout-page-message-color {*color-rgb* | *color-name* | *color-number*}	Sets the color of the message text on the user logout page.
userlogout-page-message-text *message*	Sets a note to display at the bottom of the user logout screen. Use up to 64 printable ASCII characters. Spaces are allowed.
userlogout-page-title *title*	Sets the title for the top of the user logout screen. Use up to 64 printable ASCII characters. Spaces are allowed.
userlogout-page-window-color {*color-rgb* | *color-name* | *color-number*}	Sets the color of the user logout screen's colored background.
show customized-page {*theme_name* | all}	Lists specific or all customized-page settings.
show login-page default-title	Lists the factory default title for the login page.
show login-page settings	Lists the current login page settings.

Table 66 Command Summary: Customization (continued)

COMMAND	DESCRIPTION
`show logo settings`	Lists the current logo background (banner) and floor (line below the banner) settings.
`show page-customization`	Lists whether the NXC is set to use custom login and access pages or the default ones.

CHAPTER 21
RTLS

Use the RTLS commands to use the managed APs as part of an Ekahau RTLS to track the location of Ekahau Wi-Fi tags.

21.1 RTLS Introduction

Ekahau RTLS (Real Time Location Service) tracks battery-powered Wi-Fi tags attached to APs managed by the NXC to create maps, alerts, and reports.

The Ekahau RTLS Controller is the centerpiece of the RTLS system. This server software runs on a Windows computer to track and locate Ekahau tags from Wi-Fi signal strength measurements. Use the NXC with the Ekahau RTLS system to take signal strength measurements at the APs (Integrated Approach / Blink Mode).

21.2 RTLS Commands

The following table lists the `rtls` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 67 rtls Commands

COMMAND	DESCRIPTION
`rtls ekahau activate`	Turn on RTLS to use Wi-Fi to track the location of Ekahau Wi-Fi tags.
`rtls ekahau ip address` *`ipv4_address`*	Specify the IP address of the Ekahau RTLS Controller.
`rtls ekahau ip port <1..65535>`	Specify the server port number of the Ekahau RTLS Controller.
`rtls ekahau flush`	Clear the saved RTLS information from the NXC.
`show rtls ekahau config`	Displays the RTLS configuration.
`show rtls ekahau cli`	Displays the RTLS information recorded on the NXC.

CHAPTER 22
Firewall

This chapter introduces the NXC's firewall and shows you how to configure your NXC's firewall.

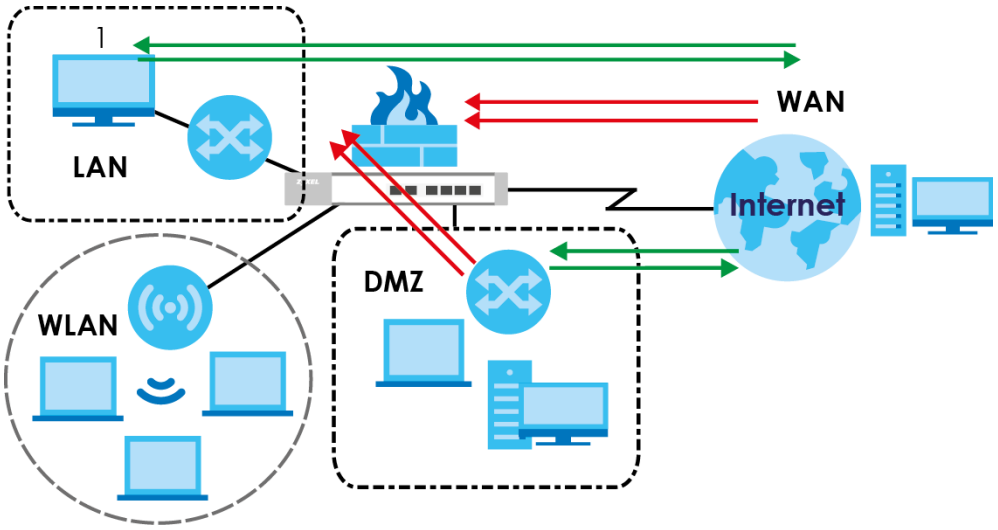
22.1 Firewall Overview

The NXC's firewall is a stateful inspection firewall. The NXC restricts access by screening data packets against defined access rules. It can also inspect sessions. For example, traffic from one zone is not allowed unless it is initiated by a computer in another zone first.

A zone is a group of interfaces. Group the NXC's interfaces into different zones based on your needs. You can configure firewall rules for data passing between zones or even between interfaces in a zone.

The following figure shows the NXC's default firewall rules in action as well as demonstrates how stateful inspection works. User **1** can initiate a Telnet session from within the LAN zone and responses to this request are allowed. However, other Telnet traffic initiated from the WAN or DMZ zone and destined for the LAN zone is blocked. Communications between the WAN and the DMZ zones are allowed.

Figure 16 Default Firewall Action



Your customized rules take precedence and override the NXC's default settings. The NXC checks the schedule, user name (user's login name on the NXC), source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the NXC takes the action specified in the rule.

For example, if you want to allow a specific user from any computer to access one zone by logging in to the NXC, you can set up a rule based on the user name only. If you also apply a schedule to the firewall

rule, the user can only access the network at the scheduled time. A user-aware firewall rule is activated whenever the user logs in to the NXC and will be disabled after the user logs out of the NXC.

22.2 Firewall Commands

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

Table 68 Input Values for General Firewall 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.
user_name	The name of a user (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
zone_object	The name of the zone. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. You can also use pre-defined zone names like LAN and WLAN.
rule_number	The priority number of a firewall rule. 1 - *X* where *X* is the highest number of rules the NXC model supports. See the NXC's User's Guide for details.
schedule_object	The name of the schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
service_name	The name of the service (group). 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 the firewall. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 69 Command Summary: Firewall

COMMAND	DESCRIPTION
`[no] connlimit max-per-host <1..8192>`	Sets the highest number of sessions that the NXC will permit a host to have at one time. The `no` command removes the settings.
`firewall` *rule_number*	Enters the firewall sub-command mode to set a firewall rule.
`firewall` *zone_object* `{`*zone_object*`|EnterpriseWLAN}` *rule_number*	Enters the firewall sub-command mode to set a direction specific through-EnterpriseWLAN rule or to-EnterpriseWLAN rule.
`firewall` *zone_object* `{`*zone_object*`|EnterpriseWLAN} append`	Enters the firewall sub-command mode to add a direction specific through-EnterpriseWLAN rule or to-EnterpriseWLAN rule to the end of the global rule list.
`firewall` *zone_object* `{`*zone_object*`|EnterpriseWLAN} delete` *rule_number*	Removes a direction specific through-EnterpriseWLAN rule or to-EnterpriseWLAN rule. `<1..5000>`: the index number in a direction specific firewall rule list.
`firewall` *zone_object* `{`*zone_object*`|EnterpriseWLAN} flush`	Removes all direction specific through-EnterpriseWLAN rule or to-EnterpriseWLAN rules.

Table 69 Command Summary: Firewall (continued)

COMMAND	DESCRIPTION
firewall *zone_object* {*zone_object*|EnterpriseWLAN} insert *rule_number*	Enters the firewall sub-command mode to add a direction specific through-EnterpriseWLAN rule or to-EnterpriseWLAN rule before the specified rule number.
firewall *zone_object* {*zone_object*|EnterpriseWLAN} move *rule_number* to *rule_number*	Moves a direction specific through-EnterpriseWLAN rule or to-EnterpriseWLAN rule to the number that you specified.
[no] firewall activate	Enables the firewall on the NXC. The no command disables the firewall.
firewall append	Enters the firewall sub-command mode to add a global firewall rule to the end of the global rule list.
firewall default-rule action {allow | deny | reject} { no log | log [alert] }	Sets how the firewall handles packets that do not match any other firewall rule.
firewall delete *rule_number*	Removes a firewall rule.
firewall flush	Removes all firewall rules.
firewall insert *rule_number*	Enters the firewall sub-command mode to add a firewall rule before the specified rule number.
firewall move *rule_number* to *rule_number*	Moves a firewall rule to the number that you specified.
show connlimit max-per-host	Displays the highest number of sessions that the NXC will permit a host to have at one time.
show firewall	Displays all firewall settings.
show firewall *rule_number*	Displays a firewall rule's settings.
show firewall *zone_object* {*zone_object*|EnterpriseWLAN}	Displays all firewall rules settings for the specified packet direction.
show firewall *zone_object* {*zone_object*|EnterpriseWLAN} *rule_number*	Displays a specified firewall rule's settings for the specified packet direction.
show firewall status	Displays whether the firewall is active or not.

22.2.1 Firewall Sub-Commands

The following table describes the sub-commands for several firewall commands.

Table 70 firewall Sub-commands

COMMAND	DESCRIPTION
action {allow|deny|reject}	Sets the action the NXC takes when packets match this rule.
[no] activate	Enables a firewall rule. The no command disables the firewall rule.
[no] ctmatch {dnat | snat}	Use dnat to block packets sent from a computer on the NXC's WAN network from being forwarded to an internal network according to a virtual server rule. Use snat to block packets sent from a computer on the NXC's internal network from being forwarded to the WAN network according to a 1:1 NAT or Many 1:1 NAT rule. The no command forwards the matched packets.

Table 70 firewall Sub-commands (continued)

COMMAND	DESCRIPTION
[no] description *description*	Sets a descriptive name (up to 60 printable ASCII characters) for a firewall rule. The no command removes the descriptive name from the rule.
[no] destinationip *address_object*	Sets the destination IP address. The no command resets the destination IP address(es) to the default (any). any means all IP addresses.
[no] from *zone_object*	Sets the zone on which the packets are received. The no command removes the zone on which the packets are received and resets it to the default (any). any means all interfaces or VPN tunnels.
[no] log [alert]	Sets the NXC to create a log (and optionally an alert) when packets match this rule. The no command sets the NXC not to create a log or alert when packets match this rule.
[no] schedule *schedule_object*	Sets the schedule that the rule uses. The no command removes the schedule settings from the rule.
[no] service *service_name*	Sets the service to which the rule applies. The no command resets the service settings to the default (any). any means all services.
[no] sourceip *address_object*	Sets the source IP address(es). The no command resets the source IP address(es) to the default (any). any means all IP addresses.
[no] sourceport {tcp|udp} {eq <1..65535>|range <1..65535> <1..65535>}	Sets the source port for a firewall rule. The no command removes the source port from the rule.
[no] to {*zone_object*|EnterpriseWLAN}	Sets the zone to which the packets are sent. The no command removes the zone to which the packets are sent and resets it to the default (any). any means all interfaces.
[no] user *user_name*	Sets a user-aware firewall rule. The rule is activated only when the specified user logs into the system. The no command resets the user name to the default (any). any means all users.

22.2.2 Firewall Command Examples

The following example shows you how to add a firewall rule to allow a MyService connection from the WLAN zone to the IP addresses Dest_1 in the LAN zone.

- Enter configuration command mode.
- Create an IP address object.
- Create a service object.
- Enter the firewall sub-command mode to add a firewall rule.
- Set the direction of travel of packets to which the rule applies.
- Set the destination IP address(es).
- Set the service to which this rule applies.

- Set the action the NXC is to take on packets which match this rule.

```
Router# configure terminal
Router(config)# service-object MyService tcp eq 1234
Router(config)# address-object Dest_1 10.0.0.10-10.0.0.15
Router(config)# firewall insert 3
Router(firewall)# from WLAN
Router(firewall)# to LAN
Router(firewall)# destinationip Dest_1
Router(firewall)# service MyService
Router(firewall)# action allow
```

The following command displays the firewall rule(s) (including the default firewall rule) that applies to the packet direction from WAN to LAN. The firewall rule numbers in the menu are the firewall rules' priority numbers in the global rule list.

```
Router# configure terminal
Router(config)# show firewall WAN LAN
firewall rule: 3
  description:
  user: any, schedule: none
  from: WAN, to: LAN
  source IP: any, source port: any
  destination IP: Dest_1, service: MyService
  log: no, action: allow, status: yes
firewall rule: 4
  description:
  user: any, schedule: none
  from: WAN, to: LAN
  source IP: any, source port: any
  destination IP: any, service: any
  log: log, action: deny, status: yes

Router(config)# show firewall WAN LAN 2
firewall rule: 4
  description:
  user: any, schedule: none
  from: WAN, to: LAN
  source IP: any, source port: any
  destination IP: any, service: any
  log: no, action: deny, status: yes
Router(config)#
```

22.3 Session Limit Commands

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

Table 71 Input Values for General Session Limit Commands

LABEL	DESCRIPTION
rule_number	The priority number of a session limit rule, 1 - 1000.
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.
user_name	The name of a user (group). 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 session-limit commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 72 Command Summary: Session Limit

COMMAND	DESCRIPTION
`[no] session-limit activate`	Turns the session-limit feature on or off.
`session-limit limit <0..8192>`	Sets the default number of concurrent NAT/ firewall sessions per host.
`session-limit` *rule_number*	Enters the session-limit sub-command mode to set a session-limit rule.
`[no] activate`	Enables the session-limit rule. The `no` command disables the session limit rule.
`[no] address` *address_object*	Sets the source IP address. The `no` command sets this to `any`, which means all IP addresses.
`[no] description` *description*	Sets a descriptive name (up to 64 printable ASCII characters) for a session-limit rule. The `no` command removes the descriptive name from the rule.
`exit`	Quits the firewall sub-command mode.
`[no] limit <0..8192>`	Sets the limit for the number of concurrent NAT/ firewall sessions this rule's users or addresses can have. 0 means any.
`[no] user` *user_name*	Sets a session-limit rule for the specified user. The `no` command resets the user name to the default (`any`). `any` means all users.
`session-limit append`	Enters the session-limit sub-command mode to add a session-limit rule to the end of the session-limit rule list.
`session-limit delete` *rule_number*	Removes a session-limit rule.
`session-limit flush`	Removes all session-limit rules.
`session-limit insert` *rule_number*	Enters the session-limit sub-command mode to add a session-limit rule before the specified rule number.
`session-limit move` *rule_number* `to` *rule_number*	Moves a session-limit to the number that you specified.
`show session-limit`	Shows the session-limit configuration.

Table 72 Command Summary: Session Limit (continued)

COMMAND	DESCRIPTION
`show session-limit begin` *`rule_number`* `end` *`rule_number`*	Shows the settings for a range of session-limit rules.
`show session-limit` *`rule_number`*	Shows the session-limit rule's settings.
`show session-limit status`	Shows the general session-limit settings.

CHAPTER 23
User/Group

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

23.1 User Account Overview

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

23.1.1 User Types

There are the types of user accounts the NXC uses.

Table 73 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
Admin	Change NXC configuration (web, CLI)	WWW, TELNET, SSH, FTP
Limited-Admin	Look at NXC configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH
Access Users		
User	Access network services Browse user-mode commands (CLI)	Captive Portal, TELNET, SSH
Guest	Access network services	Captive Portal
Ext-User	External user account.	Captive Portal
Ext-User-Group	External group user account.	Captive Portal
guest-manager	Create dynamic guest accounts	WWW
dynamic guest	Access network services	Captive Portal
mac-address	As permitted by the user-aware feature configuration.	MAC Authentication

23.2 User/Group Commands Summary

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

Table 74 username/groupname 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.
groupname	The name of the user group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. It cannot be the same as the user name.

The following sections list the `username/groupname` commands.

23.2.1 User Commands

The first table lists the commands for users.

