DSL & IAD CLI Reference Guide

DSL, IAD, and VoIP (ZyNOS) ZyXEL Devices

CLI Reference Guide

Version 3.70
11/2008
Edition 3

www.zyxel.com

About This CLI Reference Guide

Intended Audience

This manual is intended for people who want to configure the ZyXEL Device via the Command Line Interface (CLI). You should have at least a basic knowledge of TCP/IP networking concepts and topology.

This guide covers the following product lines:

- DSL modems and routers
- IAD (Integrated Access Devices) - the P-2600 series
- VoIP: ATA (Analog Terminal Adapters and Station Gateways) - the P-2300 series

The version number on the cover page refers to the latest firmware version supported by the products mentioned above. This guide applies to version 3.40 and 3.70 at the time of writing.

This guide is intended as a command reference for a series of products. Therefore many commands in this guide may not be available in your product. See your User's Guide for a list of supported features and details about feature implementation.

Please refer to www.zyxel.com or your product's CD for product specific User Guides and product certifications.

How To Use This Guide

- Read Chapter 1 on page 13 for an overview of various ways you can get to the CLI on your ZyXEL Device.
- Read Chapter 2 on page 17 for an introduction to some of the more commonly used commands.

It is highly recommended that you read at least these two chapters.

- The other chapters in this guide are arranged according to the CLI structure. Each chapter describes commands related to a feature.

See your ZyXEL Device's User Guide for feature background information.

- To find specific information in this guide, use the **Contents Overview**, the **Index of Commands**, or search the PDF file.

Documentation Feedback

Help us help you. Send all documentation-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

Warnings and notes are indicated as follows in this guide.

Warnings tell you about things that could harm you or your device. See your User's Guide for product specific warnings.

Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

This manual follows these general conventions:

- ZyXEL Devices may also be referred to as the "device", the "system" or the "product" in this guide.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.

Command descriptions follow these conventions:

- Commands are in `courier new font`.
- Required input values are in angle brackets <>; for example, `ping <ip-address>` means that you must specify an IP address for this command.
- Optional fields are in square brackets []; for instance `show logins [name]`, the name field is optional.

  The following is an example of a required field within an optional field: `snmp-server [contact <system contact>]`, the `contact` field is optional. However, if you use `contact`, then you must provide the *`system contact`* information.
- The | (bar) symbol means "or".
- *`italic`* terms represent user-defined input values; for example, in `sys datetime date [year month date]`, *`year month date`* can be replaced by the actual year month and date that you want to set, for example, 2007 08 15.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "Enter" or "Return" key on your keyboard.
- `<cr>` means press the [ENTER] key.
- An arrow (`-->`) indicates that this line is a continuation of the previous line.

Command summary tables are organized as follows:

Table 1 Table Title

COMMAND	DESCRIPTION
`ip arp status [`*`interface`*`]`	Displays an interface's ARP table.
`ip dhcp <`*`interface`*`> client release`	Releases the specified interface's DHCP IP address. The interface must be a DHCP client to use this command.
`ip dhcp <`*`interface`*`> client renew`	Renews the specified interface's DHCP IP address. The interface must be a DHCP client to use this command.

The **Table Title** identifies commands or the specific feature that the commands configure.

The **COMMAND** column shows the syntax of the command.

The **DESCRIPTION** column explains what the command does. It may also identify legal input values.

A long list of pre-defined values may be replaced by a command input value 'variable' so as to avoid a very long command in the description table. Refer to the command input values table if you are unsure of what to enter.

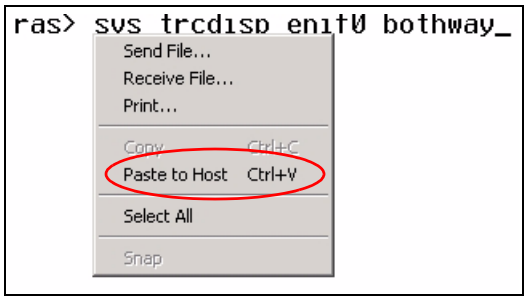
Table 2 Common Command Input Values

LABEL	DESCRIPTION
`description`	Used when a command has a description field in order to add more detail.
`ip-address`	An IP address in dotted decimal notation. For example, 192.168.1.3.
`mask`	The subnet mask in dotted decimal notation, for example, 255.255.255.0.
`mask-bits`	The number of bits in an address's subnet mask. For example type /24 for a subnet mask of 255.255.255.0.
`port`	A protocol's port number.
`interface`	An interface on the ZyXEL Device. enif refers to an Ethernet interface. `enif0`: LAN `enif1`: WLAN `enif2`: DMZ or WAN (Ethernet) (varies depending on your model) `wanif0`: WAN (PPPoE or PPPoA) For some commands you can also add a colon and a 0 or 1 to specify an IP alias. This is only for the LAN and DMZ interfaces. For example, `enif0:0` specifies LAN IP alias 1 and `enif0:1` specifies LAN IP alias 2.
`hostname`	Hostname can be an IP address or domain name.
`name`	Used for the name of a rule, policy, set, group and so on.
`number`	Used for a number, for example 10, that you have to input.

Commands are case sensitive! Enter commands exactly as seen in the command interface. Remember to also include underscores if required.

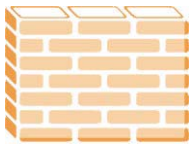
Copy and Paste Commands

You can copy and paste commands directly from this document into your terminal emulation console window (such as HyperTerminal). Use right-click (not CTRL-V) to paste your command into the console window as shown next.



Icons Used in Figures

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

ZyXEL Device 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 

Contents Overview

PART I
Introduction

1

How to Access and Use the CLI

This chapter introduces the command line interface (CLI).

1.1 Accessing the CLI

Use any of the following methods to access the CLI.

1.1.1 Console Port

You may use this method if your ZyXEL Device has a console port.

1. Connect your computer to the console port on the ZyXEL Device using the appropriate cable.
2. Use terminal emulation software with the following settings:

Table 3 Default Settings for the Console Port

SETTING	DEFAULT VALUE
Terminal Emulation	VT100
Baud Rate	9600 bps
Parity	None
Number of Data Bits	8
Number of Stop Bits	1
Flow Control	None

3. Press [ENTER] to open the login screen.

1.1.2 Telnet

4. Open a Telnet session to the ZyXEL Device's IP address. If this is your first login, use the default values.

Table 4 Default Management IP Address

SETTING	DEFAULT VALUE
IP Address	192.168.1.1
Subnet Mask	255.255.255.0

Make sure your computer IP address is in the same subnet, unless you are accessing the ZyXEL Device through one or more routers. In the latter case, make sure remote management of the ZyXEL Device is allowed via Telnet.

1.2 Logging in

Use the administrator password to log into the ZyXEL Device. The default value is ‘admin’ or ‘1234’ - see your ZyXEL Device User’s Guide to see which one to use. Some ZyXEL Devices may require you to also enter a user name. The default user name is ‘admin’.

The ZyXEL Device automatically logs you out of the management interface after five minutes of inactivity. If this happens to you, simply log back in again. Use the `sys stdio` command to extend the idle timeout. For example, the ZyXEL Device automatically logs you out of the management interface after 60 minutes of inactivity after you use the `sys stdio 60` command.

1.3 Using Shortcuts and Getting Help

This table identifies some shortcuts in the CLI, as well as how to get help.

Table 5 CLI Shortcuts and Help

COMMAND / KEY(S)	DESCRIPTION
↑↓ (up/down arrow keys)	Scrolls through the list of recently-used commands. You can edit any command or press [ENTER] to run it again.
[CTRL]+U	Clears the current command.
?	Displays the keywords and/or input values that are allowed in place of the ?.
help	Displays the (full) commands that are allowed in place of help.

Use the `help` command to view the available commands on the ZyXEL Device. Follow these steps to create a list of supported commands:

1. Log into the CLI.
2. Type `help` and press [ENTER]. A list comes up which shows all the commands available for this device.

```
ras> help
Valid commands are:
sys             exit            ether           wan
wlan            ip              ipsec           bridge
certificates    bm              lan             radius
8021x           voice
ras>
```

Abbreviations

Commands can be abbreviated to the smallest unique string that differentiates the command. For example `sys version` could be abbreviated to `s v`.

```
ras> sys version

 ZyNOS version: V3.40(ADV.3)b4 | 05/09/2007
 romRasSize: 3127550
 system up time:    24:23:59 (86087c ticks)
 bootbase version: V1.01 | 06/28/2005
ras> s v

 ZyNOS version: V3.40(ADV.3)b4 | 05/09/2007
 romRasSize: 3127550
 system up time:    24:24:15 (860eae ticks)
 bootbase version: V1.01 | 06/28/2005
ras>
```

1.4 Saving Your Configuration

In the ZyXEL Device some commands are saved as you run them and others require you to run a save command. For example, after configuring a static route rule, type `ip route addrom save` to save the static route rule in non-volatile memory. See the related section of this guide to see if a save command is required.

Unsaved configuration changes to commands that require you to run a save command are lost once you restart the ZyXEL Device

1.5 Logging Out

Enter `exit` to log out of the CLI.

Table 6 Exit Command

COMMAND	DESCRIPTION
`exit`	Logs you out of the CLI.

2

Common Commands

This chapter introduces some of the more commomly-used commands in the ZyXEL Device. For more detailed usage, see the corresponding feature chapter in this guide.

In the following examples, `ras` is the prompt as that is the default. If you configure a system name, then that prompt will display as the system name you configured. For example, change the system name to `zyxel` using the `sys hostname zyxel` command; the command prompt will then display as `zyxel>`.

2.1 Change the Idle Timeout

By default, the ZyXEL Device automatically logs you out of the management interface after five minutes of inactivity. Use the `sys stdio` command to extend the idle timeout. The following example extends the idle timeout to 120 minutes.

```
ras> sys stdio 120
Stdio Timeout = 120 minutes
ras>
```

2.2 Interface Information

ZyXEL Device interfaces are defined as shown in Table 2 on page 6.

The first command in this example shows information about a LAN port, for example, its IP address. The second command is used to change this IP address to 192.168.100.100.

```
ras> ip ifconfig enif0
enif0: mtu 1500
    inet 172.16.1.203, netmask 0xffff0000, broadcast 172.16.1.203
    RIP RX:None, TX:None,
    [InOctets      2742079] [InUnicast      624] [InMulticast       29689]
    [InDiscards        764] [InErrors         0] [InUnknownProtos     764]
    [OutOctets      414311] [OutUnicast     782] [OutMulticast       2225]
    [OutDiscards       2225] [OutErrors         0]
ras> ip ifconfig enif0 192.168.100.100
ras> ip ifconfig enif0
enif0: mtu 1500
    inet 192.168.100.100, netmask 0xffffff00, broadcast 192.168.100.255
    RIP RX:None, TX:None,
    [InOctets      3278515] [InUnicast      633] [InMulticast       34632]
    [InDiscards        926] [InErrors         0] [InUnknownProtos     926]
    [OutOctets      419351] [OutUnicast     782] [OutMulticast       2405]
    [OutDiscards       2405] [OutErrors         0]
```

Afterwards, you have to use this new IP address to access the ZyXEL Device via the LAN port.

To view information on all interfaces, enter `ip ifconfig`.

To view DHCP information on the LAN port, enter `ip dhcp enif0 status`.

```
ras> ip dhcp enif0 status
DHCP on iface enif0 is none
Status:
     Packet InCount: 477, OutCount: 0, DiscardCount: 477
ras>
```

Use these commands to release and renew DHCP-assigned information on the specified interface.

```
ras> ip dhcp enif0 client release
ras> ip dhcp enif0 client renew
ras>ras> ip ifconfig enif0
enif0: mtu 1500
    inet 172.16.17.203, netmask 0xffff0000, broadcast 172.23.255.255
    RIP RX:None, TX:None,
    [InOctets      3327150] [InUnicast      658] [InMulticast       34937]
    [InDiscards        943] [InErrors         0] [InUnknownProtos     943]
    [OutOctets      420007] [OutUnicast     782] [OutMulticast       2407]
    [OutDiscards       2405] [OutErrors         0]
ras>
```

To view the ARP table for the LAN port, enter `ip arp status enif0`.

```
ras> ip arp status enif0
received 23763 badtype 0 bogus addr 0 reqst in 3 replies 4 reqst out 34
cache hit 10529 (25%), cache miss 31410 (74%)
IP-addr         Type           Time  Addr              stat iface
172.16.17.18    10 Mb Ethernet 260   00:00:e8:7c:14:80 41   enif0
172.16.17.114   10 Mb Ethernet 210   00:10:b5:ae:56:9b 41   enif0
172.16.17.104   10 Mb Ethernet 150   00:c0:9f:cd:d4:bf 41   enif0
172.16.17.19    10 Mb Ethernet 130   00:02:e3:30:43:34 41   enif0
172.16.17.30    10 Mb Ethernet 220   00:60:b3:45:2b:c5 41   enif0
172.16.17.12    10 Mb Ethernet 80    00:c0:a8:fa:e9:27 41   enif0
172.16.17.24    10 Mb Ethernet 200   00:0e:7f:a6:a7:c1 41   enif0
172.16.17.34    10 Mb Ethernet 60    00:15:00:07:de:e1 41   enif0
172.16.17.32    10 Mb Ethernet 30    00:16:36:10:26:2d 41   enif0
172.16.17.41    10 Mb Ethernet 30    00:02:e3:57:ea:1c 41   enif0
172.16.17.44    10 Mb Ethernet 260   00:18:f8:04:f5:67 41   enif0
172.16.17.111   10 Mb Ethernet 230   00:19:cb:39:cb:ad 41   enif0
num of arp entries= 12
ras>
```

Each ZyXEL Device can support a specific number of NAT sessions in total. You can limit the number of NAT sessions allowed per host by using the `ip nat session` command. In the following example, each host may have up to 4000 NAT sessions open at one time. The total number of NAT sessions must not exceed the number for your ZyXEL Device.

```
ras> ip nat session 4000
     ip nat session
NAT session number per host: 4000
ras>
```

To see the IP routing table, enter the following command.

```
ras> ip route status
Dest            FF Len Device     Gateway         Metric stat Timer  Use
192.168.1.1     00 32  enet0      172.16.1.203     1    001f 0      0
192.168.2.36    00 32  enet0      172.16.1.203     1    001f 0      0
172.16.1.254   00 32  enet0      192.168.1.1      1    001f 0      0
172.16.1.30    00 32  enet0      192.168.1.1      1    001f 0      0
192.168.1.0     00 24  enet0      192.168.1.1       1    041b 0      0
172.23.0.0      00 16  enet0      172.16.1.203     1    041b 0      23
default         00 0   Idle       MyISP             2    002b 0      0
ras>
```

2.3 Basic System Information

Use the `sys atsh` command to view information about your ZyXEL Device.

```
ras> sys atsh
RAS version            : V3.40(ADV.3)b4 | 05/09/2007
RamSize                : 32768 Kbytes
Flash Type and Size    : Intel 32Mbits*1
romRasSize             : 3127550
bootbase version       : V1.01 | 06/28/2005
Product Model          : Prestige 2602HWNLI-D7A
MAC Address            : 001349214124
Default Country Code   : FF
Boot Module Debug Flag : 00
RomFile Version        : 14
RomFile Checksum       : b600
RAS F/W Checksum       : 4825
SNMP MIB level & OID   : 060102030405060708091011121314151617181920
Main Feature Bits      : C0
Other Feature Bits     :
9D 1A 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 03 41 13 00 00 00
ras>
```

Use the following command to view CPU utilization.

```
ras> sys cpu display
CPU usage status:
  baseline 882924 ticks
 sec  ticks  util    sec  ticks  util    sec  ticks  util    sec  ticks  util
  0  813191   7.89    1  807214   8.57    2  811101   8.13    3  811148   8.12
  4  813577   7.85    5  811697   8.06    6  812425   7.98    7  811474   8.09
  8  811686   8.06    9  809925   8.26   10  810349   8.21   11  811672   8.07
 12  812057   8.02   13  811810   8.05   14  813531   7.85   15  813221   7.89
 16  811394   8.10   17  812418   7.98   18  807217   8.57   19  808079   8.47
 20  804720   8.85   21  808472   8.43   22  810576   8.19   23  810342   8.22
 24  813690   7.84   25  810798   8.16   26  793435  10.13   27  781556  11.48
 28  800014   9.39   29  810944   8.15   30  811563   8.08   31  814575   7.74
 32  813225   7.89   33  812385   7.98   34  810931   8.15   35  811374   8.10
 36  812374   7.99   37  812445   7.98   38  782635  11.35   39  812026   8.02
 40  809550   8.31   41  809632   8.30   42  808723   8.40   43  811388   8.10
 44  812818   7.94   45  810337   8.22   46  811520   8.08   47  813600   7.85
 48  811545   8.08   49  812811   7.94   50  812414   7.98   51  812997   7.91
 52  813775   7.83   53  811116   8.13   54  812586   7.96   55  811772   8.05
 56  811885   8.04   57  810952   8.15   58  808698   8.40   59  811388   8.10
 60  813476   7.86   61  809569   8.30   62  809041   8.36
ras>
```

Use the following command to get the date and time from a time server on the Internet (or your network). You have to first configure a time server using the web configurator (or SMT menu if your ZyXEL Device has one).

```
ras> sys adjtime
Connecting to time server....
Current date is Sat 2007/09/01
Current time is 02:46:53
ras>
```

Use the following command to restart your ZyXEL Device right away.

```
ras> sys reboot
Bootbase Version: V1.01 | 06/28/2005 19:47:11
RAM: Size = 32768 Kbytes
FLASH: Intel 32M *1

ZyNOS Version: V3.40(ADV.3)b4 | 05/09/2007 14:00:00

Press any key to enter debug mode within 3 seconds.
Press any key to enter debug mode within 3 seconds.
.
```

Use the following command to reset the ZyXEL Device to the factory defaults. Make sure you back up your current configuration first (using the web configurator or SMT). The ZyXEL Device will restart and the console port speed will also reset to 9,600 bps.

```
ras> sys romreset

Do you want to restore default ROM file(y/n)?y
Default Romfile reset...

OKstore default Romfile.
System Restart(Console speed will be changed to 9600 bps)
.....................................................................
......
.............. done

VDSP921 init............ done
ISDN init.. done
Press ENTER to continue...
```

Use the following command to change the console port speed. A higher console port speed is recommended when uploading firmware via the console port. A console port speed of 115,200 bps is necessary to view CNM debug messages and packet traces on the ZyXEL Device.

```
ras> sys baud ?
Usage: baud <1..5>(1:38400, 2:19200, 3:9600, 4:57600, 5:115200)
ras> sys baud 5

Saving to ROM.  Please wait...
Change Console Speed to 115200. Then hit any key to continue
ras>
```

After you change the console port speed, you need to change it also on your terminal emulation software (such as HyperTerminal) in order to reconnect to the ZyXEL Device.