Table 75 username/groupname Commands Summary: Users

COMMAND	DESCRIPTION
`show username [`*username*`]`	Displays information about the specified user or about all users set up in the NXC.
`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* `user-type ext-group-user`	Creates the specified user (if necessary) and sets the user type to **Ext-User**.
`username` *username* `user-type mac-address`	Creates the specified user (if necessary) and sets the user type to **mac-address**.
`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* `[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).

Table 75 username/groupname Commands Summary: Users (continued)

COMMAND	DESCRIPTION
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).
username *username* logon-time-setting <default | manual>	Sets the account to use the factory default lease and reauthentication times or custom ones.
username *username* vlan activate	Enables dynamic VLAN assignment for the user account. Dynamic VLAN assignment allows you to assign a user to a specific VLAN based on the user credentials.
username *username* vlan id <1..4094>	Sets the ID number of the VLAN to which this user account is assigned after authentication is successful.

23.2.2 User Group Commands

This table lists the commands for groups.

Table 76 username/groupname Commands Summary: Groups

COMMAND	DESCRIPTION
show groupname [*groupname*]	Displays information about the specified user group or about all user groups set up in the NXC.
[no] groupname *groupname*	Creates the specified user group if necessary and enters sub-command mode. The no command deletes the specified user group.
[no] description *description*	Sets the description for the specified user group. The no command clears the description for the specified user group.
[no] groupname *groupname*	Adds the specified user group (second *groupname*) to the specified user group (first *groupname*).
[no] user *username*	Adds the specified user to the specified user group.
show	Displays information about the specified user group.
groupname rename *groupname groupname*	Renames the specified user group (first *groupname*) to the specified group-name (second *groupname*).

23.2.3 User Setting Commands

This table lists the commands for user settings, except for forcing user authentication.

Table 77 username/groupname Commands Summary: Settings

COMMAND	DESCRIPTION
show users default-setting {all | user-type {admin|user|guest|limited-admin|ext-group-user}}	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.

Table 77 username/groupname Commands Summary: Settings (continued)

COMMAND	DESCRIPTION
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 |ext-user|guest|limited-admin|ext-group-user>	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.
show users update-lease-settings	Displays whether or not access users can automatically renew their lease time.
[no] users update-lease automation	Lets users automatically renew their lease time. The no command prevents them from automatically renewing it.
show users idle-detection-settings	Displays whether or not users are automatically logged out, and, if so, how many minutes of idle time must pass before they are logged out.
[no] users idle-detection	Enables logging users out after a specified number of minutes of idle time. The no command disables logging them out.
[no] users idle-detection timeout <1..60>	Sets the number of minutes of idle time before users are automatically logged out. The no command sets the idle-detection timeout to three minutes.

23.2.3.1 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: yes
maximum simultaneous logon per administration account          : 1
enable simultaneous logon limitation for access account        : yes
maximum simultaneous logon per access account                  : 3
```

23.2.4 MAC Auth Commands

This table lists the commands for mappings MAC addresses to MAC address user accounts.

Table 78 mac-auth Commands Summary

COMMAND	DESCRIPTION
[no] mac-auth database mac *mac address* type ext-mac-address mac-role *username* description *description*	Maps the specified MAC address authenticated by an external server to the specified MAC role (MAC address user account). The no command deletes the mapping between the MAC address and the MAC role.
[no] mac-auth database mac *mac address* type int-mac-address mac-role *username* description *description*	Maps the specified MAC address authenticated by the NXC's local user database to the specified MAC role (MAC address user account). The no command deletes the mapping between the MAC address and the MAC role.
[no] mac-auth database mac *oui* type ext-oui mac-role *username* description *description*	Maps the specified OUI (Organizationally Unique Identifier) authenticated by an external server to the specified MAC role (MAC address user account). The OUI is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device. The no command deletes the mapping between the OUI and the MAC role.
[no] mac-auth database mac *oui* type int-oui mac-role *username* description *description*	Maps the specified OUI (Organizationally Unique Identifier) authenticated by the NXC's local user database to the specified MAC role (MAC address user account). The OUI is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device. The no command deletes the mapping between the OUI and the MAC role.

23.2.4.1 MAC Auth Example

This example uses an external server to authenticate wireless clients by MAC address. After authentication the NXC maps the wireless client to a mac-address user account (MAC role). Configure user-aware features to control MAC address user access to network services.

The following commands:

- Create a MAC role (mac-address user type user account) named Zyxel-mac
- Map a wireless client's MAC address of 00:13:49:11:a0:c4 to the Zyxel-mac MAC role (MAC address user account)
- Modify the WLAN security profile named secureWLAN1 as follows:
  - Turn on MAC authentication
  - Use the authentication method named Auth1
  - Use colons to separate the two-character pairs within account MAC addresses

- Use upper case letters in the account MAC addresses

```
Router(config)# username Zyxel-mac user-type mac-address
Router(config)# mac-auth database mac 00:13:49:11:a0:c4 type ext-mac-address
mac-role Zyxel-mac description zyxel mac

3. Modify wlan-security-profile
Router(config)# wlan-security-profile secureWLAN1
Router(config-wlan-security default)# mac-auth activate
Router(config-wlan-security default)# mac-auth auth-method Auth1
Router(config-wlan-security default)# mac-auth delimiter account colon
Router(config-wlan-security default)# mac-auth case account upper
Router(config-wlan-security default)# exit
```

23.2.5 Additional User Commands

This table lists additional commands for users.

Table 79 username/groupname 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.

23.2.5.1 Additional User Command Examples

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

```
Router# configure terminal
Router(config)# show users all
No.  Name                          Role                          Type
     MAC                           Service          From
     Session Time      Idle Time        Lease Timeout     Re-Auth. Timeout
     Acct. Status      Profile Name
==============================================================================
1    admin                         admin                         admin
                                   console          console
     00:35:36          unlimited        00:30:00          unlimited
     -                 N/A
2    admin                         admin                         admin
                                   http/https       192.168.1.5
     00:04:06          unlimited        00:25:57          unlimited
     -                 N/A
3    admin                         admin                         admin
                                   http/https       192.168.1.5
     00:03:39          unlimited        00:26:25          unlimited
     -                 N/A
Router(config)# users force-logout 192.168.1.5
Logout user 'admin'(from 192.168.1.5): OK
Logout user 'admin'(from 192.168.1.5): OK
Total 2 users have been forced logout
Router(config)# show users all
No.  Name                          Role                          Type
     MAC                           Service          From
     Session Time      Idle Time        Lease Timeout     Re-Auth. Timeout
     Acct. Status      Profile Name
==============================================================================
1    admin                         admin                         admin
                                   console          console
     00:37:22          unlimited        00:30:00          unlimited
     -                 N/A
```

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    192.168.1.60    2                       46

Router(config)# unlock lockout-users 192.168.1.60
User from 192.168.1.60 is unlocked
Router(config)# show lockout-users
No.  Username Tried                  From            Lockout Time Remaining
================================================================================
No.  From            Failed Login Attempt    Record Expired Timer
================================================================================
```

CHAPTER 24
Addresses

This chapter describes how to set up addresses and address groups for the NXC.

Note: Use the `configure terminal` command to enter Configuration mode in order to use the commands described in this chapter.

24.1 Address Overview

Address objects can represent a single IP address or a range of IP addresses. Address groups are composed of address objects and other address groups.

You can create IP address objects based on an interface's IP address, subnet, or gateway. The NXC automatically updates these objects whenever the interface's IP address settings change. This way every rule or setting that uses the object uses the updated IP address settings. For example, if you change the LAN1 interface's IP address, the NXC automatically updates the corresponding interface-based, LAN1 subnet address object. So any configuration that uses the LAN1 subnet address object is also updated.

Address objects and address groups are used in dynamic routes, firewall rules, application patrol, content filtering, and VPN connection policies. For example, addresses are used to specify where content restrictions apply in content filtering. Please see the respective sections for more information about how address objects and address groups are used in each one.

Address groups are composed of address objects and address groups. The sequence of members in the address group is not important.

24.2 Address Commands Summary

The following table describes the values required for many address object and address group commands. Other values are discussed with the corresponding commands.

Table 80 Input Values for Address Commands

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

Table 80 Input Values for Address Commands (continued)

LABEL	DESCRIPTION
group_name	The name of the address group. 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. Use ge*x*, *x* = 1 ~ N for Ethernet interfaces, where N equals the highest numbered Ethernet interface for your NXC model. Use vlan*x*, x= 1 ~N for VLAN interfaces where N equals the highest numbered Ethernet interface for your NXC model

The following sections list the address object and address group commands.

24.2.1 Address Object Commands

This table lists the commands for address objects.

Table 81 address-object Commands: Address Objects

COMMAND	DESCRIPTION
`show address-object [object_name]`	Displays information about the specified address or all the addresses.
`address-object object_name {ip | ip_range | ip_subnet | interface-ip | interface-subnet | interface-gateway} {interface}`	Creates the specified address object using the specified parameters. *ip_range*: <1..255>.<0..255>.<0..255>.<1..255>-<1..255>.<0..255>.<0..255>.<1..255> *ip_subnet*: <1..255>.<0..255>.<0..255>.<0..255>/<1..32> *interface*: You only need to specify an interface when you create an object based on an interface.
`no address-object object_name`	Deletes the specified address.
`address-object list`	Displays all address objects on the NXC.
`address-object rename object_name object_name`	Renames the specified address (first *object_name*) to the second *object_name*.

24.2.1.1 Address Object Command Examples

The following example creates three address objects and then deletes one.

```
Router# configure terminal
Router(config)# address-object A0 10.1.1.1
Router(config)# address-object A1 10.1.1.1-10.1.1.20
Router(config)# address-object A2 10.1.1.0/24
Router(config)# show address-object
Object name                     Type               Address

Note            Ref.
================================================================================
====
LAN_SUBNET                      INTERFACE SUBNET   192.168.1.0/24
vlan0           0
A0                              HOST               10.1.1.1
                0
A1                              RANGE              10.1.1.1-10.1.1.20
                0
A2                              SUBNET             10.1.1.0/24
                0
Router(config)# no address-object A2
Router(config)# show address-object
Object name                     Type               Address
Note            Ref.
================================================================================
====
LAN_SUBNET                      INTERFACE SUBNET   192.168.1.0/24
vlan0           0
A0                              HOST               10.1.1.1
                0
A1                              RANGE              10.1.1.1-10.1.1.20
                0
Router(config)#
```

24.2.2 Address Group Commands

This table lists the commands for address groups.

Table 82 object-group Commands: Address Groups

COMMAND	DESCRIPTION
show object-group address [*group_name*]	Displays information about the specified address group or about all address groups.
[no] object-group address *group_name*	Creates the specified address group if necessary and enters sub-command mode. The no command deletes the specified address group.
[no] address-object *object_name*	Adds the specified address to the specified address group. The no command removes the specified address from the specified group.
[no] object-group *group_name*	Adds the specified address group (second *group_name*) to the specified address group (first *group_name*). The no command removes the specified address group from the specified address group.

Table 82 object-group Commands: Address Groups (continued)

COMMAND	DESCRIPTION
[no] description *description*	Sets the description to the specified value. The no command clears the description. *description*: You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
object-group address rename *group_name group_name*	Renames the specified address group from the first *group_name* to the second *group_name*.

24.2.2.1 Address Group Command Examples

The following commands create three address objects A0, A1, and A2 and add A1 and A2 to address group RD.

```
Router# configure terminal
Router(config)# address-object A0 192.168.1.1
Router(config)# address-object A1 192.168.1.2-192.168.2.20
Router(config)# address-object A2 192.168.3.0/24
Router(config)# object-group address RD
Router(group-address)# address-object A1
Router(group-address)# address-object A2
Router(group-address)# exit
Router(config)# show object-group address
Group name                      Reference
Description
================================================================================
TW_TEAM                         5

RD                              0

Router(config)# show object-group address RD
Object/Group name               Type   Reference
================================================================================
A1                              Object 1
A2                              Object 1
```

CHAPTER 25
Services

Use service objects to define TCP applications, UDP applications, and ICMP messages. You can also create service groups to refer to multiple service objects in other features.

25.1 Services Overview

See the appendices in the web configurator's User Guide for a list of commonly-used services.

25.2 Services Commands Summary

The following table describes the values required for many service object and service group commands. Other values are discussed with the corresponding commands.

Table 83 Input Values for Service Commands

LABEL	DESCRIPTION
group_name	The name of the service group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
object_name	The name of the service. 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 service object and service group commands.

25.2.1 Service Object Commands

The first table lists the commands for service objects.

Table 84 service-object Commands: Service Objects

COMMAND	DESCRIPTION
`show service-object [`*object_name*`]`	Displays information about the specified service or about all the services.
`no service-object` *object_name*	Deletes the specified service.
`service-object` *object_name* `{tcp | udp} {eq <1..65535> | range <1..65535> <1..65535>}`	Creates the specified TCP service or UDP service using the specified parameters.

Table 84 service-object Commands: Service Objects (continued)

COMMAND	DESCRIPTION
service-object *object_name* icmp *icmp_value*	Creates the specified ICMP message using the specified parameters. *icmp_value*: <0..255> | alternate-address | conversion-error | echo | echo-reply | information-reply | information-request | mask-reply | mask-request | mobile-redirect | parameter-problem | redirect | router-advertisement | router-solicitation | source-quench | time-exceeded | timestamp-reply | timestamp-request | unreachable
service-object *object_name* protocol <1..255>	Creates the specified user-defined service using the specified parameters.
service-object list	Lists all available network services.
service-object rename *object_name* *object_name*	Renames the specified service from the first *object_name* to the second *object_name*.

25.2.1.1 Service Object Command Examples

The following commands create one service and display information about it.

```
Router# configure terminal
Router(config)# service-object FTP tcp range 20 21
Router(config)# show service-object FTP
Router(config)# show service-object FTP
Object name                    Protocol         Minmum port  Maxmum port  Ref.
=============================================================================
FTP                              TCP              20           21           1

FTP References:
Category
Rule Priority        Rule Name   Description
=============================================================================
Captive Portal
3                    N/A         N/A
Router(config)#
```

25.2.2 Service Group Commands

The first table lists the commands for service groups.

Table 85 object-group Commands: Service Groups

COMMAND	DESCRIPTION
show object-group service *group_name*	Displays information about the specified service group.
[no] object-group service *group_name*	Creates the specified service group if necessary and enters sub-command mode. The no command removes the specified service group.
[no] service-object *object_name*	Adds the specified service to the specified service group. The no command removes the specified service from the specified group.

Table 85 object-group Commands: Service Groups (continued)

COMMAND	DESCRIPTION
[no] object-group *group_name*	Adds the specified service group (second *group_name*) to the specified service group (first *group_name*). The no command removes the specified service group from the specified service group.
[no] description *description*	Sets the description to the specified value. The no command removes the description. *description*: You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
object-group service rename *group_name group_name*	Renames the specified service group from the first *group_name* to the second *group_name*.

25.2.2.1 Service Group Command Examples

The following commands create service ICMP_ECHO, create service group SG1, and add ICMP_ECHO to SG1.

```
Router# configure terminal
Router(config)# service-object ICMP_ECHO icmp echo
Router(config)# object-group service SG1
Router(group-service)# service-object ICMP_ECHO
Router(group-service)# exit
Router(config)# show service-object ICMP_ECHO
Object name                    Protocol         Minmum port  Maxmum port  Ref.
================================================================================
ICMP_ECHO                      ICMP             8            8            1

ICMP_ECHO References:
Category
Rule Priority        Rule Name  Description
================================================================================
Service Group
N/A                  SG1        N/A
Router(config)# show object-group service SG1
Object/Group name              Type   Reference
================================================================================
ICMP_ECHO                      Object 1
Router(config)#
```

CHAPTER 26
Schedules

Use schedules to set up one-time and recurring schedules for policy routes, firewall rules, application patrol, and content filtering.