Logs are very useful for troubleshooting. If you are having problems with your ZyXEL Device, then customer support may request that you send them the logs. Use the following command to display all ZyXEL Device error logs

```
ras> sys logs errlog disp
  32 Sat Jan 01 00:00:06 2000 PP01  INFO  vc opened,vc=0,vpi=0,vci=0,qos=0
  33 Sat Jan 01 00:00:08 2000 PP0a -WARN  SNMP TRAP 3: link up
  34 Sat Jan 01 00:00:10 2000 PP15 -WARN  Last errorlog repeat 1 Times
  35 Sat Jan 01 00:00:10 2000 PP15  INFO  LAN promiscuous mode <0>
  36 Sat Jan 01 00:00:10 2000 PP15  INFO  LAN promiscuous mode <1>
  37 Sat Jan 01 00:00:10 2000 PP15  INFO  LAN promiscuous mode <0>
  38 Sat Jan 01 00:00:10 2000 PP15  INFO  LAN promiscuous mode <1>
  39 Sat Jan 01 00:00:10 2000 PP01 -WARN  SNMP TRAP 1: warm start
  40 Sat Jan 01 00:00:10 2000 PP01  INFO  main: init completed
  41 Sat Jan 01 00:00:10 2000 PP01  INFO  Starting Connectivity Monitor
  42 Sat Jan 01 00:00:11 2000 PP26  INFO  adjtime task pause 1 day
  43 Sat Jan 01 00:00:11 2000 PP28  INFO  monitoring WAN connectivity
  44 Sat Jan 01 00:00:44 2000 PP15  WARN  netMakeChannDial: err=-3001
rn_p=950cc
4d8
  45 Sat Jan 01 00:05:15 2000 PP01  WARN  Last errorlog repeat 20 Times
  46 Sat Jan 01 00:05:15 2000 PP01  INFO  SMT Session Begin
  47 Sat Jan 01 00:05:47 2000 PP15  WARN  netMakeChannDial: err=-3001
rn_p=950cc
4d8
  48 Sat Jan 01 00:10:42 2000 PP01  WARN  Last errorlog repeat 20 Times
  49 Sat Jan 01 00:10:42 2000 PP01 -WARN  SNMP TRAP 6: System reboot by user!
  50 Sat Jan 01 00:10:48 2000 PP01  INFO  vc opened,vc=0,vpi=0,vci=0,qos=0
  51 Sat Jan 01 00:10:50 2000 PP0a -WARN  SNMP TRAP 3: link up
  52 Sat Jan 01 00:10:52 2000 PP15 -WARN  Last errorlog repeat 1 Times
  53 Sat Jan 01 00:10:52 2000 PP15  INFO  LAN promiscuous mode <0>
  54 Sat Jan 01 00:10:52 2000 PP15  INFO  LAN promiscuous mode <1>
  55 Sat Jan 01 00:10:52 2000 PP15  INFO  LAN promiscuous mode <0>
  56 Sat Jan 01 00:10:52 2000 PP15  INFO  LAN promiscuous mode <1>
  57 Sat Jan 01 00:10:52 2000 PP01 -WARN  SNMP TRAP 1: warm start
  58 Sat Jan 01 00:10:52 2000 PP01  INFO  main: init completed
  59 Sat Jan 01 00:10:52 2000 PP01  INFO  Starting Connectivity Monitor
  60 Sat Jan 01 00:10:53 2000 PP26  INFO  adjtime task pause 1 day
  61 Sat Jan 01 00:10:53 2000 PP28  INFO  monitoring WAN connectivity
  62 Sat Jan 01 00:11:30 2000 PP01  INFO  SMT Session Begin
  63 Sat Jan 01 00:12:01 2000 PP15  WARN  netMakeChannDial: err=-3001
rn_p=950cc
4d8
Clear Error Log (y/n):
```

Use the following commands for system debugging. A console port speed of 115,200 bps is necessary to view packet traces on the ZyXEL Device.

```
ras> sys trcpacket sw on
ras> sys trcdisp brief
   0 02:13:43.650 ENET1-R[0092] UDP 192.168.1.33:137->192.168.1.255:137
   1 02:13:43.650 ENET1-R[0092] UDP 192.168.1.33:137->192.168.1.255:137
   2 02:13:44.010 ENET1-T[0060] ARP Request 192.168.1.1->192.168.1.200
   3 02:13:44.390 ENET1-R[0092] UDP 192.168.1.33:137->192.168.1.255:137
   4 02:13:44.390 ENET1-R[0092] UDP 192.168.1.33:137->192.168.1.255:137
   5 02:13:45.140 ENET1-R[0092] UDP 192.168.1.33:137->192.168.1.255:137
   6 02:13:45.140 ENET1-R[0092] UDP 192.168.1.33:137->192.168.1.255:137
ras>
ras> sys trcdisp enif0 bothway

TIME:02:17:08.780  enet1-XMIT len:1192 call=0
  0000: ff ff ff ff ff ff 00 18 f8 04 f5 67 88 a2 10 00
  0010: ff ff ff 01 00 00 00 00 00 00 00 00 00 00 00 00
  0020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0030: 00 00 00 00 00 00 00 00 00 00 00 00
ras>
```

Use the ping command to have the ZyXEL Device ping an IP address as shown in the following example.

```
ras> ip ping 172.16.17.12
Resolving 172.16.17.12... 172.16.17.12
      sent      rcvd  rate    rtt     avg    mdev     max     min
         1         1  100      10      10       0      10      10
         2         2  100       0       9       3      10       0
         3         3  100       0       8       5      10       0
ras>
```

2.4 UTM and myZyXEL.com

Use these commands to create an account at myZyXEL.com and view what services you have activated.

Ensure your ZyXEL Device is connected to the Internet before you use the following commands.

You need to create an account at my ZyXEL.com in order to activate content filtering, anti-spam and anti-virus UTM (Unified Threat Management) services. See the myZyXEL.com chapter for information on the country code you should use.

```
ras> sys myZyxelCom register <username> <password> <email> <countryCode>
```

This command displays your ZyXEL Device's registration information.

```
ras> sys myZyxelCom display

register server address : www.myzyxel.com
register server path : /register/registration?

username : aseawfasf
password : aaaaaa

email : aa@aa.aa.aa

sku : CFRT=1&CFST=319&ZASS=469&ISUS=469&ZAVS=469

country code : 204

register state 1

register MAC : 0000AA220765
CF expired day : 2008-05-26 14:58:19
Last update day : 2007-07-12 14:58:19
```

This command displays ZyXEL Device service registration details.

```
ras> sys myZyxelCom serviceDisplay
Content Filter Service :
Actived, Licenced, Trial, Expired : 2007-07-08 16:36:15
ras>
```

Use the following commands to enable anti-virus on the ZyXEL Device You first need to use the load command.

```
ras> av load
ras> av config enable on
ras> av save
ras> av disp
 AV Enable : On
 AV Forward Over ZIP Session : Off
 AV Forward Over ZIP Session : Off
-----------------------------------
```

Use the following commands to enable content filtering on the ZyXEL Device, then on the external database (DB) and then display the default policy.

```
ras> ip cf common enable on
ras> ip cf externalDB enable on
ras> ip cf policy displayAll
   index  Name           Active    IP Group
                                   Start Addr End Addr
==========================================================================

    1  Default Policy       Y       0.0.0.0/0.0.0.0
```

The default policy does not actually block anything. Use the following commands to edit the default policy, turn the external database service content filtering (category-based content filtering), see what the categories are, block a category 92 in the following example) and then save the policy.

```
ras> ip cf policy edit 1
ras> ip cf policy config webControl enable on
ras> ip cf policy config webControl display
The Categories:
type 1        :Adult/Mature Content
type 2        :Pornography
type 3        :Sex Education
type 4        :Intimate Apparel/Swimsuit
type 5        :Nudity
type 6        :Alcohol/Tobacco
type 7        :Illegal/Questionable
type 8        :Gambling
type 9        :Violence/Hate/Racism
type10        :Weapons
type11        :Abortion
type12        :Hacking
type13        :Phishing
type14        :Arts/Entertainment
type15        :Business/Economy
type16        :Alternative Spirituality/Occult
type17        :Illegal Drugs
type18        :Education
type19        :Cultural/Charitable Organization
type20        :Financial Services
type21        :Brokerage/Trading
type22        :Online Games
type23        :Government/Legal
type24        :Military
type25        :Political/Activist Groups
type26        :Health
type27        :Computers/Internet
type28        :Search Engines/Portals
type29        :Spyware/Malware Sources
type30        :Spyware Effects/Privacy Concerns
type31        :Job Search/Careers
type32        :News/Media
type33        :Personals/Dating
type34        :Reference
type35        :Open Image/Media Search
type36        :Chat/Instant Messaging
type37        :Email
type38        :Blogs/Newsgroups
type39        :Religion
type40        :Social Networking
type41        :Online Storage
type42        :Remote Access Tools
type43        :Shopping
type44        :Auctions
type45        :Real Estate
type46        :Society/Lifestyle
type47        :Sexuality/Alternative Lifestyles
type48        :Restaurants/Dining/Food
type49        :Sports/Recreation/Hobbies
type50        :Travel
type51        :Vehicles
type52        :Humor/Jokes
type53        :Software Downloads
type54        :Pay to Surf
type55        :Peer-to-Peer
type56        :Streaming Media/MP3s
type57        :Proxy Avoidance
type58        :For Kids
type59        :Web Advertisements
type60        :Web Hosting
type61        :Unrated
ras> ip cf policy config webControl category block 2
The Categories:
type 1        :Adult/Mature Content
type 2 (block):Pornography
-------
ras> ip cf policy save
ras>
```

You may also configure and schedule new policies using commands as well as configure what to block using the external database.

2.5 Firewall

Use the following command to enable the firewall on the ZyXEL Device.

```
ras> sys firewall active yes
ras>
```

2.6 VPN

Use the following command to show what IPsec VPN tunnels are active on your ZyXEL Device.

```
ras> ipsec show_runtime sa
Runtime SA status:

No phase 1 IKE SA exist
No phase 2 IPSec SA exist
Active SA pair = 0

ras>
```

Use the following command to manually bring up a previously configured VPN tunnel.

```
ras> ipsec dial 1
Start dialing for tunnel <rule# 1>...
.....................
```

2.7 Dialing PPPoE and PPTP Connections

This example shows dialing up remote node “WAN 1” using PPPoE..

```
ras> poe dial "WAN 1"
Start dialing for node <WAN 1>...
### Hit any key to continue.###
$$$ DIALING dev=6 ch=0..........
$$$ OUTGOING-CALL phone()
$$$ CALL CONNECT speed<100000000> type<6> chan<0>
$$$ LCP opened
$$$ PAP sending user/pswd
$$$ IPCP negotiation started
$$$ IPCP neg' Primary DNS 192.168.30.1
$$$ IPCP neg' Primary DNS 172.16.5.2
$$$ IPCP opened
```

This example shows dialing up remote node “WAN 1” using PPTP.

```
ras> pptp dial "WAN 1"
Start dialing for node <WAN 1>...
### Hit any key to continue.###


ras>
```

PART II
Reference

3

IEEE 802.1Q/1P Commands

Use these commands to configure IEEE 802.1Q VLAN groups and IEEE 802.1P priority levels for the ports on the ZyXEL Device.

3.1 Command Summary

The following section lists the commands for this feature.