26.1 Schedule Overview

The NXC supports two types of schedules: one-time and recurring. One-time schedules are effective only once, while recurring schedules usually repeat. Both types of schedules are based on the current date and time in the NXC.

Note: Schedules are based on the current date and time in the NXC.

One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods.

Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules always begin and end in the same day. Recurring schedules are useful for defining the workday and off-work hours.

26.2 Schedule Commands Summary

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

Table 86 Input Values for Schedule Commands

LABEL	DESCRIPTION
object_name	The name of the schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
time	24-hour time, hours and minutes; <0..23>:<0..59>.

The following table lists the schedule commands.

Table 87 schedule Commands

COMMAND	DESCRIPTION
`show schedule-object`	Displays information about the schedules in the NXC.
`no schedule-object` *object_name*	Deletes the schedule object.
`schedule-object list`	Lists all schedules configured on the NXC.

Table 87 schedule Commands (continued)

COMMAND	DESCRIPTION
schedule-object *object_name date time date time*	Creates or updates a one-time schedule. *date*: yyyy-mm-dd date format; yyyy-<01..12>-<01..31>
schedule-object *object_name time time* [*day*] [*day*] [*day*] [*day*] [*day*] [*day*] [*day*]	Creates or updates a recurring schedule. *day*: 3-character day of the week; sun | mon | tue | wed | thu | fri | sat

26.2.1 Schedule Command Examples

The following commands create recurring schedule SCHEDULE1 and one-time schedule SCHEDULE2 and then delete SCHEDULE1.

```
Router# configure terminal
Router(config)# schedule-object SCHEDULE1 11:00 12:00 mon tue wed thu fri
Router(config)# schedule-object SCHEDULE2 2006-07-29 11:00 2006-07-31 12:00
Router(config)# show schedule-object
Object name                    Type      Start/End                        Ref.
=============================================================================
SCHEDULE1                      Recurring 11:00/12:00 ===MonTueWedThuFri=== 0
SCHEDULE2                      Once      2006-07-29 11:00/2006-07-31 12:00 0

Router(config)# no schedule-object SCHEDULE1
Router(config)# show schedule-object
Object name                    Type      Start/End                        Ref.
=============================================================================
SCHEDULE2                      Once      2006-07-29 11:00/2006-07-31 12:00 0
```

CHAPTER 27
AAA Server

This chapter introduces and shows you how to configure the NXC to use external authentication servers.

27.1 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 NXC supports.

- Local user database

  The NXC uses the built-in local user database to authenticate administrative users logging into the NXC's web configurator or network access users logging into the network through the NXC. 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.

27.2 Authentication Server Command Summary

This section describes the commands for authentication server settings.

27.2.1 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 88 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 a base distinguished name (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 NXC uses to log into the AD server group. The `no` command clears this setting.
`[no] server cn-identifier uid`	Sets the unique common name (cn) to identify a record. 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 NXC 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.

Table 88 aaa group server ad Commands (continued)

COMMAND	DESCRIPTION
server domain-auth domain-name <*netbios_name*>	Adds the NetBIOS name of the AD server. The NXC uses it with the user name in the format NetBIOS\USERNAME to do authentication. The NXC uses the format USERNAME@realm if you do not configure the NetBIOS name.
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 NXC to establish a secure connection to the AD server. The no command disables this feature.

27.2.2 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 89 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.
[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 a base distinguished name (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 NXC uses to log into the LDAP server group. The no command clears this setting.
[no] server cn-identifier *uid*	Sets the unique common name (cn) to identify a record. 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.

Table 89 aaa group server ldap Commands (continued)

COMMAND	DESCRIPTION
[no] server group-attribute *group-attribute*	Sets the name of the attribute that the NXC 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 NXC to establish a secure connection to the LDAP server. The no command disables this feature.

27.2.3 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 90 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*	Changes the descriptive name for a RADIUS server group.
aaa group server radius *group-name*	Enter the sub-command mode.

Table 90 aaa group server radius Commands (continued)

COMMAND	DESCRIPTION
[no] coa	Sets the NXC to disconnect wireless clients based on the information (such as client's user name and MAC address) specified in CoA or RADIUS Disconnect messages sent by the RADIUS server. The external RADIUS server can change its authentication policy and send CoA (Change of Authorization) or RADIUS Disconnect messages in order to terminate the subscriber's service. The no command disables this feature.
[no] server acct-address *radius_server* acct-port *port*	Enter the IP address (in dotted decimal notation) or domain name and authentication port of the RADIUS accounting server to add to this server group. The no command clears this setting.
[no] server acct-secret *key*	Enter the key (up to 15 alphanumeric characters) to share between the external accounting server and the NXC. The key is not sent over the network. This key must be the same on the external accounting server and the NXC. The no command clears this setting.
[no] server acct-interim activate	Enable this to have the NXC send subscriber status updates to the RADIUS server. The no command has the NXC not send subscriber status updates to the RADIUS server.
[no] server acct-interim-interval <1..1440>	Specifies the interval (in minutes) at which the NXC sends subscriber status updates to the RADIUS server. The no command clears this setting.
[no] server acct-retry-count <*retry_times*>	Sets the number of times the NXC reattempts to use the primary RADIUS server before attempting to use the secondary RADIUS server. This also sets how many times the NXC attempts to use the secondary RADIUS server. The no command clears this setting.
[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 NXC 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* auth-port *port*	Enter the IP address (in dotted decimal notation) or domain name and authentication port 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 NXC. The no command clears this setting.
[no] server nas-id <*nas_identifier*>	Specifies the Network Access Server identifier attribute value if the RADIUS server requires it. The no command clears this setting.
[no] server nas-ip <*nas_address*>	Specifies the Network Access Server IP address attribute value if the RADIUS server requires it. The no command clears this setting.

Table 90 aaa group server radius Commands (continued)

COMMAND	DESCRIPTION
[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.
show	Displays the RADIUS server settings.

27.2.4 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 172.16.22.100 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
Router(config)# show aaa group server radius RADIUSGroup1
key                : 12345678
timeout            : 100
description        :
group attribute    : 11
nas-ip             : 127.0.0.1
nas-id             :
case-sensitive     : yes

No.  Host Member                                                    Auth. Port

==========================================================================
1    192.168.1.100                                                    1812
2    172.16.22.100                                                    1812

Router(config)#
```

CHAPTER 28
Authentication Objects

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

28.1 Authentication Objects Overview

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

28.2 aaa authentication Commands

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

Table 91 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.

Table 91 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 ad, group ldap, 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 ad, group ldap, 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.

28.2.1 aaa authentication Command Example

The following example creates an authentication profile to authentication users using the LDAP server group and then the local user database.

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

28.3 test aaa Command

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

Table 92 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.

28.3.1 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 NXC 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 29
Authentication Server

This chapter shows you how to configure the NXC as an authentication server for access points.

29.1 Authentication Server Overview

The NXC can also work as a RADIUS server to exchange messages with other APs for user authentication and authorization.

29.2 Authentication Server Commands

The following table lists the authentication server commands you use to configure the NXC's built-in authentication server settings.

Table 93 Command Summary: Authentication Server

COMMAND	DESCRIPTION
`[no] auth-server activate`	Sets the NXC to act as an authentication server for other RADIUS clients, such as APs. The `no` command sets the NXC to not act as an authentication server for other APs.
`auth-server authentication` *`auth_method`*	Specifies an authentication method used by the authentication server.
`no auth-server authentication`	Resets the authentication method used by the authentication server to the factory default (`default`).
`[no] auth-server cert` *`certificate_name`*	Specifies a certificate used by the authentication server (NXC). The `no` command resets the certificate used by the authentication server to the factory default (`default`). *`certificate_name`*: The name of the certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
`[no] auth-server peap-default-use-gtc`	Has the NXC's authentication server propose GTC as the default PEAP EAP type when using 802.1X with an internal authentication server. Disable it to propose the MS-CHAPv2 type instead.
`[no] auth-server trusted-client` *`profile_name`*	Creates a trusted RADIUS client profile. The `no` command deletes the specified profile. *`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.
`[no] activate`	Enables the client profile. The `no` command disables the profile.
`[no] ip address` *`ip subnet_mask`*	Sets the client's IP address and subnet mask. The `no` command clears this setting.

Table 93 Command Summary: Authentication Server (continued)

COMMAND	DESCRIPTION
[no] secret *secret*	Sets a password as the key to be shared between the NXC and the client. The no command clears this setting.
[no] description *description*	Sets the description for the profile. The no command clears this setting. *description*: You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
show auth-server status	Displays the NXC's authentication server settings.
show auth-server trusted-client	Displays all RADIUS client profile settings.
show auth-server trusted-client *profile_name*	Displays the specified RADIUS client profile settings.

29.2.1 Authentication Server Command Examples

The following example shows you how to enable the authentication server feature on the NXC and sets a trusted RADIUS client profile. This example also shows you the authentication server and client profile settings.

```
Router# configure terminal
Router(config)# auth-server activate
Router(config)# auth-server trusted-client AP-1
Router(config-trusted-client-AP-1)# activate
Router(config-trusted-client-AP-1)# ip address 10.10.1.2 255.255.255.0
Router(config-trusted-client-AP-1)# secret 12345678
Router(config-trusted-client-AP-1)# exit
Router(config)# show auth-server status
activation: yes
authentication method: default
certificate: default
Router(config)# show auth-server trusted-client AP-1
Client: AP-1
  Activation: yes
  Description:
  IP: 10.10.1.2
  Netmask: 255.255.255.0
  Secret: VQEq907jWB8=
Router(config)#
```

CHAPTER 30
Certificates

This chapter explains how to use the **Certificates**.

30.1 Certificates Overview

The NXC 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 NXC to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

30.2 Certificate Commands

This section describes the commands for configuring certificates.

30.3 Certificates Commands Input Values

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

Table 94 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 94 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 NXC 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; | `~!@#$%^&*()_+\{}':,./<>=-
ca_name	When you have the NXC enroll for a certificate immediately online, you must have the certification authority's certificate already imported as a trusted certificate. Specify the name of the certification authority's certificate. It can be up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
url	When you have the NXC 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'()+,/:.=?;!*#@$_%-

30.4 Certificates Commands Summary

The following table lists the commands that you can use to display and manage the NXC'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 95 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*] [usr-def *certificate_name*] 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*] [usr-def *certificate_name*] 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.

Table 95 ca Commands Summary (continued)

COMMAND	DESCRIPTION
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*] [usr-def *certificate_name*] 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.
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*] [usr-def *certificate_name*] 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.

30.5 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=nxc2500_B0B2DC6EA897
  issuer: CN=nxc2500_B0B2DC6EA897
  status: VALID
  ID: nxc2500_B0B2DC6EA897
    type: EMAIL
  valid from: 2012-12-07 10:49:31 GMT
  valid to: 2032-12-02 10:49:31 GMT
certificate: MyCertificate
  type: SELF
  subject: CN=Mydevice@example.com
  issuer: CN=Mydevice@example.com
  status: VALID
  ID: Mydevice@example.com
    type: EMAIL
  valid from: 2014-04-09 10:44:04 GMT
  valid to: 2017-04-08 10:44:04 GMT
certificate: pkcs12request
  type: REQ
  subject: CN=1.1.1.2
  issuer: none
  status: VALID
  ID: 1.1.1.2
    type: IP
  valid from: none
  valid to: none
certificate: test_x509
  type: SELF
  subject: CN=10.0.0.58
  issuer: CN=10.0.0.58
  status: VALID
  ID: 10.0.0.58
    type: IP
  valid from: 2014-06-07 15:52:52 GMT
  valid to: 2017-06-06 15:52:52 GMT
Router(config)# no ca category local pkcs12request
```

CHAPTER 31
DHCPv6 Objects

This chapter describes how to configure and view DHCPv6 request objects.

31.1 DHCPv6 Object Commands Summary

The following table identifies the values required for many DHCPv6 object commands. Other input values are discussed with the corresponding commands.

Table 96 DHCPv6 Object Command Input Values

LABEL	DESCRIPTION
dhcp6_profile	The name of a DHCPv6 request object. Use a string of less than 31 characters.
interface_name	The name of the interface. Ethernet interface: ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your NXC model. VLAN interface: vlan*x*, *x* = 0 - 4094

The following sections list the DHCPv6 object commands.

31.1.1 DHCPv6 Object Commands

This table lists the commands for creating endpoint security objects. Use the `configure terminal` command to enter the configuration mode to be able to use the commands that configure settings.

Table 97 DHCPv6 Object Commands

COMMAND	DESCRIPTION
`show dhcp6 interface`	Displays all DHCPv6 server, client and relay interfaces.
`show dhcp6 object-binding` *interface_name*	Displays the DHCPv6 object bound to the specified interface.
`show dhcp6 request-object` [*dhcp6_profile*]	Displays the specified DHCPv6 request object or all of them.
`dhcp6-request-object` *dhcp6_profile* { `dns-server | ntp-server` }	Creates or edits the specified DNS server, or NTP server DHCP request object.
`dhcp6-request-object rename` *dhcp6_profile dhcp6_profile*	Renames the specified DHCPv6 request object to the specified name.
`no dhcp6-request-object` *dhcp6_profile*	Deletes the specified DHCPv6 request object.

31.1.2 DHCPv6 Object Command Examples

This example creates and displays a DHCPv6 request object named “test1” for DNS server information.

```
Router(config)# dhcp6-request-object test1 dns-server
Router(config)# show dhcp6 request-object
DHCP6 Request Object: test1
  Object Type: dns-server
  Object Value:
  Bind Iface:
  REFERENCE: 0
Router(config)#
```

CHAPTER 32
System

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

32.1 System Overview

Use these commands to configure general NXC 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 NXC zones (if any) from which computers.

32.2 Customizing the WWW Login Page

Use these commands to customize the Web Configurator login screen. You can also customize the page that displays after an access user logs into the Web Configurator to access network services like the Internet.

The following figures identify the parts you can customize in the login, access, and user-logout pages.

Figure 17 Login Page Customization

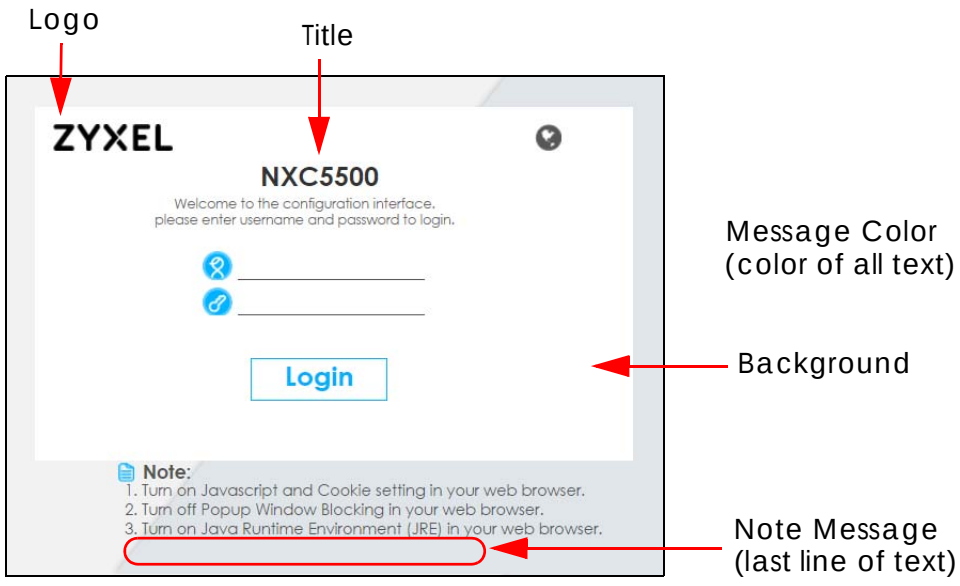


Figure 18 Access Page Customization

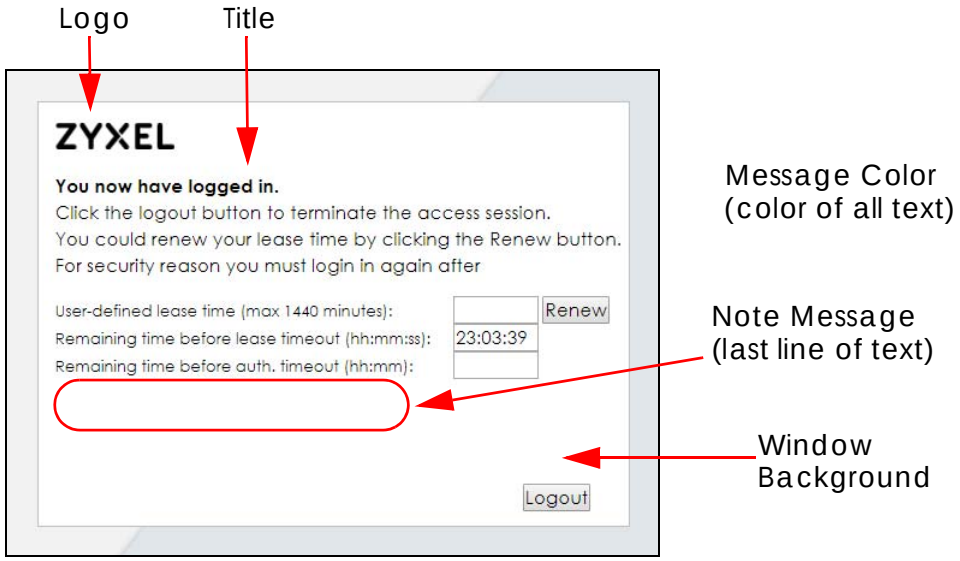
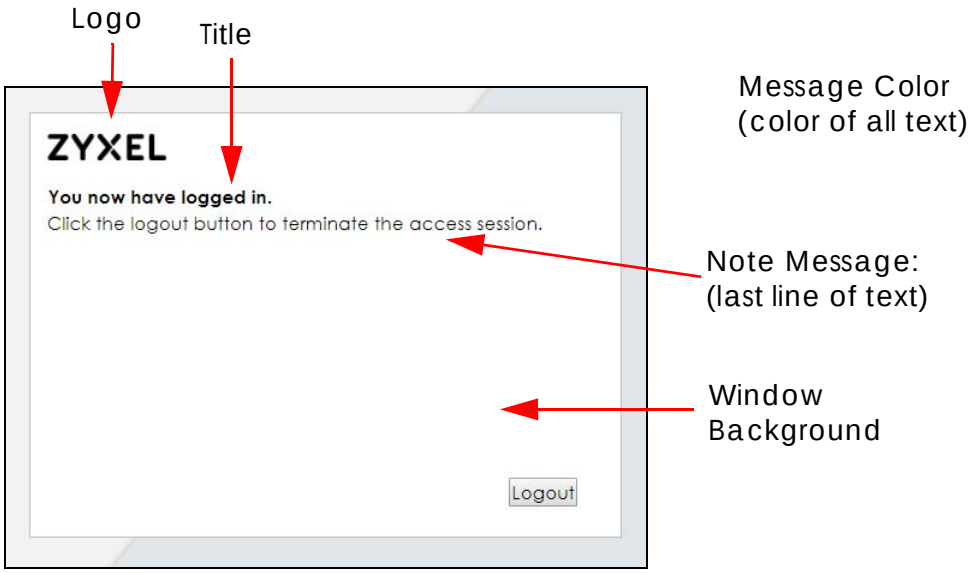


Figure 19 User Logout Customization



You can specify colors in one of the following ways:

- *color-rgb*: Enter red, green, and blue values in parenthesis and separate by commas. For example, use “rgb(0,0,0)” for black.
- *color-name*: Enter the name of the desired color.
- *color-number*: Enter a pound sign (#) followed by the six-digit hexadecimal number that represents the desired color. For example, use “#000000” for black.

The following table describes the commands available for customizing the Web Configurator login screen, user logout screen and the page that displays after an access user logs into the Web

Configurator to access network services like the Internet. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 98 Command Summary: Customization

COMMAND	DESCRIPTION
`customized-page` *theme_name*	Enters the sub-command mode for page customization.
`access-page color-window-background {yes | no}`	Sets whether or not the access page uses a colored background.
`access-page-message-color {`*color-rgb* `|` *color-name* `|` *color-number*`}`	Sets the color of the message text on the access page.
`[no] access-page message-text` *message*	Sets a note to display below the access page's title. Use up to 64 printable ASCII characters. Spaces are allowed.
`access-page-title <title>`	Sets the title for the top of the access page. Use up to 64 printable ASCII characters. Spaces are allowed.
`access-page-window-color {`*color-rgb* `|` *color-name* `|` *color-number*`}`	Sets the color of the access page's colored background.
`login-page-background-color {`*color-rgb* `|` *color-name* `|` *color-number*`}`	Sets the color of the login page's background.
`login-page-color-background {yes | no}`	Sets the login page to use a solid colored background.
`login-page-message-color {`*color-rgb* `|` *color-name* `|` *color-number*`}`	Sets the color of the message text on the login page.
`[no] login-page-message-text` *message*	Sets a note to display at the bottom of the login screen. Use up to 64 printable ASCII characters. Spaces are allowed.
`login-page-title` *title*	Sets the title for the top of the login screen. Use up to 64 printable ASCII characters. Spaces are allowed.
`login-page-title-color {`*color-rgb* `|` *color-name* `|` *color-number*`}`	Sets the title text color of the login page.
`userlogout-page-color-window-background {`*yes* `|` *no*`}`	Sets whether or not the user logout page uses a colored background.
`userlogout-page-message-color {`*color-rgb* `|` *color-name* `|` *color-number*`}`	Sets the color of the message text on the user logout page.
`userlogout-page-message-text` *message*	Sets a note to display at the bottom of the user logout screen. Use up to 64 printable ASCII characters. Spaces are allowed.
`userlogout-page-title` *title*	Sets the title for the top of the user logout screen. Use up to 64 printable ASCII characters. Spaces are allowed.
`userlogout-page-window-color {`*color-rgb* `|` *color-name* `|` *color-number*`}`	Sets the color of the user logout screen's colored background.
`show customized-page {`*theme_name* `|` `all}`	Lists specific or all customized-page settings.
`show login-page default-title`	Lists the factory default title for the login page.
`show login-page settings`	Lists the current login page settings.

Table 98 Command Summary: Customization (continued)

COMMAND	DESCRIPTION
show logo settings	Lists the current logo background (banner) and floor (line below the banner) settings.
show page-customization	Lists whether the NXC is set to use custom login and access pages or the default ones.

32.3 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 99 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 NXC. The no command removes the host name.
show fqdn	Displays the fully qualified domain name.

32.4 Time and Date

For effective scheduling and logging, the NXC system time must be accurate. The NXC's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server.

32.4.1 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 100 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 100 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 NXC.
show clock status	Displays your time zone and daylight saving settings.
show clock time	Displays the current time of your NXC.
show ntp server	Displays time server settings.

32.5 Console Port Speed

This section shows you how to set the console port speed when you connect to the NXC 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 101 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.

32.6 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.

32.6.1 DNS Commands

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

Table 102 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 NXC 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 103 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.
`[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..64>|append|insert <1..64>} 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..64> to <1..64>`	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 NXC connects to the DNS server through a VPN tunnel. Otherwise, use the `interface` command to set the interface through which the NXC sends DNS queries to a DNS server. The `auto` means any interface that the NXC 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..64>`	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.
`show ip dns server cache`	Displays all DNS records.
`show ip dns server tcp-listen`	Displays whether TCP listen is enabled to allow an application to accept incoming TCP connections.

32.6.2 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
```

32.7 Language Commands

Use the `language` commands to display what language the web configurator is using or change it. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 104 Command Summary: Language

COMMAND	DESCRIPTION
`language <English | Simplified_Chinese | Traditional_Chinese>`	Specifies the language used in the web configurator screens.
`show language {setting | all}`	`setting` displays the current display language in the web configurator screens. `all` displays the available languages.

CHAPTER 33
System Remote Management

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

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

33.1 Remote Management Overview

You may manage your NXC from a remote location via:

- Internet (WAN only)
- LAN only
- ALL (LAN&WAN&DMZ)
- DMZ only

To disable remote management of a service, deselect **Enable** in the corresponding service screen.

33.1.1 Remote Management Limitations

Remote management will not work when:

1. You have disabled that service in the corresponding screen.
2. The accepted IP address in the **Service Control** table does not match the client IP address. If it does not match, the NXC will disconnect the session immediately.
3. There is a firewall rule that blocks it.

33.1.2 System Timeout

There is a lease timeout for administrators. The NXC 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 NXC for authentication again when the reauthentication time expires.

33.2 Common System Command Input Values

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

Table 105 Input Values for General System 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.
rule_number	The number of a service control rule. 1 - *X* where *X* is the highest number of rules the NXC model supports.
zone_object	The name of the zone. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. The NXC uses pre-defined zone names like LAN and WLAN.

33.3 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 106 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).
`[no] ip http secure-server`	Enables HTTPS access to the NXC web configurator. The `no` command disables HTTPS access to the NXC 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.

Table 106 Command Summary: HTTP/HTTPS (continued)

COMMAND	DESCRIPTION
[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 table {admin|user} rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny}	Sets a service control rule for HTTPS service.
ip http secure-server table {admin|user} rule move *rule_number* to *rule_number*	Changes the index number of a HTTPS service control rule.
ip http secure-server cipher-suite {*cipher_algorithm*} [*cipher_algorithm*] [*cipher_algorithm*] [*cipher_algorithm*]	Sets the encryption algorithms (up to four) that the NXC 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 NXC's CPU performance since the NXC'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 NXC not use the specified encryption algorithm for the SSL in HTTPS connections.
[no] ip http server	Allows HTTP access to the NXC web configurator. The no command disables HTTP access to the NXC web configurator.
ip http server table {admin|user} rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny}	Sets a service control rule for HTTP service.
ip http server table {admin|user} rule move *rule_number* to *rule_number*	Changes the number of a HTTP service control rule.
no ip http secure-server table {admin|user} rule *rule_number*	Deletes a service control rule for HTTPS service.
no ip http server table {admin|user} rule *rule_number*	Deletes a service control rule for HTTP service.
show ip http server status	Displays HTTP settings.
show ip http server secure status	Displays HTTPS settings.

33.3.1 HTTP/HTTPS Command Examples

This following example adds a service control rule that allowed an administrator from the computers with the IP addresses matching the Marketing address object to access the WAN zone using HTTP service.

```
Router# configure terminal
Router(config)# ip http server table admin rule append access-group
Marketing zone WAN action accept
```

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
```

33.4 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.

33.4.1 SSH Implementation on the NXC

Your NXC 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 NXC for remote management on port 22 (by default).

33.4.2 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 NXC over SSH.

33.4.3 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 107 Command Summary: SSH

COMMAND	DESCRIPTION
`[no] ip ssh server`	Allows SSH access to the NXC CLI. The `no` command disables SSH access to the NXC CLI.
`[no] ip ssh server cert` *certificate_name*	Sets a certificate whose corresponding private key is to be used to identify the NXC 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.

Table 107 Command Summary: SSH (continued)

COMMAND	DESCRIPTION
[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).
ip ssh server rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny}	Sets a service control rule for SSH service. *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. *zone_object*: The name of the zone. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. You can also use pre-defined zone names like LAN and WLAN.
ip ssh server rule move *rule_number* to *rule_number*	Changes the index number of a SSH service control rule.
[no] ip ssh server v1	Enables remote management using SSH v1. The no command stops the NXC from using SSH v1.
no ip ssh server rule *rule_number*	Deletes a service control rule for SSH service.
show ip ssh server status	Displays SSH settings.

33.4.4 SSH Command Examples

This command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using SSH service.

```
Router# configure terminal
Router(config)# ip ssh server rule 2 access-group Marketing zone LAN action
accept
```

This command sets a certificate (Default) to be used to identify the NXC.

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

33.5 Telnet

You can configure your NXC for remote Telnet access.

33.6 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 108 Command Summary: Telnet

COMMAND	DESCRIPTION
`[no] ip telnet server`	Allows Telnet access to the NXC CLI. The `no` command disables Telnet access to the NXC 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).
`ip telnet server rule {`*`rule_number`*`|append|insert `*`rule_number`*`} access-group {ALL|`*`address_object`*`} zone {ALL|`*`zone_object`*`} action {accept|deny}`	Sets a service control rule for Telnet service. *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. *zone_object*: The name of the zone. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. You can also use pre-defined zone names like LAN and WLAN.
`ip telnet server rule move `*`rule_number`*` to `*`rule_number`*	Changes the index number of a service control rule.
`no ip telnet server rule `*`rule_number`*	Deletes a service control rule for Telnet service.
`show ip telnet server status`	Displays Telnet settings.

33.6.1 Telnet Commands Examples

This command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using Telnet service.

```
Router# configure terminal
Router(config)# ip telnet server rule 11 access-group RD zone LAN action
accept
```

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)#
```

33.7 Configuring FTP

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

33.7.1 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 109 Command Summary: FTP

COMMAND	DESCRIPTION
`[no] ip ftp server`	Allows FTP access to the NXC. The `no` command disables FTP access to the NXC.
`[no] ip ftp server cert certificate_name`	Sets a certificate to be used to identify the NXC. 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.
`ip ftp server rule {rule_number|append|insert rule_number} access-group {ALL|address_object} zone {ALL|zone_object} action {accept|deny}`	Sets a service control rule for FTP service. *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. *zone_object*: The name of the zone. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. You can also use pre-defined zone names like LAN and WLAN.
`ip ftp server rule move rule_number to rule_number`	Changes the index number of a service control rule.
`no ip ftp server rule rule_number`	Deletes a service control rule for FTP service.
`show ip ftp server status`	Displays FTP settings.

33.7.2 FTP Commands Examples

This command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using FTP service.

```
Router# configure terminal
Router(config)# ip ftp server rule 4 access-group Sales zone LAN action
accept
```

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
================================================================================
```

33.8 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your NXC supports SNMP agent functionality, which allows a manager station to manage and monitor the NXC through the network. The NXC supports SNMP version one (SNMPv1) and version two (SNMPv2c).

33.8.1 Supported MIBs

The NXC supports MIB II that is defined in RFC-1213 and RFC-1215. The NXC also supports private MIBs (AAT-private-lol.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 NXC's MIBs from www.zyxel.com.

33.8.2 SNMP Traps

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

Table 110 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 NXC 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.