Table 7 8021Q Command Summary

COMMAND	DESCRIPTION
`802.1Q load`	Loads the IEEE 802.1Q settings for configuration.
`802.1Q disp`	Shows the current IEEE 802.1Q settings.
`802.1Q clear`	Resets the IEEE 802.1Q settings to the factory defaults.
`802.1Q active <1:active|0:inactive>`	Enables or disables the IEEE 802.1Q feature on the ZyXEL Device.
`802.1Q mgtvid <1~4094>`	Sets the ID number of the management VLAN group.
`802.1Q setpvid <LAN|PVC|WLAN> <index> <1~4094>`	Sets the port VLAN ID of the specified interface on the ZyXEL Device.
`802.1Q set1p <LAN|PVC|WLAN> <index> <0~7>`	Sets the IEEE 802.1P priority level of the specified interface on the ZyXEL Device.
`802.1Q groupset <groupid> <vid> <LAN <index>|<PVC|WLAN> <index>> <u|t>`	Sets a VLAN group. `u|t`: Sets the interface to tag or untag all outgoing traffic transmitted through this VLAN.
`802.1Q setlanAttri LAN <index> <t|u>`	Sets an Ethernet port to tag or untag all outgoing traffic transmitted.
`802.1Q igmpsnp enable`	Enables IGMP snooping.
`802.1Q igmpsnp disable`	Disables IGMP snooping.
`802.1Q igmpsnp maxresptime <0~255>`	Sets the maximum response time that can elapse before the ZyXEL Device removes an IGMP group membership entry.
`802.1Q igmpsnp queryinterval <0~255>`	Sets the IGMP snooping query interval (in seconds) at which the ZyXEL Device sends host-query messages.
`802.1Q igmpsnp robust <0~255>`	Sets the IGMP robust value.
`802.1Q igmpsnp disp`	Displays the IGMP table on the ZyXEL Device.
`802.1Q save`	Saves the IEEE 802.1Q settings.

3.2 Command Examples

This example loads the IEEE 802.1Q settings and enables the IEEE 802.1Q feature on the ZyXEL Device.

```
ras> 8021Q load
ras> 8021Q active 1
set 802.1Q active
ras>
```

This example sets the port VLAN ID of Ethernet LAN port 4 to 123.

```
ras> 8021Q setpvid LAN 4 123
ras>
```

This example adds Ethernet LAN port 2 and WLAN 2 to VLAN group 2. The VLAN ID of this group is “111”. This example also displays and saves the current IEEE 802.1Q settings.

```
ras> 8021Q groupset 2 111 LAN 2 WLAN 2 u
ras> 8021Q disp

802.1Q is: Enabled
Management VID: 1
-------------------------------------------------------
PVID:
LAN1: 2  LAN2: 2  LAN3: 3  LAN4:123  SSID1: 4 SSID2: 4 SSID3: 4 SSID4: 4
PVC1: 1  PVC2: 1  PVC3: 1  PVC4: 1  PVC5: 1  PVC6: 1  PVC7: 1  PVC8: 1
Priority:
LAN1: 7  LAN2: 7  LAN3: 2  LAN4: 2  SSID1: 5 SSID2: 5 SSID3: 5 SSID4: 5
PVC1:-1  PVC2:-1  PVC3:-1  PVC4:-1  PVC5:-1  PVC6:-1  PVC7:-1  PVC8:-1
=======================================================
VLAN Group Setting: (u-untagged  t-tagged)
Group 1   VID: 1    LAN:  1 u   2 u   3 u   4 u
                    WLAN:  1 u   2 u   3 u   4 u
                    PVC:  1 u   2 u   3 u   4 u   5 u   6 u   7 u   8 u
Group 2   VID: 111  LAN:  2 u
                    WLAN:  2 u
                    PVC:
Group 3   VID: 3    LAN:  3 u   4 u
                    WLAN:
                    PVC:  2 u
Group 4   VID: 4    LAN:
                    WLAN:  1 u   2 u
                    PVC:  3 u
ras> 8021Q save
ras>
```

4

IEEE 802.1x Commands

Use these commans to configure IEEE 802.1x authentication on the ZyXEL Device.

4.1 Command Summary

The following section lists the commands for this feature.

Table 8 8021x Command Summary

COMMAND	DESCRIPTION
`8021x debug level <debug-level> [filter <mac-address>]`	Sets the IEEE 802.1x debug message level. Optionally, specifies the MAC address of the debug target. *debug-level*: the following are the debug levels available, type the number in parenthesis () to activate the debug level. • debug packet (1) • debug state machine (2) • debug timer (4) • debug supplicant (8) • debug error (16) • debug backend server (32) • debug function (64) • debug vlantag (128) type 0 to turn all debugging off.
`8021x debug trace`	Displays all supplicants (users and/or clients which are going to be authenticated) in the supplicants table.
`8021x debug user <username>`	Displays the specified user status in the supplicant table.
`8021x show showkey`	Displays details about the authentication key used for IEEE 802.1x authentication.
`8021x set mode <WPA_PSK|others>`	Sets the IEEE 802.1x security mode. Note: At the time of writing only WPA-PSK can be selected.
`8021x set key <key>`	Sets the IEEE 802.1x key. The key must consist of ASCII characters including spaces and symbols and must be between 8-63 characters long.
`8021x set save`	Saves the IEEE 802.1x configuration settings.

4.2 Command Examples

This example activates WPA-PSK mode for IEEE 802.1x authentication and specifies the authentication key (shared secret) to be **abSecret123**.

```
ras> 8021x set mode WPA_PSK
ras> 8021x set key abSecret123
ras> 8021x set save
```

5

Dial Backup Commands

Use these commands to configure dial backup port settings on the ZyXEL Device.

At the time of writing, only P-662 series has the commands described in this chapter.

5.1 Command Summary

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

Table 9 AUX Command Input Values

LABEL	DESCRIPTION
aux-port	This identifies the channel for dial backup. *aux0*: This is the dial backup port.

The following section lists the aux commands.

Table 10 AUX Commands

COMMAND	DESCRIPTION
aux atring <*aux-port*>	Shows the AT command binary strings that the ZyXEL Device sent to the connected modem and the responses.
aux clearstat <*aux-port*>	Resets channel statistics.
aux cnt disp <*aux-port*>	Displays the auxiliary port's counter information.
aux cnt clear <*aux-port*>	Clears the auxiliary port's counter information.
aux drop <*aux-port*>	Disconnects the auxiliary port's connection.
aux init <*aux-port*>	Initializes the the auxiliary port's connection.
aux mstatus <*aux-port*>	Displays the status of the modem's last call.
aux mtype <*aux-port*>	Displays the type of modem connected to the auxiliary port.
aux netstat <*aux-port*>	Displays upper layer packet information and the corresponding transmit and receive counts.
aux rate <*aux-port*>	Displays the transmit and receive rates.
aux signal <*aux-port*>	Displays the auxiliary port's signal.

5.2 Command Examples

This example displays the historical AT commands the ZyWALL sent to the modem connected to the dial backup port and the responses.

```
ras> aux atring aux0
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

94b13960: 02 0d 0c 00 be af 00 00 00 00 08 00 61 74 68 0d     ............ath.
94b13970: 0d 0a 4f 4b 0d 0a 61 74 26 66 73 30 3d 30 0d 0d     ..OK..at&fs0=0..
94b13980: 0a 4f 4b 0d 0a 61 74 64 30 2c 34 30 35 30 38 38     .OK..atd0,405088
94b13990: 38 38 0d 0d 0a 42 55 53 59 0d 0a 61 74 64 30 2c     88...BUSY..atd0,
94b139a0: 34 30 35 30 38 38 38 38 0d 0d 0a 52 49 4e 47 49     40508888...RINGI
94b139b0: 4e 47 0d 0a 0d 0a 42 55 53 59 0d 0a 61 74 64 30     NG....BUSY..atd0
94b139c0: 2c 34 30 35 30 38 38 38 38 0d 0d 0a 43 4f 4e 4e     ,40508888...CONN
94b139d0: 45 43 54 20 31 31 35 32 30 30 2f 56 2e 33 34 20      ECT 115200/V.34
94b139e0: 31 36 38 30 30 2f 56 34 32 62 0d 0d 0a 4e 4f 20      16800/V42b...NO
94b139f0: 43 41 52 52 49 45 52 0d 0a 61 74 68 0d 0d 0a 4f     CARRIER..ath...O
94b13a00: 4b 0d 61 74 68 0d 0d 0a 4f 4b 0d 0a 61 74 26 66     K.ath...OK..at&f
94b13a10: 73 30 3d 30 0d 0d 0a 4f 4b 0d 0a 61 74 64 30 2c     s0=0...OK..atd0,
94b13a20: 34 30 35 30 38 38 38 38 0d 0d 0a 43 4f 4e 4e 45     40508888...CONNE
94b13a30: 43 54 20 31 31 35 32 30 30 2f 56 2e 33 34 20 31     CT 115200/V.34 1
94b13a40: 34 34 30 30 2f 56 34 32 62 0d 0d 0a 4e 4f 20 43     4400/V42b...NO C
94b13a50: 41 52 52 49 45 52 0d 0a 61 74 68 0d 0d 0a 4f 4b     ARRIER..ath...OK
94b13a60: 0d 61 74 68 0d 0d 0a 4f 4b 0d 0a 61 74 26 66 73     .ath...OK..at&fs
94b13a70: 30 3d 30 0d 0d 0a 4f 4b 0d 0a 61 74 64 30 2c 34     0=0...OK..atd0,4
94b13a80: 30 35 30 38 38 38 38 0d 0d 0a 43 4f 4e 4e 45 43     0508888...CONNEC
94b13a90: 54 20 31 31 35 32 30 30 2f 56 2e 33 34 20 20 39     T 115200/V.34  9
94b13aa0: 36 30 30 2f 56 34 32 62 0d 00 00 00 00 00 00 00     600/V42b........
```

This example displays upper layer packet information for the dial backup port.

```
ras> aux netstat aux0
Name   :       aux0, Dev type  :    3, Chann id:    0

RX(pkt):         73, RX discard:    0, RX error:    0, RX(octet):       7764
TX(pkt):         89, TX discard:    0, TX error:    0, TX(octet):       6801
```

The following table describes the labels in this display.

Table 11 aux netstat aux0

LABEL	DESCRIPTION
Name	Name of the channel.
Dev type	The type of auxillary device, there are several possibilities: 0: NONE 1: 56k modem 2: modems other than 56k 3: TA 4: X25_PAD 5: MultiProtocol over AAL5 6: PPP over Ethernet, RFC-2516 7: PPTP
Chann id	The number of the channel that the device is using.
RX (pkt)	Received packets.
TX (pkt)	Transmitted packets.
RX discard	Received octets the ZyXEL Device discarded.
TX discard	Transmitted octets the ZyXEL Device discarded.
RX error	Received errored frames.
TX error	Transmitted errored frames.
RX(octet)	Received errored octects.
TX(octet)	Transmitted errored octets.