33.8.3 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 111 Command Summary: SNMP

COMMAND	DESCRIPTION
`[no] snmp-server`	Allows SNMP access to the NXC. The `no` command disables SNMP access to the NXC.
`[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 NXC. The `no` command removes the contact information for the person in charge of the NXC.
`[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 host {`*`fqdn | ipv4_address`*`} [`*`community_string`*`]`	Sets the IP address or domain name of the host that receives the SNMP notifications. The `no` command removes the host that receives the SNMP notifications.
`[no] snmp-server location` *`description`*	Sets the geographic location (of up to 60 characters) for the NXC. The `no` command removes the geographic location for the NXC.
`[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`).
`snmp-server rule {`*`rule_number`*`|append|insert` *`rule_number`*`} access-group {ALL|`*`address_object`*`} zone {ALL|`*`zone_object`*`} action {accept|deny}`	Sets a service control rule for SNMP service. *`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. *`zone_object`*: The name of the zone. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. You can also use pre-defined zone names like LAN and WLAN.
`snmp-server rule move` *`rule_number`* `to` *`rule_number`*	Changes the index number of a service control rule.
`no snmp-server rule` *`rule_number`*	Deletes a service control rule for SNMP service.
`[no] snmp-server version {v2c|v3}`	Sets the SNMP version to use for communication with the SNMP manager. The `no` command does not allow SNMP managers using the specified SNMP version to access the NXC.
`[no] snmp-server v3user username` *`username`* `authentication {md5|sha} privacy {aes|des|none} privilege {ro|rw}`	Sets the SNMPv3 user account and its privilege of read-only (ro) or read-write (rw) access. The `no` command removes the SNMPv3 user account.
`show snmp status`	Displays SNMP Settings.
`show snmp-server v3user status`	Displays SNMPv3 user status.

33.8.4 SNMP Commands Examples

The following command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using SNMP service.

```
Router# configure terminal
Router(config)# snmp-server rule 11 access-group Example zone WAN action
accept
```

The following command sets the password (secret) for read-write (rw) access.

```
Router# configure terminal
Router(config)# snmp-server community secret rw
```

The following command sets the IP address of the host that receives the SNMP notifications to 172.23.15.84 and the password (sent with each trap) to qwerty.

```
Router# configure terminal
Router(config)# snmp-server host 172.23.15.84 qwerty
```

CHAPTER 34
Logs

This chapter provides information about the NXC'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 the User's Guide for the maximum number of system log messages in the NXC.

34.1 Log Commands Summary

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

Table 112 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.

34.1.1 Log Entries Commands

This table lists the commands to look at log entries.

Table 113 logging Commands: Log Entries

COMMAND	DESCRIPTION
show logging entries [priority *pri*] [category *module_name*] [srcip *ip*] [dstip *ip*] [service *service_name]* [begin <1..512> end <1..512>] [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..512> end <1..512>]	Displays the selected fields in the system log. *field*: time | msg | src | dst | note | pri | cat | all

34.1.2 System Log Commands

This table lists the commands for the system log settings.

Table 114 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 NXC generate a log for each connectivity check. The no command has the NXC only log the first connectivity check.
show connectivity-check continuous-log status	Displays whether or not the NXC generates a log for each connectivity check.
clear logging system-log buffer	Clears the system log.

34.1.2.1 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
512 events logged
suppression active  : yes
suppression interval: 10
category settings   :
    content-filter    : normal , forward-web-sites : no     ,
    blocked-web-sites : normal , user              : normal ,
    myZyxel.com       : normal , zysh              : normal ,
    idp               : normal , app-patrol        : normal ,
    ike               : normal , ipsec             : normal ,
    firewall          : normal , sessions-limit    : normal ,
    policy-route      : normal , built-in-service  : normal ,
    system            : normal , connectivity-check: normal ,
    device-ha         : normal , routing-protocol  : normal ,
    nat               : normal , pki               : normal ,
    interface         : normal , interface-statistics: no     ,
    account           : normal , port-grouping     : normal ,
    force-auth        : normal , l2tp-over-ipsec   : normal ,
    anti-virus        : normal , white-list        : normal ,
    black-list        : normal , ssl-vpn           : normal ,
    cnm               : normal , traffic-log       : no     ,
    file-manage       : normal , dial-in           : normal ,
    adp               : normal , default           : all    ,
```

34.1.3 Debug Log Commands

This table lists the commands for the debug log settings.

Table 115 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.

34.1.4 Remote Syslog Server Log Commands

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

Table 116 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> category {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.
[no] logging syslog <1..4> port <1..65535>	Sets the syslog server port number. The no command removes the port number setting.
[no] logging syslog <1..4> tls	Uses Transport Layer Security (TLS) to have encrypted communications between the syslog server and the NXC. The no command sets the NXC to not encrypt the communications.

34.1.5 E-mail Profile Log Commands

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

Table 117 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.
[no] logging mail <1..2> authentication	Enables SMTP authentication. The no command disables SMTP authentication.

Table 117 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 NXC 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 NXC to add the system date and time or the system name to the subject when the NXC mails to the specified e-mail profile. The no command sets the NXC 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> from *e_mail*	Sets the e-mail address from which the outgoing e-mail is delivered. The no command clears this field.
[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
[no] logging mail <1..2> tls activate	Encrypts the communications between the mail server and the NXC. The no command disables communication encryption.
logging mail <1..2> tls-type {tls | starttls}	Sets how you want communications between the mail server and the NXC 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.
logging mail sending_now	Sends mail immediately, according to the current settings.

34.1.5.1 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
```

34.1.6 Console Port Log Commands

This table lists the commands for the console port settings.

Table 118 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.

34.1.7 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 119 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.

Table 119 logging Commands: Access Point Settings (continued)

COMMAND	DESCRIPTION
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.
show wtp-logging result-status	Displays the AP logging result status.
show wtp-logging dbg-result-status	Displays the AP logging debug result status.
[no] wtp-logging syslog <1..4> category *module_name* disable	Disables the logging of the specified syslog category.
[no] wtp-logging syslog <1..4> category *module_name* level {normal | all}	Enables logging of the specified syslog category and specifies the logging level.
[no] wtp-logging mail <1..2> 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 system-log suppression	Enables log consolidation in the system log on the APs. The no command disables log consolidation in the debug log.
[no] wtp-logging system-log suppression interval <10..600>	Sets the log consolidation interval for the system log on the APs. The no command sets the interval to ten.
[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 35
Reports and Reboot

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

35.1 Report Commands Summary

The following sections list the report and session commands.

35.1.1 Report Commands

This table lists the commands for reports.

Table 120 report Commands

COMMAND	DESCRIPTION
`[no] report`	Begins data collection. The `no` command stops data collection.
`show report status`	Displays whether or not the NXC 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

35.1.2 Report Command Examples

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

```
Router# configure terminal
Router(config)# show report ge1 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 ge1 service
No. Port  Service          Amount          Direction
=================================================================
1   21    ftp              1273(bytes)     Outgoing
2   21    ftp              711(bytes)      Incoming
Router(config)# show report ge1 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
```

35.1.3 Session Commands

This table lists the command to display the current sessions for debugging or statistical analysis.

Table 121 session Commands

COMMAND	DESCRIPTION
show conn [user {*username*|any|unknown}] [service {*service-name*|any|unknown}] [source {*ip*|any}] [destination {*ip*|any}] [begin <1..100000>] [end <1..100000>]	Displays information about the selected sessions or about all sessions. You can look at all the active sessions or filter the information by user name, service object, source IP, destination IP, or session number(s). any means all users, services and IP addresses respectively. unknow means unknown users and services respectively.
show conn ip-traffic destination	Displays information about traffic session sorted by the destination.
show conn ip-traffic source	Displays information about traffic session sorted by the source.
show conn status	Displays the number of active sessions.

35.2 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 122 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 NXC 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 123 Email Daily Report Commands

COMMAND	DESCRIPTION
`daily-report [no] activate`	Turns daily e-mail reports on or off.
`show daily-report status`	Displays the e-mail daily report settings.
`daily-report`	Enter the daily report sub-command mode.
`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 NXC 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 cf-report`	Determines whether or not content filtering statistics are 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 station-count`	Determines whether or not the station statistics are included in the report e-mails.
`[no] item wtp-tx`	Determines whether or not the NXC's outgoing traffic statistics are included in the report e-mails.
`[no] item session-usage`	Determines whether or not session 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 idp-report`	Determines whether or not IDP statistics are included in the report e-mails.

Table 123 Email Daily Report Commands (continued)

COMMAND	DESCRIPTION
[no] item av-report	Determines whether or not anti-virus statistics are included in the report e-mails.
[no] item traffic-report	Determines whether or not network traffic statistics are included in 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.
schedule hour <0..23> minute <00..59>	Sets the time for sending out the report e-mails.
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.
no smtp-address	Resets the SMTP mail server configuration.
no smtp-auth username	Resets the authentication configuration.
smtp-port <1..65535>	Sets the SMTP service port.
no smtp-port	Resets the SMTP service port configuration.
smtp-tls {tls|starttls}	Sets how you want communications between the SMTP mail server and the NXC 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 NXC. The no command disables communication encryption.
send-now	Sends the daily e-mail report immediately.
reset-counter-now	Discards all report data and starts all of the counters over at zero.
[no] item wtp-rx	Determines whether or not the NXC's incoming traffic statistics are included in the report e-mails.

35.2.1 Email Daily Report Example

This example sets the NXC to send a daily report e-mail.

```
Router(config)# daily-report
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)# example-administrator@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 reset-counter
Router(config-daily-report)# item cpu-usage
Router(config-daily-report)# item mem-usage
Router(config-daily-report)# item session-usage
Router(config-daily-report)# item port-usage
Router(config-daily-report)# item idp-report
Router(config-daily-report)# item av-report
Router(config-daily-report)# item traffic-report
Router(config-daily-report)# daily-report activate
```

This displays the email daily report settings and has the NXC send the report now.

```
Router(config)# show daily-report status
email daily report status
=========================
activate: yes
scheduled time: 13:57
reset counter: no
smtp address: example-SMTP-mail-server.com
smtp auth: yes
smtp username: 12345
smtp password: pass12345
mail subject:  test subject
append system name: no
append date time: yes
mail from: my-email@example.com
mail-to-1: example-administrator@example.com
mail-to-2:
mail-to-3:
mail-to-4: my-email@example.com
mail-to-5:
cpu-usage: yes
mem-usage: yes
session-usage: yes
port-usage: yes
idp-report: yes
av-report: yes
as-report: yes
traffic-report: yes


Router(config)# daily-report send-now
```

35.3 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 36
Session Timeout

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 124 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> }`	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 | udp}`	Displays ICMP, TCP, and UDP session timeouts.

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 37
File Manager

This chapter covers how to work with the NXC's firmware, certificates, configuration files, custom IDP signatures, packet trace results, shell scripts and temporary files.

37.1 File Directories

The NXC stores files in the following directories.

Table 125 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
idp	IDP custom signatures	rules
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.

37.2 Configuration Files and Shell Scripts Overview

You can store multiple configuration files and shell script files on the NXC.

When you apply a configuration file, the NXC 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 NXC and run when you need them. When you run a shell script, the NXC 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 NXC. 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 20 Configuration File / Shell Script: Example

```
# enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
# configure ge3
interface ge3
ip address 172.16.37.240 255.255.255.0
ip gateway 172.16.37.254 metric 1
exit
# create address objects for remote management / to-NXC firewall rules
# use the address group in case we want to open up remote management later
address-object TW_SUBNET 172.16.37.0/24
object-group address TW_TEAM
address-object TW_SUBNET
exit
# enable Telnet access (not enabled by default, unlike other services)
ip telnet server
# open WLAN-to-NXC firewall for TW_TEAM for remote management
firewall WLAN NXC insert 4
sourceip TW_TEAM
service TELNET
action allow
exit
write
```

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

Table 126 Configuration Files and Shell Scripts in the NXC

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 20 on page 215 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 1.5 on page 21 for more information about CLI modes.)

37.2.1 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 NXC 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 NXC exit sub command mode.

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

Line 3 in the following example exits sub command mode.

```
interface ge1
ip address dhcp
!
```

Lines 1 and 3 in the following example are comments and line 4 exits sub command mode.

```
!
interface ge1
# this interface is a DHCP client
!
```

Lines 1 and 2 are comments. Line 5 exits sub command mode.

```
! this is from Joe
# on 2006/06/05
interface ge1
ip address dhcp
!
```

37.2.2 Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the NXC processes the file line-by-line. The NXC checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the NXC 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 NXC ignores any errors in the configuration file or shell script and applies all of the valid commands. The NXC still generates a log for any errors.

37.2.3 NXC Configuration File Details

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

- When you first receive the NXC, it uses the **system-default.conf** configuration file of default settings.
- When you change the configuration, the NXC creates a **startup-config.conf** file of the current configuration.
- The NXC checks the **startup-config.conf** file for errors when it restarts. If there is an error in the **startup-config.conf** file, the NXC 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 NXC reboots, if the **startup-config.conf** file passes the error check, the NXC 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.

37.2.4 Configuration File Flow at Restart

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

If there is a **startup-config.conf**, the NXC checks it for errors and applies it. If there are no errors, the NXC uses it and copies it to the **lastgood.conf** configuration file. If there is an error, the NXC 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 NXC 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 NXC ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The NXC still generates a log for any errors.

37.3 File Manager Commands Input Values

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

Table 127 File Manager Command Input Values

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

37.4 File Manager Commands Summary

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

Table 128 File Manager Commands Summary

COMMAND	DESCRIPTION
`apply /conf/`*`file_name.conf`* `[ignore-error] [rollback]`	Has the NXC 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 NXC 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 NXC with a fully valid configuration file. Use `rollback` without `ignore-error`: this gets the NXC started with a fully valid configuration file as quickly as possible. You can use the "`apply /conf/system-default.conf`" command to reset the NXC 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 NXC 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 NXC 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 NXC restarts.
`copy running-config /conf/`*`file_name.conf`*	Saves a duplicate of the configuration file that the NXC 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.
`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.

Table 128 File Manager Commands Summary (continued)

COMMAND	DESCRIPTION
run /script/*file_name.zysh*	Has the NXC 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 NXC ignore any errors in the startup-config.conf file and apply all of the valid commands.
show setenv-startup	Displays whether or not the NXC 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 NXC immediately uses configuration changes made via commands, but if you do not use the write command, the changes will be lost when the NXC restarts.

37.5 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/vpn_setup.zysh
```

37.6 FTP File Transfer

You can use FTP to transfer files to and from the NXC for advanced maintenance and support.

37.6.1 Command Line FTP File Upload

1. Connect to the NXC.
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 NXC.[1] For example:

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

   "put 1.00(XL.0).bin” transfers the firmware (1.00(XL.0).bin) to the NXC.

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

The firmware update can take up to five minutes. Do not turn off or reset the NXC while the firmware update is in progress! If you lose power during the firmware upload, you may need to refer to Section 37.9 on page 222 to recover the firmware.

37.6.2 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 NXC as next.conf.

Note: Uploading a custom signature file named "custom.rules", overwrites all custom signatures on the NXC.

Figure 21 FTP Configuration File Upload 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> 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.
```

37.6.3 Command Line FTP File Download

1. Connect to the NXC.
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.
5. Use "get” to download files. For example:

   “get vlan_setup.zysh vlan.zysh” transfers the vlan_setup.zysh configuration file on the NXC to your computer and renames it “vlan.zysh.”

37.6.4 Command Line FTP Configuration File Download Example

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

Figure 22 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.
```

37.7 Firmware Update Scheduling Commands

The NXC can be scheduled to install the firmware you uploaded at the specified date and time.

The following table lists the commands that you can use for firmware update scheduling.

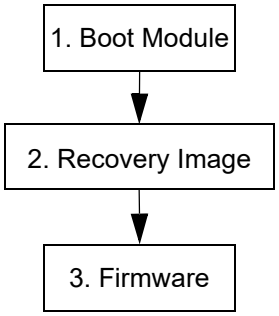
Table 129 Firmware Update Scheduling Commands Summary

COMMAND	DESCRIPTION
`firmware-update-schedule activate`	Turns on the firmware update scheduling feature.
`no firmware-update-schedule activate`	Turns off the firmware update scheduling feature.
`firmware-update-schedule time` *`date time`*	Sets the day in year-month-date format and the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to install the firmware. *`date`*: `yyyy-mm-dd` *`time`*: `hh:mm`
`no firmware-update-schedule time`	Removes the schedule settings.
`show firmware-update-schedule status`	Displays the version of the firmware that you uploaded to the NXC (via FTP or the Web Configurator) and the current firmware update scheduling settings.

37.8 NXC File Usage at Startup

The NXC uses the following files at system startup.

Figure 23 NXC 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 NXC notifies you if the recovery image is damaged.

2 The recovery image checks and loads the firmware. The NXC notifies you if the firmware is damaged.

37.9 Notification of a Damaged Recovery Image or Firmware

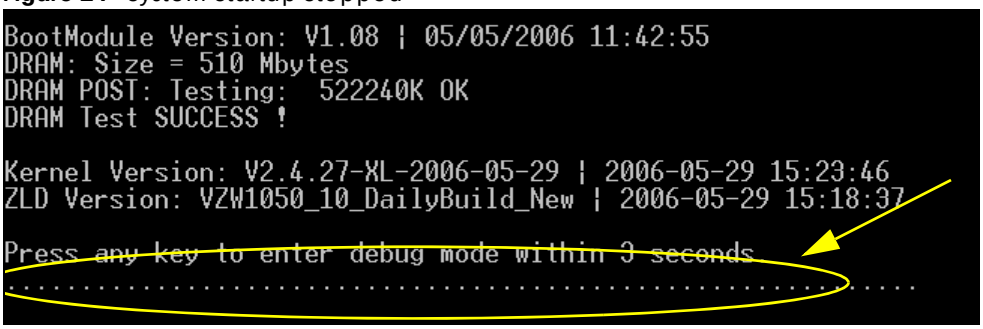
The NXC's recovery image and/or firmware could be damaged, for example by the power going off during a firmware upgrade. This section describes how the NXC notifies you of a damaged recovery image or firmware file. Use this section if your device has stopped responding for an extended period of time and you cannot access or ping it. Note that the NXC 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 NXC via a terminal emulation program (such as HyperTerminal). Your console session displays the NXC's startup messages. If you cannot see any messages, check the terminal emulation program's settings (see Section 1.2.1 on page 15) and restart the NXC.

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

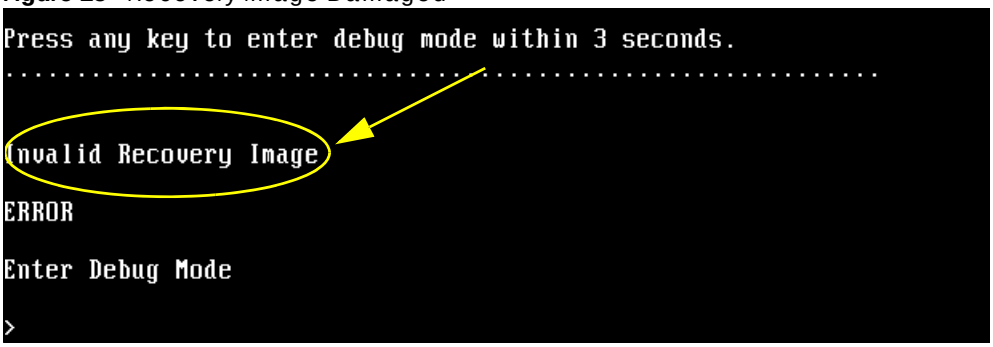
Note: Do not press any keys at this point. Wait to see what displays next.

Figure 24 System Startup Stopped



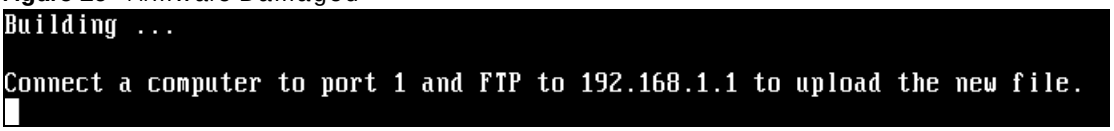
3 If the console session displays “Invalid Firmware”, or “Invalid Recovery Image”, or the console freezes at "Press any key to enter debug mode within 3 seconds" for more than one minute, go to Section 37.10 on page 223 to restore the recovery image.

Figure 25 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 37.11 on page 225 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 26 Firmware Damaged



37.10 Restoring the Recovery Image (NXC5200 Only)

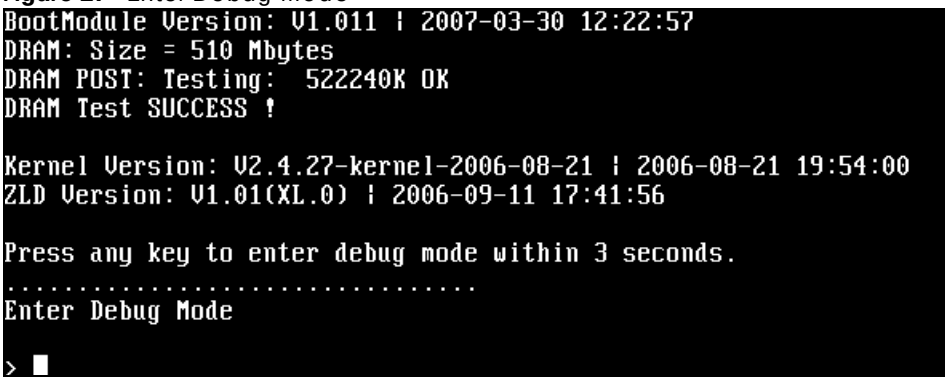
This procedure requires the NXC’s recovery image. Download the firmware package from www.zyxel.com and unzip it. The recovery image uses a .ri extension, for example, "1.01(XL.0)C0.ri". Do the following after you have obtained the recovery image file.

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

1 Restart the NXC.

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

Figure 27 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 28 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)
```

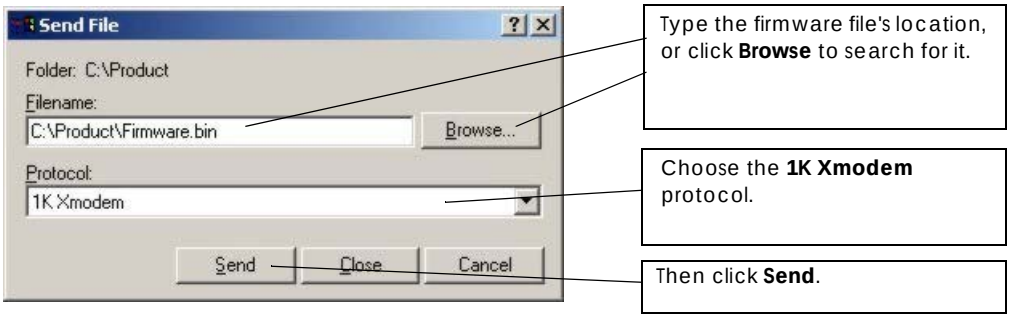
4 Enter `Y` and wait for the “Starting XMODEM upload” message before activating XMODEM upload on your terminal.

Figure 29 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 30 Example Xmodem Upload



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

Figure 31 Recovery Image Upload Complete

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

OK


>
```

7 Enter `atgo`. The NXC 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 37.11 on page 225 to recover the firmware.

Figure 32 atgo Debug Command

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

37.11 Restoring the Firmware

This procedure requires the NXC'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 NXC's port **1** (only port **1** can be used).

2 The NXC'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 NXC. 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 NXC. 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 33 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 34 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 NXC recovers the firmware.

Figure 35 Firmware Received and Recovery Started

```
Firmware received ...

[Update Filesystem]
       Updating Code
       ..
```

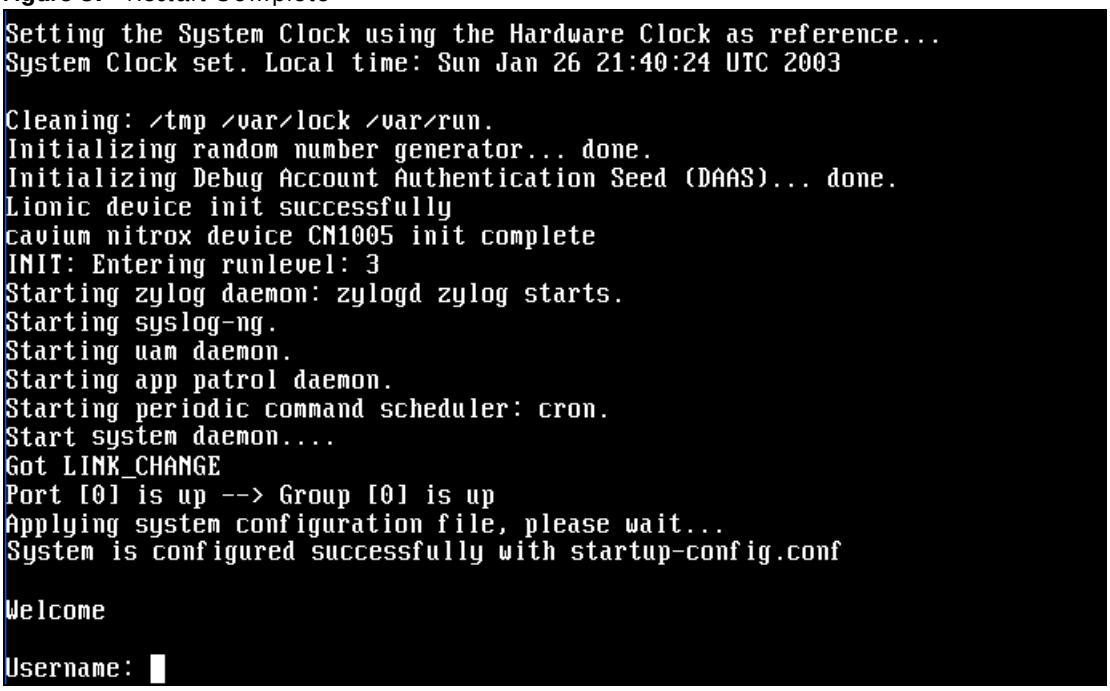
9 The console session displays “done” when the firmware recovery is complete. Then the NXC automatically restarts.

Figure 36 Firmware Recovery Complete and Restart

```
.....
.....
.....
.....
.....
.....
.....
       done

[Update Kernel]
       Extracting Kernel Image
       ..
       done
       Writing Kernel Image ... done

[Update BootModule]
       Extracting BootModule Image
       .
       done
       Writing BootModule
       .....
.....                                  done
Restarting system.
```

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

Figure 37 Restart Complete



37.12 Restoring the Default System Database

The default system database stores information such as the default anti-virus or IDP signatures. The NXC can still operate if the default system database is damaged or missing, but related features (like anti-virus or IDP) may not function properly.

If the default system database file is not valid, the NXC displays a warning message in your console session at startup or when reloading the anti-virus or IDP signatures. It also generates a log. Here are some examples. Use this section to restore the NXC's default system database.

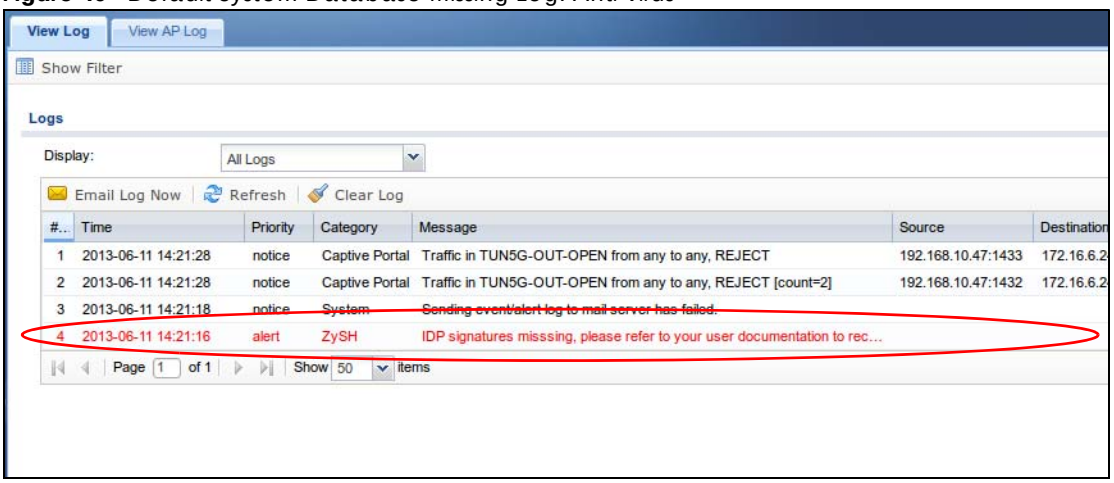
Figure 38 Default System Database Console Session Warning at Startup: Anti-virus

```
Hostname: localhost.

Setting the System Clock using the Hardware Clock as reference...
System Clock set. Local time: Fri May 11 09:31:55 GMT 2007

Cleaning: /tmp /var/lock /var/run.
Initializing random number generator... done.
Initializing Debug Account Authentication Seed (DAAS)... done.
INIT: Entering runlevel: 3
Starting zylog daemon: zylogd zylog starts.
Starting syslog-ng.
Starting uam daemon.
Starting app patrol daemon.
Starting periodic command scheduler: cron.
Start system daemon....
Got LINK_CHANGE
Port [1] is up --> Group [1] is up
% Anti-Virus signatures misssing, refer to your user documentation to recover th
e default database file.
% Loading AV signature database has failed.
Applying system configuration file, please wait...
System is configured successfully with startup-config.conf

Welcome

Username:
```

Figure 39 Default System Database Console Session Warning When Reloading IDP

```
Router(config)# idp reload
IDP signatures misssing, please refer to your user documentation to recover the
default database file.
retval = -32056
ERROR: Enable IDP engine failed.
Router(config)#
```

Figure 40 Default System Database Missing Log: Anti-virus



This procedure requires the NXC's default system database file. Download the firmware package from www.zyxel.com and unzip it. The default system database file uses a .db extension, for example, "1.01(XL.0)C0.db". Do the following after you have obtained the default system database file.

37.12.1 Using the atkz -u Debug Command (NXC5200 Only)

Note: You only need to use the `atkz -u` command if the default system database is damaged.

1 Restart the NXC.

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

Figure 41 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 `atkz -u` to start the recovery process.

Figure 42 atkz -u Command for Restoring the Default System Database

```
> atkz -u
-u
OK

> atgo
Booting...
```

4 "Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file" displays on the screen. Connect your computer to the NXC's port **1** (only port **1** can be used).

Figure 43 Use FTP with Port 1 and IP 192.168.1.1 to Upload File

```
Checking CODE ... Done

Updating ...

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

5 The NXC'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.

6 Use an FTP client on your computer to connect to the NXC. For example, in the Windows command prompt, type `ftp 192.168.1.1`. Keep the console session connected in order to see when the default system database recovery finishes.