This example displays the dial backup port's transmit and receive rates.

```
ras> aux rate aux0
 No. TX(byte) Rx(byte)  TX Rate   RX Rate   TX Queue
==== ======== ======== ========= ========= ==========
   1        0        0         0         0          0
   2        0       15         0         5          0
   3       14       14         4         4          0
   4        0       15         0         5          0
   5       14       14         4         4          0
   6        0       15         0         5          0
   7       14       14         4         4          0
   8        0        0         0         0          0
   9       14       29         4         9          0
  10        0        0         0         0          0
  11       14       29         4         9          0
  12        0        0         0         0          0
  13       14       29         4         9          0
  14        3       14         1         4          0
  15        4       10         1         3          0
  16        0        0         0         0          0
  17       27       39         9        13          0
  18       14       29         4         9          0
  19        0        0         0         0          0
  20       14       29         4         9          0
```

The following table describes the labels in this display.

Table 12 aux rate aux0

LABEL	DESCRIPTION
No.	The entry in the rate statistics.
TX (byte)	Transmitted bypts.
Rx (byte)	Received bytes.
TX Rate	Transmission rate.
RX Rate	Reiceived rate
TX Queue	Number of packets waiting to be transmitte.

This example displays details about the dial backup port's signal.

```
ras> aux signal aux0

 DTR: ON  DSR: ON  RTS: ON  CTS: ON  DCD: OFF
```

The following table describes the labels in this display.

Table 13 aux rate aux0

LABEL	DESCRIPTION
DTR	Data Terminal Ready: The signal the ZyXEL Device sends to the modem to indicate the ZyXEL Device is ready to receive data.
DSR	Data Set Ready: The signal the modem sends to the ZyXEL Device to indicate the modem is ready to receive data.
RTS	Request to Send: The signal the ZyXEL Device sends to the modem to have the modem prepare to receive data.
CTS	Clear to Send: The signal the modem sends to the ZyXEL Device to acknowledge the ZyXEL Device and allow the ZyXEL Device to transmit data.
DCD	Data Carrier Detect: The signal the modem sends to the ZyXEL Device when the modem has a connection with the remote device.

6

Bandwidth Management

Use these commands to configure bandwidth management (BWM) settings on the ZyXEL Device.

6.1 Command Summary

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

Table 14 Bandwidth Management Command Input Values

LABEL	DESCRIPTION
interface	The bandwidth management interface name includes `lan`, `wan`, `dmz`, and `wlan`. The interfaces to which you can apply bandwidth management vary by ZyXEL Device model.
class-name	This is a class name. Enter a descriptive name of up to 20 alphanumeric characters, including spaces.
class-number	This is a class number. Each class for each interface has an unique number. The number format is "xx.xx.xx.xx ... xx" and the range of xx is from 01 to 98. Each ".xx" is a subclass. And the length of "xx.xx.xx.xx ..." is the depth of this class. Different model supports different class depth.

The following section lists the commands for this feature.

Table 15 Bandwidth Management Commands

COMMAND	DESCRIPTION
`bm class <`*interface*`> <add|mod> <`*class-number*`> <bandwidth <`*bandwidth*`>> [name <`*class-name*`>] [priority <`*priority*`>] [borrow <on|off>]`	Adds or modifies a class for the specified interface with the specified bandwidth. You can also configure the name, priority, and whether or not the class can borrow bandwidth from its parent class. `add|mod`: Add or modifies the class. When you delete a class, it also deletes its sub-classes. *bandwidth*: The unit is bps and its minimum is 30 Kbps. You can add "K" (or "k") to specify Kbps or "M" (or "m") to specify Mbps. If you do not specify the bandwidth, the default value is 100 Mbps. *class-name*: Specify a descriptive name of up to 19 alphanumeric characters. *priority*: Sets the class priority ranging from 0 (the lowest) to 7 (the highest). `borrow <on|off>`: Enables or disables bandwidth borrowing.
`bm class <`*interface*`> del <`*class-number*`>`	Removes the specified class from the specified interface. When you delete a class, it also deletes its sub-classes.
`bm config [load|save|clear]`	Loads, saves, clears BWM configuration from/to the permanent memory.

Table 15 Bandwidth Management Commands (continued)

COMMAND	DESCRIPTION
bm debug [config|config_action|flow|classifier|statistics|web]	Turns the bandwidth management debug features on or off. config: Displays debug messages when entering bm commands. config_action: Displays special configuration messages, such as dynamic filters. flow: Displays the BWM function flow. classifier: Displays the classification matching results, including filter and packet content. statistics: Displays the data transferred through BWM. web: Displays debug message when configuring BWM through the web configurator.
bm defaultClassBw <*bandwidth*>	Sets the default class bandwidth in the Media Bandwidth Management wizard. *bandwidth*: The unit is kbps and the range is 0~65535.
bm filter <*interface*> <disable|enable> <*class-number*>	Disables or enables a filter for class # in the specified interface.
bm filter <*interface*> add <*class-number*> [service <ftp|sip|h323>] <*dest-ip-address*> [mask *dest-mask*] <*dest-port*> <*src-ip-address*> [mask *src-mask*] <*src-port*> <*protocol*>	Adds a filter for class # in the specified interface. The filter contains destination address (netmask), destination port, source address (netmask), source port and protocol. Use 0 for items that you do not want the filter to include. *protocol*: Enter the number of the protocol type (the protocol field in the IP header). For example 1 for ICMP, 6 for TCP, and 17 for UDP.
bm filter <*interface*> del <*class-number*>	Deletes a filter for class # in the specified interface.
bm interface <*interface*> <enable|disable> [auto <on|off>] [bandwidth <*bandwidth*>] [prr|wrr] [efficient]	Enables or disables BWM for traffic going out of the specified interface. auto <on|off>: Enables or disables automatic classification of traffic types. *bandwidth*: The unit is bps and its minimum is 30 Kbps. You can add "K" (or "k") to specify Kbps or "M" (or "m") to specify Mbps. If you do not specify the bandwidth, the default value is 100 Mbps. prr|wrr: Sets the queuing mechanism to fairness-based (WRR) or priority-based (PRR). efficient: Enables or disables maximum bandwidth usage.
bm monitor <*interface*> [*class-number*]	Displays the bandwidth usage of the specified interface or its class. The first time you use the command turns it on; the second time turns it off, and so on.
bm moveFilter <*interface*> <*from-class-number*> <*to-class-number*>	Changes the BWM filter order.
bm show <class|filter|statistics> <*interface*> [*class-number*]	Displays bandwidth management class settings, filter settings, or statistics for the specified interface. You can also specify the class.
bm show interface <*interface*>	Displays the general bandwidth management settings for the specified interface.
bm threshold <high|low> [*threshold*]	Configures the Automatic Traffic Classifier (ATC) high and low packet size thresholds (in bytes). Packets smaller than the high priority threshold get high priority. Packets larger than the low priority threshold get low priority. The rest get medium priority.

6.2 Command Examples

This example configures BWM at the interface level. It does the following.

1. Turns on BWM on the WLAN interface.
2. Enables automatic traffic classification.
3. Sets the interface's bandwidth limit to 25 Mbps.
4. Enables maximum bandwidth usage.
5. Sets the queuing mechanism to fairness-based (WRR).
6. Displays the WLAN interface's BWM settings.

```
ras> bm interface wlan enable auto on bandwidth 25m wrr efficient
BM Interface setting done.
ras> bm show interface wlan
================================================================================
Interface : wlan               Automatic Traffic Classify: Enable
                        [ Fairness-Based : Maximize BW Usage ]

        bandwidth =     25M (bps)
        allocated bandwidth =      0 (bps)
        MTU = 1500 (byte)
================================================================================
```

This example adds one WLAN class using the following settings (and then displays it).

- Class number: 1
- Class name: WLAN-class1
- Bandwidth: 5 Mbps
- Priority: 7
- Bandwidth borrowing: Enabled

```
ras> bm class wlan add 1 name WLAN-class1 bandwidth 5m priority 7 borrow on
Class setting is done.
ras> bm show class wlan 1
================================================================================
Class: 1        Name: WLAN-class1
        depth: 1        priority: 7     filter setting: No
        queue: 0/30
        borrow class: 0
        parent class: 0 (Root Class)

        total bandwidth:          5M (bps)
        allocated bandwidth:      0 (bps)
================================================================================
```

This example adds a filter on the WLAN class using the following settings.

- Class number: 1
- Service: FTP
- Destination address: 172.16.1.208

- Source port: Any
- Source address: Any
- Destination address: Any
- Destination port: Any
- Protocol: Any.

```
ras> bm filter wlan add 1 service ftp 172.16.1.208 0 0 0 0 0
Filter setting is done.
ras> bm show filter wlan 1
================================================================================
  Class 1       Class Note:             WLAN-class1
                Filter Enabled:         Yes
                Destination(A : P):    (172.16.1.208 : 0)
                Destination Netmask:    255.255.255.255
                Source(A : P):         (0.0.0.0 : 0)
                Source Netmask:         0.0.0.0
                Protocol:               0
                Special for Service:    FTP
================================================================================
```

This example monitors the runtime situation for all WAN classes.

Each interface has one root class (0) and one default class (99). In this example, you can see only one user-defined class (1). The root class (0) displays total traffic amount for the WLAN interface. You can see the current bandwidth usage matching the class 1 rule is 0 b. The default class (99) includes the bandwidth usage for traffic that doesn't match any user-defined class rules. 97 and 98 are classes for automatically classified traffic.

```
ras> bm monitor wlan
ras>
wlan -  0:     14Kb     1:      0b      97:      6Kb    98:      8Kb
        99:      0b
wlan -  0:      3Kb     1:      0b      97:      3Kb    98:      0b
        99:    448b
wlan -  0:      3Kb     1:      0b      97:      3Kb    98:      0b
        99:      0b
wlan -  0:      2Kb     1:      0b      97:      2Kb    98:      0b
        99:    448bbm monitor wlan
ras>
```

7

Bridge Commands

Use these commands to configure bridge settings on your device.

7.1 Command Summary

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

Table 16 Bridge Command Input Values

LABEL	DESCRIPTION
entry#	This identifies a bridge route (1-4).
bridge_group#	This identifies a bridge group number (1~31).

The following section lists the `bridge` commands..