7 Hit enter to log in anonymously.

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

9 Transfer the firmware file from your computer to the NXC. 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.db`.

Figure 44 FTP Default System Database 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 03:56 and the load is 0.00. 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> bin
200 TYPE is now 8-bit binary
ftp> put E:\ftproot\ZLD_FW\101XL\101XL0C0\1.01(XL.0)C0.db
```

10 Wait for the file transfer to complete.

Figure 45 FTP Default System Database Transfer Complete

```
200 PORT command successful
150 Connecting to port 3709
226-248.5 Mbytes free disk space
226-File successfully transferred
226 0.008 seconds (measured here), 13.31 Mbytes per second
ftp: 112398 bytes sent in 0.02Seconds 7024.88Kbytes/sec.
ftp> _
```

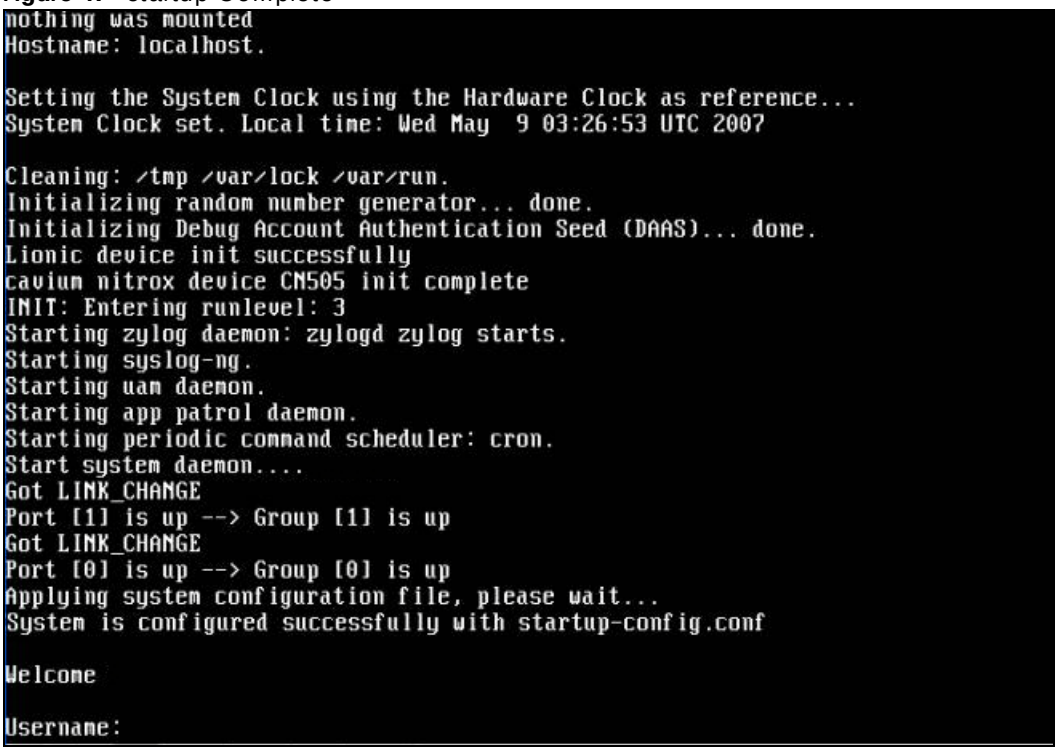
11 The console session displays "done" after the default system database is recovered.

Figure 46 Default System Database Received and Recovery Complete

```
Default System Database received ...

[Update Filesystem]
        Updating Database
        .
        done
```

12 The username prompt displays after the NXC starts up successfully. The default system database recovery process is now complete and the NXC IDP and anti-virus features are ready to use again.

Figure 47 Startup Complete



CHAPTER 38
Diagnostics

This chapter covers how to use the diagnostics feature.

38.1 Diagnostics

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

38.2 Diagnosis Commands

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

Table 130 diagnosis Commands

COMMAND	DESCRIPTION
`show tech-support <category> [commands]`	Use this command when instructed by customer support or if an AP doesn't respond when using the diagnostic button in the web configurator. Displays diagnostics information of a specific managed AP. You can choose to displays all information or information for a certain category. Follow the steps below: 1. Access the Command Line Interface (CLI) of a specific AP by using the IP address of the AP and an SSH client, or access the AP directly from the console port. Do not use Telnet. 2. If you access the AP through an SSH client, type `sshcon enable`, then `show tech-support`. Type `sshcon disable` when you are done. 3. If you access the AP through its console port, type `show tech-support`.
`diag-info collect`	Has the NXC create a new diagnostic file.
`[no] diag-info copy usb-storage`	Sets the NXC to create an extra copy of the diagnostic file to a connected USB storage device. Use the `no` parameter to not create an extra copy of the diagnostic file to a connected USB storage device.
`diaginfo collect ac`	Has the NXC create a new diagnostic file containing its own configuration and diagnostic information.

Table 130 diagnosis Commands (continued)

COMMAND	DESCRIPTION
diaginfo collect wtp	Has the NXC create a new diagnostic file containing the managed AP's configuration and diagnostic information.
diaginfo set {ac|wtp} <1..511>	Sets which categories you want the NXC to include in the diagnostic file. 1: the system category 511: all categories
diaginfo set wtpmac *mac_address*	Specifies the MAC address of the managed AP that you want the NXC to generate a diagnostic file containing its configuration.
show diag-info	Displays the name, size, and creation date (in yyyy-mm-dd hh:mm:ss format) of the diagnostic file.
show diaginfo category {ac|wtp}	Displays each category of settings and which categories you set the NXC to include in the diagnostic file.
show diag-info copy usb-storage	Displays whether the NXC is set to create an extra copy of the diagnostic file to a connected USB storage device.
show diaginfo collect ac status	Displays whether the NXC is ready to or have finished generating a diagnostic file (**Standby**), the NXC is generating a diagnostic file containing its own configuration and diagnostic information (**Busy on Controller**) or the NXC is generating a diagnostic file for the selected managed AP(s) (**Busy on AP**).
show diaginfo collect wtp status	Displays whether the NXC is ready to or have finished generating a diagnostic file (**Standby**), the NXC is generating a diagnostic file for the selected managed AP(s) (**Busy on AP**) or the NXC is generating a diagnostic file containing its own configuration and diagnostic information (**Busy on Controller**). This also shows the number of managed APs whose configuration has been contained in the file and the number of managed APs you selected to generate a diagnostic file.

38.3 Diagnosis Commands Example

The following example shows the result of `show tech-support` using an SSH client.

Note: This information can be used by customer support to troubleshoot a managed AP that is not responding to the NXC.

```
Router> sshcon enable
ioctl ret: 0, 2
argv list: zysh, attach, 1
cmd: /util/suexec /sbin/insmod /lib/modules/2.6.32.27/
extra/ptycon.koptyconsole
=/dev/pts/0
ioctl ret: 0, 2
DEBUG: pid = 9653, ppid = 9616
DEBUG: compare pid: 1539
DEBUG: compare pid: 9616
DEBUG: SSH login session, ppid: 9616
DEBUG: is SSH user.
DEBUG: cmd: ps aux | grep 9616 | grep ssh
DEBUG: cmd result: root     9616  4.8  0.2  16972  2912 ?
Ss 06:50 0
:00 sshd: admin@pts/0

DEBUG: pts ridx str: /0

DEBUG: pts #: 0
DEBUG: cmd: lsmod | grep ptycon
DEBUG: cmd result:
ptycon                  2671  0

DEBUG: cmd: lsmod | grep ptycon
DEBUG: cmd result:
ptycon                  2671  0

sshcon driver attached successfully.
Router> show tech-support
aaa           capwap       interface    networking   system
all           customized   logs         others
Router> show tech-support networking
Router> ZySH system commands output
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++
debug system brctl show
--------------------------------------------------------------
---------------------
bridge name     bridge id               STP enabled
interfaces
vlan0           8000.1c740df81dec       no              old1-1
                                                        old2-1

debug system ifstat
```

The following example shows how to use the command `sshcon disable`.

```
Name: admin
Type: admin
From: 172.21.40.31
MAC: DC-4A-3E-40-EC-67
Associated AP: -
Service: ssh
MP_Idx: 0
Session_Time: 00:00:23
Idle_Time: unlimited
Lease_Timeout: 00:29:55
Re_Auth_Timeout: unlimited
User_Info: admin(admin),
Re-Auth. Type: re-auth-time
Due Time: 12:00
Acct. Status: -
Profile Name: N/A
Authenticator: -



Router> sshcon disable
ioctl ret: 0, 2
```

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
```

The following example specifies the MAC address of the managed AP, sets the categories and creates a diagnostic file.

```
Router# configure terminal
Router(config)# diaginfo set wtpmac 00:a0:c5:01:23:45
Router(config)# diaginfo set wtp 511
Router(config)# show diaginfo category ac
No.  Diagnostic Category              Active         Hidden
================================================================================
1    System                            yes            no
2    Networking                        yes            no
3    Interface                         yes            no
4    CAPWAP                            yes            no
5    Wireless                          yes            no
6    AAA                               yes            no
7    Logs                              yes            no
8    Others                            yes            no
9    Customized                        yes            no
10   CustomizedScript                  511            no
Router(config)# diaginfo collect wtp
Please wait, collecting information
Router(config)#
```

CHAPTER 39
Packet Flow Explore

This chapter covers how to use the packet flow explore feature.

39.1 Packet Flow Explore

Use this to get a clear picture on how the NXC determines where to forward a packet and how to change the source IP address of the packet according to your current settings. This function provides you a summary of all your routing and SNAT settings and helps troubleshoot the related problems.

39.2 Packet Flow Explore Commands

The following table lists the commands that you can use to have the NXC display routing and SNAT related settings.

Table 131 Packet Flow Explore Commands

COMMAND	DESCRIPTION
`show route order`	Displays the order of routing related functions the NXC checks for packets. Once a packet matches the criteria of a routing rule, the NXC takes the corresponding action and does not perform any further flow checking.
`show system snat order`	Displays the order of SNAT related functions the NXC checks for packets. Once a packet matches the criteria of an SNAT rule, the NXC uses the corresponding source IP address and does not perform any further flow checking.
`show system default-snat`	Displays whether the NXC enable SNAT or not. The NXC performs SNAT by default for traffic going to or from the WAN interfaces.
`show system route policy-route`	Displays activated policy routes.
`show system route nat-1-1`	Displays activated 1-to-1 NAT rules.
`show system snat default-snat`	Displays activated default routes which use SNAT.
`show system snat order`	Displays the order of SNAT related functions the NXC checks for packets. Once a packet matches the criteria of an SNAT rule, the NXC uses the corresponding source IP address and does not perform any further flow checking.
`show system snat nat-1-1`	Displays activated NAT rules which use SNAT.
`show system snat nat-loopback`	Displays activated NAT rules which use SNAT with NAT loopback enabled.
`show system snat policy-route`	Displays activated policy routes which use SNAT.

39.3 Packet Flow Explore Commands Example

The following example shows all routing related functions and their order.

```
Router> show route order
route order: Direct Route, Policy Route, 1-1 SNAT, Main Route
```

The following example shows all SNAT related functions and their order.

```
Router> show system snat order
snat order: Policy Route SNAT, 1-1 SNAT, Loopback SNAT, Default SNAT
```

The following example shows all activated policy routes.

```
Router> show system route policy-route
No.  PR NO. Source                         Destination                    In
coming
     DSCP   Service                        Source Port                    Ne
xthop Type                     Nexthop Info
================================================================================
====
```

The following example shows all activated 1-to-1 SNAT rules.

```
Router> show system route nat-1-1
No.  VS Name                          Source                         Destinati
on   Outgoing        Gateway
================================================================================
==========================================
```

The following example shows all activated policy routes which use SNAT.

```
Router> show system snat policy-route
No.  PR NO. Outgoing        SNAT
================================================================================
Router>
```

The following example shows all activated 1-to-1 NAT rules.

```
Router> show system snat nat-1-1
No.  VS Name                          Source                         Destinati
on   Outgoing        SNAT
================================================================================
===========
```

CHAPTER 40
Maintenance Tools

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

40.1 Maintenance Tools Commands

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

Table 132 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*]	Sends traffic through the specified interface with the specified protocol, source address, destination address, and/or port number. If you specify `file`, the NXC dumps the traffic to `/packet_trace/packet_trace_interface`. Use FTP to retrieve the files (see Section 37.6 on page 219). If you do not assign the duration, the NXC 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.
show arp-table	Displays the current Address Resolution Protocol table.
show arp reply restricted	Displays whether the NXC is set to only respond to ARP requests, in which both the source and destination IP addresses are in different subnets.
show packet-capture status	Displays whether a packet capture is ongoing.
show packet-capture config	Displays current packet capture settings.

Table 132 Maintenance Tools Commands in Privilege Mode (continued)

COMMAND	DESCRIPTION
show wtp-packet-capture available-size	Displays the storage size available on the AP.
show wtp-packet-capture config	Displays current packet capture settings for the AP.
show wtp-packet-capture interface	Displays the interfaces available on the AP.
show wtp-packet-capture query-status	Displays whether the interfaces, filter configuration and available storage size for the AP are updated successfully.
show wtp-packet-capture status	Displays whether a packet capture for an AP is ongoing.

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

Table 133 Maintenance Tools Commands in Configuration Mode

COMMAND	DESCRIPTION
arp *ip_address mac_address*	Edits or creates an ARP table entry.
no arp *ip_address*	Removes an ARP table entry.
[no] arp reply restricted	Sets the NXC to only respond to ARP requests, in which both the source and destination IP addresses are in different subnets. The no command sets the NXC to respond to any ARP request.
[no] packet-capture activate	Performs a packet capture that captures network traffic going through the set NXC's interface(s). Studying these packet captures may help you identify network problems. The no command stops the running packet capture on the NXC. 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 NXC 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.
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".

Table 133 Maintenance Tools Commands in Configuration Mode (continued)

COMMAND	DESCRIPTION
files-size <1..1000000000>	Specify a maximum size limit in kilobytes for the total combined size of all the capture files on the NXC, including any existing capture files and any new capture files you generate. The NXC 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-version {any | ip | ip6}	Sets the version of the Internet Protocol (IP) by which traffic is routed across the networks and Internet. any means to capture packets for traffic sent by either IP version.
proto-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 NXC 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.
[no] wtp-packet-capture *ap_mac* activate	Performs a packet capture that captures network traffic going through the set AP's interface(s). Studying these packet captures may help you identify network problems. The no command stops the running packet capture on the specified AP. Note: Use the wtp-packet-capture configure command to configure the AP packet-capture settings before using this command.
wtp-packet-capture *ap_mac* configure	Enters the sub-command mode.
duration <0..300>	Sets a time limit in seconds for the capture. The NXC has the AP stop the capture and generate 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.
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".

Table 133 Maintenance Tools Commands in Configuration Mode (continued)

COMMAND	DESCRIPTION
files-size <1..10>	Specify a maximum size limit in megabytes for the total combined size of all the capture files on the NXC, including any existing capture files and any new capture files you generate. The valid range depends on the AP's available storage size. Use the show wtp-packet-capture available-size command to display the storage size available on the AP. The NXC has the AP stop the capture and generate 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-version {any | ip | ip6}	Sets the version of the Internet Protocol (IP) by which traffic is routed across the networks and Internet. any means to capture packets for traffic sent by either IP version.
proto-type {ah | any | esp | icmp | icmp6 | igmp | igrp | pim | tcp | udp | vrrp}	Sets the protocol of traffic for which to capture packets. any means to capture packets for all types of traffic.
snaplen <1..1514>	Specifies the maximum number of bytes to capture per packet. The AP 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.
storage {internal | usbstorage}	Sets the location where the packet captures files are stored. internal: the NXC only stores packet capture entries on the NXC. The NXC reserves some onboard storage space as a buffer. usbstorage: the NXC stores packet capture entries only on a USB storage device connected to the NXC. The NXC reserves some USB storage space as a buffer.
wtp-packet-capture *ap_mac* query	Updates the interfaces, filter configuration and available storage size for the specified AP.

40.1.1 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 ge2 ip-proto icmp file extension-filter -s
-> 500 -n
tcpdump: listening on eth1
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# packet-trace interface ge2 ip-proto icmp file extension-filter
-> and src host 192.168.105.133 and dst host 192.168.105.40 -s 500 -n
tcpdump: listening on eth1
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# traceroute www.zyxel.com
traceroute to www.zyxel.com (203.160.232.7), 30 hops max, 38 byte packets
 1  172.16.13.254  3.049 ms  1.947 ms  1.979 ms
 2  172.16.6.253  2.983 ms  2.961 ms  2.980 ms
 3  172.16.6.1  5.991 ms  5.968 ms  6.984 ms
 4  * * *
```

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                    ge1
172.23.19.254           ether   00:04:80:9B:78:00   C                     ge2
Router# no arp 192.168.1.10
Router# show arp-table
Address                HWtype  HWaddress           Flags Mask            Iface
192.168.1.10                    (incomplete)                              ge1
172.23.19.254           ether   00:04:80:9B:78:00   C                     ge2
```

The following examples show how to configure packet capture settings and perform a packet capture of network traffic going through the NXC's interface(s).

1 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: wan1,lan2,wan2
ip-type: any
host-port: 0
host-ip: any
file-suffix: Example
snaplen: 1500
duration: 150
file-size: 10000
```

2 Then configure the following settings to capture packets going through the NXC's WAN1 interface only (this means you have to remove LAN2 and WAN2 from the iface list).

- IP address: any
- Host IP: any
- Host port: any (then you do not need to configure this setting)
- File suffix: Example
- File size: 10000 bytes
- Duration: 150 seconds

```
Router(config)# packet-capture configure
Router(packet-capture)# iface add wan1
Router(packet-capture)# iface del lan2
Router(packet-capture)# iface del wan2
Router(packet-capture)# ip-type any
Router(packet-capture)# host-ip any
Router(packet-capture)# file-suffix Example
Router(packet-capture)# files-size 10000
Router(packet-capture)# duration 150
Router(packet-capture)#
```

3 Exit the sub-command mode and have the NXC capture packets according to the settings you just configured.

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

4 Manually stop the running packet capturing.

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

5 Check current packet capture status and list all packet captures the NXC has performed.

```
Router(config)# show packet-capture status
capture status: off
Router(config)# dir /packet_trace
File Name                                          Size     Modified Time
==========================================================================
wan1-Example.cap                                 575160   2009-11-24 09:06:59
Router(config)#
```

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

The following examples show how to configure packet capture settings and perform a packet capture of network traffic going through the managed AP's interface(s).

1 First you have to update the interface and filter configuration and storage size available on the managed AP. You can check whether they are updated successfully.

```
Router(config)# wtp-packet-capture A0:E4:CB:84:B9:F2 query
Router(config)# show wtp-packet-capture query-status
query status: success
```

2 Then you can also check the AP's available storage size, interfaces and current packet capture settings.

```
Router(config)# show wtp-packet-capture available-size
MAC: A0:E4:CB:84:B9:F2
Available Size: 10 MB
Router(config)# show wtp-packet-capture interface
MAC: A0:E4:CB:84:B9:F2
Available Interface:
eth0,br0,localbr4000,vlan1,hostvlan4000,brtunnel4000,wlan-2-1.4000,wlan-1-
2.1,wlan-2-1,wlan-1-2
Router(config)# show wtp-packet-capture config
MAC: A0:E4:CB:84:B9:F2
iface: None
ip-version: any
proto-type: any
host-port: 0
host-ip: any
file-suffix: -packet-capture
snaplen: 1500
duration: 0
file-size: 10
storage: 0
```

3 Then configure the interface setting and a maximum limit in megabytes for each capture file to capture packets going through the AP's wlan-2-1 interface. Exit the sub-command mode.

```
Router(config)# wtp-packet-capture A0:E4:CB:84:B9:F2 configure
Router(wtp-packet-capture)# iface add wlan-2-1
Router(wtp-packet-capture)# files-size 5
Router(wtp-packet-capture)# exit
```

4 Have the managed AP capture packets according to the settings you just configured. Check current packet capture status.

```
Router(config)# wtp-packet-capture A0:E4:CB:84:B9:F2 activate
Router(config)# show wtp-packet-capture status
MAC: A0:E4:CB:84:B9:F2
capture status: on
```

5 Manually stop the running packet capturing and show current packet capture status.

```
Router(config)# no wtp-packet-capture A0:E4:CB:84:B9:F2 activate
Router(config)# show wtp-packet-capture status
MAC: A0:E4:CB:84:B9:F2
capture status: off
```

6 List all packet captures the AP has performed.

```
Router(config)# dir /packet_trace/
File Name                                                 Size        Modified Time
================================================================================
ge1--packet-capture-packet-capture.00000.cap            144732   2018-11-19 14:49:06
ap-A0E4CB84B9F2-wlan-2-1--packet-capture.cap              1440   2018-11-21 15:50:22
```

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

CHAPTER 41
Watchdog Timer

This chapter provides information about the NXC's watchdog timers.

41.1 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 134 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.
`hardware-watchdog-timer start`	Enables the hardware watchdog timer.
`show hardware-watchdog-timer status`	Displays the settings of the hardware watchdog timer.

41.2 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 135 software-watchdog-timer Commands

COMMAND	DESCRIPTION
`[no] software-watchdog-timer` *`timer`*	Sets how long the system's core firmware can be unresponsive before resetting. The `no` command turns the timer off. *`timer`*: 10 to 600 (NXC5200) or 10 to 60 (NXC2500).
`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.

41.3 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 136 app-watchdog Commands

COMMAND	DESCRIPTION
`[no] app-watch-dog activate`	Turns the application watchdog timer on or off.
`[no] app-watch-dog alert`	Has the NXC send an alert the user when the system is out of memory or disk space.
`[no] app-watch-dog auto-recover`	If app-watch-dog detects a dead process, app-watch-dog will try to auto recover. The `no` command turns off auto-recover.
`[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 cpu-threshold min <1..100> max <1..100>`	Sets the percentage thresholds for sending a CPU usage alert. The NXC starts sending alerts when CPU usage exceeds the maximum (the second threshold you enter). The NXC stops sending alerts when the CPU 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 disk-threshold min <1..100> max <1..100>`	Sets the percentage thresholds for sending a disk usage alert. The NXC starts sending alerts when disk usage exceeds the maximum (the second threshold you enter). The NXC 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 interval` *`interval`*	Sets how frequently (in seconds) the NXC checks the system processes. The `no` command changes the setting back to the default. *`interval`*: 5 to 60 (NXC5200) or 5 to 300 (NXC2500).
`[no] app-watch-dog mem-threshold min <1..100> max <1..100>`	Sets the percentage thresholds for sending a memory usage alert. The NXC starts sending alerts when memory usage exceeds the maximum (the second threshold you enter). The NXC 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.
`app-watch-dog reboot-log flush`	Flushes the reboot log record.
`[no] app-watch-dog retry-count <1..5>`	Set how many times the NXC is to re-check a process before considering it failed. The `no` command changes the setting back to the default.
`[no] app-watch-dog sys-reboot`	If auto recover fail reaches the maximum retry count, app-watch-dog reboots the device. The `no` command turns off system auto reboot.
`show app-watch-dog config`	Displays the application watchdog timer settings.
`show app-watch-dog monitor-list`	Displays the list of applications that the application watchdog is monitoring.
`show app-watch-dog reboot-log`	Displays the application watchdog reboot log.

41.3.1 Application Watchdog Commands Example

The following example displays the application watchdog configuration.

```
Router# configure terminal
Router(config)# show app-watch-dog config
Application Watch Dog Setting:
  activate: yes
  alert: yes
  console print: always
  retry count: 3
  auto recover: yes
  system reboot: yes
  interval: 60 seconds
  mem threshold: 80% ~ 90%
  cpu threshold: 80% ~ 90%
  disk threshold: 80% ~ 90%
Router(config)#
```

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

```
Router# configure terminal
Router(config)# show app-watch-dog monitor-list
#app_name        min_process_count  max_process_count(-1 unlimited) recover_enable
      recover_reboot  recover_always  recover_max_try_count  ecover_max_fail_count
uamd                    1                                -1                      1
                2               1               1                       3
firewalld               1                                -1                      0
                1               1               1                       3
policyd                 1                                -1                      1
                1               1               1                       3
classify                1                                -1                      0
                1               1               1                       3
resd                    1                                -1                      0
                1               1               1                       3
zyshd_wd                1                                -1                      0
                1               1               1                       3
zyshd                   1                                -1                      0
                0               1               1                       3
httpd                   1                                -1                      1
httpd                   1                                -1                      1
dhcpd                   1                                -1                      1
                1               1               1                       3
zylogd                  1                                -1                      0
                1               1               1                       3
syslog-ng               1                                -1                      0
                1               1               1                       3
zylogger                1                                -1                      0
                1               1               1                       3
ddns_had                1                                -1                      0
                1               1               1                       3
zebra                   1                                -1                      0
                1               1               1                       3
link_updown             1                                -1                      0
                1               1               1                       3
fauthd                  1                                -1                      0
                1               1               1                       3
signal_wrapper          1                                -1                      0
                1               1               1                       3
capwap_srv              1                                1                       0
                1               1               1                       3
ipmonitord              1                                -1                      0
                1               1               1                       3
Router(config)#
```

CHAPTER 42
Managed AP Commands

Connect directly to a managed AP's CLI (Command Line Interface) to configure the managed AP's CAPWAP (Control And Provisioning of Wireless Access Points) client and DNS server settings.

42.1 Managed Series AP Commands Overview

Log into an AP's CLI and use the commands in this chapter if the AP does not automatically connect to the NXC or you need to configure the AP's DNS server. Use the CAPWAP client commands to configure settings to let the AP connect to the NXC. Use the DNS server commands to configure the DNS server address to which the AP connects. When the AP reboots, it only keeps the configuration from commands covered in this chapter.

42.2 Accessing the AP CLI

Connect to the AP's console port and use a terminal emulation program or connect through the network using Telnet or SSH. The settings and steps for logging in are similar to connecting to the NXC. See Section 1.2 on page 14 for details.

Note: The AP's default login username is **admin** and password is **1234**. The username and password are case-sensitive. If the AP has connected to the NXC, the AP uses the same admin password as the NXC.

Use the `write` command to save the current configuration to the NXC.

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

42.3 CAPWAP Client Commands

Use the CAPWAP client commands to configure the AP's IP address and other related management interface settings. Do not use the original interface commands to configure the IP address and related settings on the AP, because the AP does not save interface command settings after rebooting.

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

Table 137 Input Values for CAPWAP Client Commands

LABEL	DESCRIPTION
ip	IPv4 address.
netmask	The network subnet mask. For example, 255.255.255.0.
gateway	The default gateway IP address of the interface. Enter a standard IPv4 IP address (for example, 127.0.0.1).
primary_ac_ap	The primary IPv4 address of the NXC.
secondary_ac_ap	Optional IPv4 address of the NXC.
vid	The VLAN ID (1~4094) of the managed AP.
primary_ac_dns	The primary fully qualified domain name (FQDN) of the NXC.
secondary_ac_dns	The secondary fully qualified domain name (FQDN) of the NXC.

The following table describes commands for configuring the AP's CAPWAP client parameters, which include the management interface. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 138 Command Summary: CAPWAP Client

COMMAND	DESCRIPTION
`capwap ap vlan ip address` *ip netmask*	Sets the IP address and network mask of the AP's management interface.
`capwap ap vlan ip gateway` *gateway*	Sets the default gateway IP address for the AP's management interface.
`capwap ap vlan no ip gateway`	Clears the default gateway IP address setting for the AP's management interface.
`capwap ap vlan vlan-id` *vid* `{ tag | untag }`	Sets the AP's management VLAN ID as well as whether the AP sends tagged or untagged packets. The management VLAN on the NXC and AP must match for the NXC to manage the AP. The NXC's force vlan command (see Table 31 on page 70) takes priority over this command.
`capwap ap ac-ip` *{primary_ac_ip|primary_ac_dns} {secondary_ac_ip|secondary_ac_dns}*	Specifies the primary and secondary IP address or domain name of the AP controller (the NXC) to which the AP connects.
`capwap ap ac-ip auto`	Sets the AP to use DHCP to get the address of the AP controller (the NXC).
`show capwap ap info`	Displays the IP address of the NXC managing the AP and CAPWAP settings and status.
`show capwap ap discovery-type`	Displays how the AP finds the NXC.
`show capwap ap ac-ip`	Displays the address of the NXC or `auto` if the AP finds the NXC through broadcast packets.

42.3.1 CAPWAP Client Commands Example

This example shows how to configure the AP's management interface and how it connects to the AP controller (the NXC), and check the connecting status. The following commands:

- Display how the AP finds the NXC

- Set the AP's management IP address to 192.168.1.37 and netmask 255.255.255.0
- Set the AP's default gateway IP address to 192.168.1.32
- Sets the AP's management interface to use VLAN ID 2 and send tagged packets
- Specifies the primary and secondary IP addresses of the NXC (192.168.1.1 and 192.168.1.2) to which the AP connects.
- Displays the settings it configured

```
Router# configure terminal
Router(config)# show capwap 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 vlan vlan-id 2 tag
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
                AC-IP                   192.168.1.1
       Discovery type                   Static AC IP
             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
```

42.4 DNS Server Commands

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

Table 139 Command Summary: DNS Server

COMMAND	DESCRIPTION
`ip dns server zone-forwarder {<1..32>|append|insert <1..32>} {`*`domain_zone_name`*`|*} {interface `*`interface_name`*` | user-defined `*`ipv4_address`*` [interface {`*`interface_name`*` | auto}]}`	Sets a domain zone forwarder record that specifies a fully qualified domain name. You can also use a asterisk (*) if all domain zones are served by the specified DNS server(s). *domain_zone_name*: This is a domain zone, not a host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. So whenever the NXC receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address. *interface_name*: This is the interface through which the ISP provides a DNS server. The interface should be activated and set to be a DHCP client. auto: any interface that the NXC 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 zone-forwarder <1..4>`	Removes the specified zone forwarder record.

42.4.1 DNS Server Commands Example

This example configures the AP to connect to the AP controller (the NXC) by DNS. The following commands:

- Set the AP's management IP address to 192.168.1.100 and netmask 255.255.255.0
- Sets the AP's management interface to use VLAN ID 3
- Set the AP's default gateway IP address to 192.168.1.1
- Add a domain zone forwarder record that specifies a DNS server's IP address of 10.1.1.1 and uses the bridge 0 interface to send queries to that DNS server
- Set the AP controller's primary domain name as capwap-server.zyxel.com and secondary domain name as capwap.test.com

```
Router(config)# capwap ap vlan ip address 192.168.1.100 255.255.255.0
Router(config)# capwap ap vlan vlan-id 3
Router(config)# capwap ap vlan ip gateway 192.168.1.1
Router(config)# ip dns server zone-forwarder append * user-defined 10.1.1.1
interface br0
Router(config)# capwap ap ac-ip capwap-server.zyxel.com capwap.test.com
```

42.4.2 DNS Server Commands and DHCP

The AP in the example in Section 42.4.1 on page 255 uses a static IP address. If the AP uses DHCP instead, you do not need to configure the DNS server's IP address on the AP when you configure DHCP

option 6 on the DHCP server. For the example in Section 42.4.1 on page 255, you would just need to configure the management interface's VLAN ID (`capwap ap vlan vlan-id 3`).

List of Commands

This section lists the root commands in alphabetical order.