Table 17 Bridge Commands

COMMAND	DESCRIPTION
`bridge cnt clear <entry#>`	Resets the packet statistics counter for the specified bridge.
`bridge cnt disp <entry#>`	Displays the packet statistics table for the specified bridge.
`bridge stat active <on|off>`	Enables or disables the bridge specified with the `index` command. More than one bridge can be active.
`bridge stat clear`	Resets the bridge statistics counter.
`bridge stat display`	Displays statistics on a specified bridge route. If `"please use index first: ip route addrom index [index#]"` appears, use the `index` command in this table to specify a bridge.
`bridge stat freememory`	Frees the current working buffer. After using this command you can then select a bridge route to display or edit.
`bridge stat index <entry#>`	Specifies a bridge route (1-4) to display or edit. Use `freememory` before specifying a bridge route different from the current one.
`bridge stat name <string>`	Sets a name for the bridge specified with the `index` command (10 characters).

Table 17 Bridge Commands (continued)

COMMAND	DESCRIPTION
`bridge stat set [mac-address][gateway-ip] [gateway-node]`	Sets a route for the the bridge specified with the `index` command. [*mac-address*]: The MAC address of the final destination. [*gateway-ip*]: The IP address of the gateway. The gateway is both an immediate neighbor of your ZyXEL device and also forwards the packet to its destination. • On the LAN, the gateway must be a router on the same segment as your ZyXEL device. • On the WAN, the gateway must be the IP address of one of the remote nodes. [*gateway-node*]: The index number of the gateway for this static route. Use `wan node` commands to find the index number of a node.
`bridge stat save`	Saves the changes to the bridge's configuration.

7.2 Command Examples

This example shows how to set up a bridge and save it.

1. First, use `freememory` to clear the working buffer.
2. Then specify which bridge to configure by selecting its index.
3. Set the name of the bridge.
4. Set the MAC address, IP address and number of the node.
5. Activate the bridge.
6. Display the new bridge configuration for checking.
7. Save your changes.

```
ras> bridge stat freememory
ras> bridge stat index 1
ras> bridge stat name MyISP
Bridge StaticRoute Name= MyISP
ras> bridge stat set 00:13:49:34:56:78 172.23.34.202 1
ras> bridge stat active on
ras> bridge stat display
 Route:#1
 Route name = MyISP
active = on
Ether Address = 00:13:49:34:56:78
IP address = 172.23.34.202
Gateway node = 1
ras> bridge stat save
ip policyrouting set configurations save ok
```

The following table describes the fields displayed using the `display` command in the example above.

Table 18 bridge stat display

LABEL	DESCRIPTION
Route	The index number of the static route.
Route name	A descriptive name for the bridge route. Use a string of up to 10 ASCII characters.

Table 18 bridge stat display

LABEL	DESCRIPTION
active	This shows whether the bridge is active or not. It is either on or off. More than one bridge may be active at one time.
Ether Address	This refers to the MAC address of the final destination of the bridge static route.
IP address	This is the IP address of the gateway. See the `bridge stat set command` description for an explanation of gateways.
Gateway node	The index number of the remote node. The remote node is the end point of a bridge, for example, your ISP. Use `wan node` commands to find a list of available bridges.

8

Certificate Commands

Use these commands to configure certificates.

8.1 Command Summary

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

Table 19 `certificates` Command Input Values

LABEL	DESCRIPTION
<addr[:port]>	Specifies the server address (required) and port (optional). The format is "*server-address[:port]*".
auth-key	Specifies the certificate's key for user authentication. If the key contains spaces, put it in quotes. To leave it blank, type "".
ca-addr	The IP address or domain name of the CA (Certification Authority) server.
ca-cert	The name of the CA certificate.
key-length	The length of the key to use in creating a certificate or certificate request. Valid options are 512, 768, 1024, 1536 and 2048 bits.
[*login:password*]	The login name and password for the directory server, if required. The format is "*login:password*".
name, old-name, new-name	The identifying name of a certificate or certification request. Use up to 31 characters to identify a certificate. You may use any character (not including spaces). <*old-name*> specifies the name of the certificate to be renamed. <*new-name*> specifies the new name for the certificate.
server-name	A descriptive name for a directory server. Use up to 31 ASCII characters (spaces are not permitted).
subject	A certificate's subject name and alternative name. Both are required. The format is "subject-name-dn;{ip,dns,email}=value". Example 1: "CN=ZyWALL,OU=CPE SW2,O=ZyXEL,C=TW;ip=172.21.177.79" Example 2: "CN=ZyWALL,O=ZyXEL,C=TW;dns=www.zyxel.com" Example 3: "CN=ZyWALL,O=ZyXEL,C=TW;email=dummy@zyxel.com.tw" If the name contains spaces, put it in quotes.
timeout	The verification timeout value in seconds (optional).

The following section lists the `certificates` commands.

Table 20 certificates Commands

COMMAND	DESCRIPTION
certificates ca_trusted crl_issuer <*name*> [on|off]	[on|off] specifies whether or not the specified CA issues CRL. If [on|off] is not specified, the current crl_issuer status of the CA displays.
certificates ca_trusted delete <*name*>	Removes the specified trusted CA certificate.
certificates ca_trusted export <*name*>	Exports the specified PEM-encoded certificate to your CLI session's window for you to copy and paste.
certificates ca_trusted import <*name*>	Imports the specified PEM-encoded CA certificate from your CLI session. After you enter the command, copy and paste the PEM-encoded certificate into your CLI session window. With some terminal emulation software you may need to move your mouse around to get the transfer going.
certificates ca_trusted list	Displays all trusted CA certificate names and their basic information.
certificates ca_trusted rename <*old-name*><*new-name*>	Renames the specified trusted CA certificate.
certificates ca_trusted verify <*name*>[*timeout*]	Has the ZyXEL Device verify the certification path of the specified trusted CA certificate.
certificates ca_trusted view <*name*>	Displays details about the specified trusted CA certificate.
certificates dir_server add <*server_name*> <*addr[:port]*> [*login:password*]	Adds a new directory server entry.
certificates dir_server delete <*server-name*>	Removes the specified directory server entry.
certificates dir_server edit <*server-name*> <*addr[:port]*> [*login:password*]	Edits the specified directory server entry.
certificates dir_server list	Displays all directory server entry names and their basic information.
certificates dir_server rename <*old-server-name*><*new-server-name*>	Renames the specified directory server entry. <*old-server-name*> specifies the name of the directory server entry to be renamed. <*new-server-name*> specifies the new name for the directory server entry.
certificates dir_server view <*server-name*>	Displays details about the specified directory server entry.
certificates my_cert create cmp_enroll <*name*><*ca-addr*> <*ca-cert*><*auth-key*><*subject*> [*key-length*]	Creates a certificate request and enroll for a certificate immediately online using CMP protocol.
certificates my_cert create request <*name*><*subject*>[*key-length*]	Creates a certificate request and saves it on the ZyXEL Device for later manual enrollment.
certificates my_cert create scep_enroll <*name*><*ca-addr*> <*ca-cert*><*ra-sign*><*ra-encr*> <*auth-key*><*subject*>[*key-length*]	Creates a certificate request and enrolls for a certificate immediately online using SCEP protocol. <*ra-sign*> specifies the name of the RA (Registration Authority) signing certificate. If it is not required, type "" to leave it blank. <*ra-encr*> specifies the name of the RA encryption certificate. If it is not required, type "" to leave it blank.

Table 20 certificates Commands (continued)

COMMAND	DESCRIPTION
certificates my_cert create self_signed <*name*><*subject*> <*key-length*>	Creates a self-signed local host certificate.
certificates my_cert delete <*name*>	Removes the specified local host certificate.
certificates my_cert def_self_signed [*name*]	Sets the specified self-signed certificate as the default self-signed certificate. If you do not specify a name, the name of the current self-signed certificate displays.
certificates my_cert export <*name*>	Exports the PEM-encoded certificate to your CLI session window for you to copy and paste.
certificates my_cert import [*name*]	Imports the PEM-encoded certificate from your CLI session. A corresponding certification request must already exist on the ZyWALL. The certification request is automatically deleted after the importation. The name is optional, if you do not specify one, the certificate adopts the name of the certification request. After you enter the command, copy and paste the PEM-encoded certificate into your CLI session window. With some terminal emulation software you may need to move your mouse around to get the transfer going.
certificates my_cert list	Displays all my certificate names and basic information.
certificates my_cert rename <*old-name*><*new-name*>	Renames the specified my certificate.
certificates my_cert replace_factory	Creates a certificate using your device MAC address that is specific to this device. The factory default certificate is a common default certificate for all ZyXEL Device models.
certificates my_cert verify <*name*>[*timeout*]	Has the ZyXEL Device verify the certification path of the specified local host certificate.
certificates my_cert view <*name*>	Displays information about the specified local host certificate.
certificates remote_trusted delete <*name*>	Removes the specified trusted remote host certificate.
certificates remote_trusted export <*name*>	Exports the PEM-encoded certificate to your CLI session's window for you to copy and paste.
certificates remote_trusted import <*name*>	Imports the specified PEM-encoded remote host certificate from your CLI session. After you enter the command, copy and paste the PEM-encoded certificate into your CLI session window. With some terminal emulation software you may need to move your mouse around to get the transfer going.
certificates remote_trusted list	Displays all trusted remote host certificate names and their basic information.
certificates remote_trusted rename <*old-name*><*new-name*>	Renames the specified trusted remote host certificate.
certificates remote_trusted verify <*name*>[*timeout*]	Has the ZyXEL Device verify the certification path of the specified trusted remote host certificate.
certificates remote_trusted view <*name*>	Displays information about the specified trusted remote host certificate.

8.2 Default Values

The following table shows a list of default values.

Table 21 `certificates` Default Values

VARIABLE	DEFAULT VALUE
port	389
timeout	20 seconds
key-length	1024

8.3 Command Examples

This example creates and displays a self signed certificate named “test” with a subject alternative common name of “cert-test,” organization of “my-company”, country of “TW”, and IP 172.16.1.203. It uses a 512 bit key and is valid for 5 years.

```
ras> certificates my_cert create self_signed test "CN=cert-test,O=my-
company,C=TW;ip=172.16.1.203" 512 5
The self-signed certificate has been successfully generated.
ras> certificates my_cert list
PKI Storage Space in Use: 2%
[      Certificate Name       ]  Type [ Subject Name ] [ Issuer Name ] From [To]
auto_generated_self_signed_cert *SELF CN=ZyWALL 70 ... CN=ZyWALL 70... 2000 2030
test                            SELF CN=cert-test,... CN=cert-test... 2007 2012
------------------------------------------------------------------------------
Total number of certificates: 2
Legends: NYV - Not Yet Valid, EXPD - Expired, EXPG - Expiring, CERT -
Certificate, REQ - Certification Request, SELF - Self-signed Certificate, *SELF
- Default Self-signed Certificate
```

This example displays the certificate that the ZyXEL Device is using as the default self-signed certificate. Then it has the ZyXEL Device use the self signed certificate named “test” as the default self-signed certificate.

```
ras> certificates my_cert def_self_signed
The default self-signed certificate: auto_generated_self_signed_cert
ras> certificates my_cert def_self_signed test
Would you like to make "test" as the default self-signed certificate? (y/n):y
ras> certificates my_cert def_self_signed
The default self-signed certificate: test
```

This example exports the self signed certificate named “test”. After the certificate displays on the screen, copy and paste it into a text editor (like Notepad) and save it as a .crt or .cer file.

```
ras> certificates my_cert export test
-----BEGIN CERTIFICATE-----
MIIBlzCCAUGgAwIBAgIEOlptnzANBgkqhkiG9w0BAQUFADA2MQswCQYDVQQGEwJU
VzETMBEGA1UEChMKbXktY29tcGFueTESMBAGA1UEAxMJY2VydC10ZXN0MB4XDTAx
MDEwODAxNDcxMVoXDTA2MDEwOTAxNDcxMVowNjELMAkGA1UEBhMCVFcxEzARBgNV
BAoTCm15LWNvbXBhbnkxEjAQBgNVBAMTCWNlcnQtdGVzdDBcMA0GCSqGSIb3DQEB
AQUAA0sAMEgCQQDmnKh6ZZ5xaPukE4+djC6bu0Uyjf5aQ/QysD+Udv8xF0L/DpT1
c3xnu8hkp/RCFS3/fK6ALiLsoMCOUmqg5bdDAgMBAAGjNzA1MA4GA1UdDwEBAAQE
AwICpDAPBgNVHREECDAGhwSsFyXLMBIGA1UdEwEBAAQIMAYBAf8CAQEwDQYJKoZI
hvcNAQEFBQADQQC9hq27VCDTu6L2JsDgU8jXwYghDDKXzPR5PZ4/oryX5PFILrtr
rNLh2eTCExnyyEggaRhJ0B63Ucam7hG4k5xW
-----END CERTIFICATE-----
```

This example imports a VeriSign certificate as a trusted CA. The CA certificate has to be PEM-encoded. Refer to Section 8.3.1 on page 53 for how to save a certificate in PEM-encoded format.

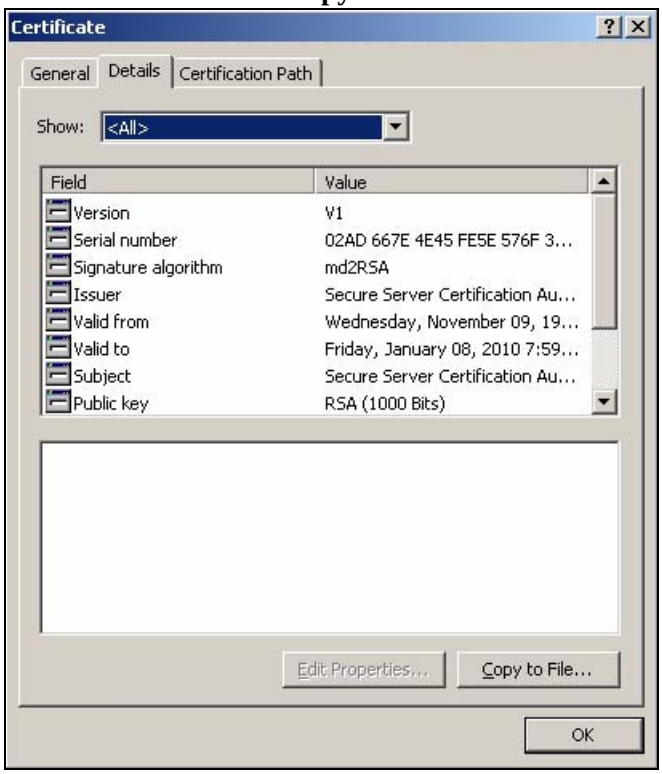
```
ras> certificates ca_trusted import VeriSign
Please paste the PEM-encoded certificate onto the screen.
Press Ctrl+D when finished or Ctrl+C to cancel.
Note: 9600 bps console port speed guarantees minimum transmission error
rate.
-----END CERTIFICATE-----rTJXwT4OPjr0l91X817/OWOgHz8UA==ZHuO3ABc
```

8.3.1 Saving Certificates as PEM-encoded Format

Do the following to save a certificate in PEM-encoded format.

1 In Windows Explorer, locate and double-click the (non PEM-encoded) certificate file.

2 Click **Details** and **Copy to File**.



3 Click **Next** in the welcome screen. Select **Base-64 encoded X.509 (.CER)**.

4 Type a file name (or browse for one).

5 Click **Finish**.

6 Open the newly created file in a text editor (like Notepad) to be able to copy and paste the certificate into your CLI session.

9

CNM Agent Commands

Use these commands to configure CNM agent settings on the ZyXEL Device.

At the time of writing, only P-662 series has the commands described in this chapter.

9.1 Command Summary

The following section lists the commands for this feature.

Table 22 CNM Commands

COMMAND	DESCRIPTION
`cnm active [0:disable|1:enable]`	Enables or disables the CNM service on the ZyXEL Device. After enabled, the ZyXEL Device communicates with the CNM server through the ZyXEL Device's WAN.
`cnm sgid [id]`	Displays the unique ID received from the CNM server after the ZyXEL Device registered suceessfully.
`cnm managerIp`	Displays or sets the CNM server's IP address.
`cnm debug [0:disable|1:enable]`	Controls whether the debugging information is displayed on the console. You must use 115200 bps for the baud rate to display the debugging message.
`cnm reset`	Resets the CNM service to the initial status on the ZyXEL Device. The ZyXEL Device will register itself to the CNM server again if the service is enabled.
`cnm encrymode [0:none|1:des|2:3des]`	Displays or sets the encryption mode.
`cnm encrykey [key]`	Displays or sets the encryption key. The encryption key is 8 characters when the encryption mode is set to "DES". The encryption key is 24 characters when the encryption mode is set to "3DES".
`cnm keepalive <10-655>`	Sets how often (in seconds) the ZyXEL Device sends a keepalive packet to inform the CNM server of its existence.

Table 22 CNM Commands (continued)

COMMAND	DESCRIPTION
`cnm version`	Displays the CNM agent version on the ZyWALL.
`cnm regiserTime [30-2147483]`	Sets how often in seconds the ZyXEL Device registers itself to the CNM server. The default is 180 seconds. Configure this to prevent multiple ZyXEL Devices from registering at the same time and causing heavy system loading on the CNM server.

9.2 Command Examples

This example displays the CNM agent version on the ZyXEL Device.

```
ras> cnm version
cnm version: 2.1.6(XJ.0)base
```

This example configures the CNM settings and activates the service on the ZyXEL Device using the following settings.

- CNM server IP address: 10.1.1.252
- Encryption mode: DES
- Encryption key: 12345678
- How often to send a keepalive packet to the CNM server: every 90 seconds

```
ras> cnm managerIp 10.1.1.252
managerIp 10.1.1.252
ras> cnm encrymode 1
cnm encrymode 1
ras> cnm encrykey 12345678
encrykey 12345678
ras> cnm keepalive 300
cnm keepalive 300
ras> cnm active 1
cnm active 1
Last Register Time: 0-0-0 0:0:0
```

This example displays the CNM debug messages. It's useful for monitoring register or keepalive packets the ZyXEL Device sends and receives to and from the CNM server.

```
ras> cnm debug 1
cnm debug 1 <0:Disable 1:Enable> CNM debug messges can only be printed at 115200
 baud rate.
ras>
agentIpAddr: 10.1.1.252
CNM protocol version = 1
sendSgmpRegisterRequest sessionID = [0]
sgmpAgentRx iface_p=b04088 cnt=1
sgmpRxEventProcess opType 1
procAgentRegister
SessionID is modified by Vantage to [0]
received SGMP_T_REGISTER:SGMP_C_RESPONSE
Error tUnit=4096
sendSgmpRegisterAck ackCode=9
procAgentRetrieve event SGMP_EVENT_REGISTER_RESP
sendSgmpRetrieveStoreRequest opType=2
sgmpd state SGMP_STATE_REGISTERING
sgmpAgentRx iface_p=b04088 cnt=1
sgmpRxEventProcess opType 2
procAgentRetrieve, agentState = 1
SessionID is modified by Vantage to [0]
received SGMP_T_RETRIEVE:SGMP_C_RESPONSE
sendSgmpRetrieveStoreAck opType=2 ackCode=9
procAgentRetrieve event SGMP_EVENT_RETRIEVE_RESP
sgmpd state SGMP_STATE_RETRIEVE_INIT
 event: SGMP_EVENT_RETRIEVE_SUCCESS
sendRetrieveStoreSucc opType=2 opCode=3
sendSgmpRegisterSuccess
sgmpd state SGMP_STATE_ACTIVE
 No Alarms Exist!
sgmpAgentRx iface_p=b04088 cnt=1
sgmpRxEventProcess opType 9
SessionID is modified by Vantage to [478043139]
tUint = 4110, Amount_Item = 1, nUnit = 1
procInquireData FORWARD COMPATIBILITY
 Device (1b55) unsupport CNM Forward Compatibility!!
 Fail to send Forward Comp Information to CNM.
call sendSgmpInquireSuccess
sendSgmpInquireSuccess opType=9 opCode=4 sessionID =[1909254747]
Send SGMP KA Trap IP=10.1.1.252, life=0, interval=90 (secs)
 No Alarms Exist!
Send SGMP KA Trap IP=10.1.1.252, life=90, interval=90 (secs)
 No Alarms Exist!
```

10

VoIP DECT Commands

Use these commands to configure DECT (Digitally Enhanced Cordless Telecommunications) settings on the ZyXEL Device.

These commands are only available on ZyXEL Devices which have a DECT cordless phone base station.

10.1 Command Summary

The following section lists the commands for this feature.

Table 23 dect Command Summary

COMMAND	DESCRIPTION
`voice config dect index <index>`	Loads the DECT settings for configuration.
`voice config dect bspassword <index> <base-station-password>`	Sets the base station password. This is the password that DECT phones must enter when registering with the base station. *base-station-password*: 4 digit number, for example “0987”.
`voice config dect save <index>`	Saves the DECT configuration on the ZyXEL Device.
`voice config dect display <index>`	Shows the base station password. *index*: 1
`voice dect page`	Pages all handset registered with the base station on the ZyXEL Device.
`voice dect reset`	Resets the base station and initiates it.
`voice dect handsetlist`	Displays the list of registered handsets.
`voice dect version`	Displays the base station firmware version.
`voice dect upgradefw`	Upgrades the base station firmware via a console. The DECT upgrade should only be performed by a service technician.
`voice dect subscript`	Enables DECT subscription to allow DECT phones to register with the base station.
`voice dect restoredectrom`	Resets the DECT module to the factory defaults.
`voice dect fwupgrade`	Upgrades the base station firmware via a console. The DECT upgrade should only be performed by a service technician.
`voice dect clearhandset`	Removes the list of registered handsets.
`voice dect fwversion`	Displays the base station firmware version.

10.2 Command Examples

This example sets the base station password on the ZyXEL Device to be **1155**.

```
ras> voice config dect index 1
ras> voice config dect bspassword 1 1155
ras> voice config dect save 1
```

11

Ethernet Commands

Use these commands to configure the settings of Ethernet ports on ZyXEL Device.

11.1 Command Summary

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

Table 24 Ethernet Command Input Values

LABEL	DESCRIPTION
ch-name	This is a channel name, for example in a DSL product with WLAN and DMZ, the LAN is `enet0`, the WLAN is `enet1` and the DMZ is `enet2`. The channel varies by your ZyXEL Device model.

The following section lists the commands for this feature. Not all commands are available on all models.

Table 25 Ethernet Commands

COMMAND	DESCRIPTION
`ether bridge`	Displays whether or not bridge mode is enabled on the ZyXEL Device.
`ether config`	Displays the Ethernet configuration.
`ether driver cnt disp <ch-name>`	Displays the specified interface's Ethernet statistics.
`ether driver status <ch-name>`	Displays the specified interface information, including the channel ID number and MAC address.
`ether driver config [0|1=auto|normal] [0|1=10|100] [0|1=HD|FD] <ch-name>`	Sets an interface's connection speed and duplex mode. This command is for a ZyXEL Device with one Ethernet LAN port only.
`ether driver qroute`	Displays the current quick route setting.
`ether driver qroute [0:Off|1:ISR|2:Task]`	Disables or enables quick routing in ISR (Interrupt-related System Register) mode or task mode to speed up routing. In ISR mode, the ZyXEL Device generates an interrupt signal when receiving a packet. In task mode, the ZyXEL Device creates a task to handle the received packets. By default, quick route is enabled in task mode in the ZyXEL Device. This command is configurable only on system reboot.
`ether edit load <ether-no>`	Loads the Ethernet configuration for the specified interface. *ether-no*: 1:LAN, 2:WAN, 3:DMZ, 4: WLAN

Table 25 Ethernet Commands (continued)

COMMAND	DESCRIPTION
`ether edit mtu <value>`	Sets the Ethernet Maximum Transmission Unit (MTU) size for the specified interface.
`ether edit accessblock <0:disable|1:enable>`	Allows or disallows packets through the specified interface.
`ether edit save`	Saves the Ethernet configuration.
`ether portStatus`	Displays whether the port is connected and the speed of the connection.
`ether switch cnt <all|clear|0|1|2|3|4|5>`	Displays or removes the Ethernet port's packet statistics.
`ether switch igmpsnp disable`	Deactivates IGMP snooping on the ZyXEL Device.
`ether switch igmpsnp enable`	Activates IGMP snooping on the ZyXEL Device.
`ether switch igmpsnp status`	Displays whether or not IGMP snooping is enabled on the ZyXEL Device.
`ether switch speedDuplex <port-id> [a|m =auto|manual] [10|100] [h|f =half|full-duplex]`	Sets an Ethernet port's connection speed and duplex mode. This command is for a ZyXEL Device with a four-port switch only. *port-id*: all|1|2|3|4
`ether switch status`	Displays the link status, speed and duplex mode of each Ethernet port.
`ether version`	Displays the Ethernet driver version.

11.2 Command Examples

This example changes the LAN speed of a ZyXEL Device with one Ethernet LAN port to 10 Mbps and full duplex.

```
ras> ether driver config 1 0 1 enet0
```

This example set the speed of LAN port 3 in the ZyXEL Device with a four-port switch to 10 Mbps and full duplex. This also displays the link status, speed and duplex mode of each Ethernet port.

```
ras> ether switch speedDuplex 3 m 10 f
Done
ras> ether switch status
Port#    Link    Speed    Duplex
  1       -        -        -
  2       -        -        -
  3       Y        10      Full
  4       Y        100     Full
ras>
```

This example loads the Ethernet configuration for the LAN, sets the MTU size to 1500 bytes, allows packets transmitting through the LAN and saves the changes.

```
ras> ether edit load 1
ras> ether edit mtu 1500
ras> ether edit accessblock 0
ras> ether edit save
ras>
```

12

Firewall Commands

Use these commands to configure firewall settings on the ZyXEL Device.

12.1 Command Summary

The following table describes input values for some of the `firewall` commands. Other values are discussed with the corresponding commands.

Table 26 Firewall Command Input Values

LABEL	DESCRIPTION
set-number	The number of a set of firewall rules. The firewall rules are grouped in sets by packet direction. Refer to Table 27 on page 67 for which set number to use for each firewall direction.
rule-number	The number of a specific firewall rule.
from	A traffic source (where the traffic enters the ZyXEL Device). Use one of the following. lan/wan/dmz
to	A traffic destination (where the traffic leaves the ZyXEL Device). Use one of the following. lan/wan/dmz

The following section lists the `firewall` commands.

Table 27 Firewall Set Numbers

FIREWALL DIRECTION	SET-NUMBER
LAN to WAN	1
WAN to LAN	2
DMZ to LAN	3
DMZ to WAN	4
WAN to DMZ	5
LAN to DMZ	6
LAN to LAN	7
WAN to WAN	8
DMZ to DMZ	9

Table 28 Firewall Commands

COMMAND	DESCRIPTION
sys firewall acl disp [*set-number*] [*rule-number*]	Displays all of the firewall rules, rules for a specific direction of packet travel, or a a specific rule.
sys firewall active <yes|no>	Enables or disables the firewall.
sys firewall cnt disp	Displays the firewall log type and count.
sys firewall cnt clear	Clears the firewall log count.
sys firewall update	Update the firewall configuration.
sys firewall dos smtp	Enables or disables the SMTP Denial of Service (DoS) defender.
sys firewall dos display	Displays the SMTP DoS defender setting.
sys firewall dos ignore <lan|wan|dmz|wlan> [on|off]	Sets the firewall to ignore DoS attacks on the specified interface.
sys firewall ignore dos <lan|wan|dmz|wlan> [on|off]	Sets the firewall to ignore DoS attacks on the specified interface. Same function as the previous command.
sys firewall ignore triangle	Sets if the firewall ignores triangle route packets on the LAN or WAN.
sys firewall schedule load <*set-number*> <*rule-number*>	Loads the firewall schedule by rule.
sys firewall schedule display	Displays the firewall schedule.
sys firewall schedule save	Saves and applies the firewall schedule.
sys firewall schedule week monday <on|off>	Turns the firewall schedule on or off for Mondays.
sys firewall schedule week tuesday <on|off>	Turns the firewall schedule on or off for Tuesdays.
sys firewall schedule week wednesday <on|off>	Turns the firewall schedule on or off for Wednesdays.
sys firewall schedule week thursday <on|off>	Turns the firewall schedule on or off for Thursdays.
sys firewall schedule week friday <on|off>	Turns the firewall schedule on or off for Fridays.
sys firewall schedule week saturday <on|off>	Turns the firewall schedule on or off for Saturdays.
sys firewall schedule week sunday <on|off>	Turns the firewall schedule on or off for Sundays.
sys firewall schedule week allweek <on|off>	Turns the firewall schedule on or off for all week.
sys firewall schedule timeOfDay <always|hh:mm <*hh:mm*>>	Sets what time the firewall schedule applies to.

12.2 Command Examples

This example loads a firewall schedule for LAN to WAN firewall rule 1 and sets the schedule to apply the rule on all days of the week except Saturday and saves the schedule.

```
ras> sys firewall schedule load 2 1
Schedule Active(0=no, 1=yes): 0
ras> sys firewall schedule week monday off
Sun: 1, Mon: 0, Tue: 1, Wed: 1, Thu: 1, Fri: 1, Sat: 1.
Schedule Enable All Day On.
ras> sys firewall schedule save
Save schedule successful.
ras> sys firewall acl disp 2 1

ACL Runtime Data for ACL Set Number: 2
    Number of Rules: 2
        ACL default action (0=Drop, 1=Permit, 2=Reject): 0
    ICMP Idle Timeout: 0
    UDP Idle Timeout: 0
    TCP SYN Wait Timeout: 0
    TCP FIN Wait Timeout: 0
    TCP Idle Timeout: 0
    DNS Idle Timeout: 0
    Runtime Rule Number: 1
        Name: W2L_Rule_1        Active (0=no, 1=yes): 0
        Schedule (0=no, 1=yes): 1
        Sun: 1, Mon: 0, Tue: 1, Wed: 1, Thu: 1, Fri: 1, Sat: 1.
        Schedule Enable All Day On.
        Action (0=block, 1=permit, 2=reject): 1
        Log (0=disable, 1=enable, 2=not-m, 3=both): 0
        Alert (0=no, 1=yes): 0
        Protocol: 0
        Source IP Any: 1
        Source IP Number of Single: 0
        Source IP Number of Range: 0
        Source IP Number of Subnet: 0
        Dest IP Any: 1
        Dest IP Number of Single: 0
        Dest IP Number of Range: 0
        Dest IP Number of Subnet: 0
        TCP Source Port Any: 1
        TCP Source Port Number of Single: 0
        TCP Source Port Number of Range: 0
        UDP Source Port Any: 1
        UDP Source Port Number of Single: 0
        UDP Source Port Number of Range: 0
        TCP Dest Port Any: 0
        TCP Dest Port Number of Single: 0
        TCP Dest Port Number of Range: 0
        UDP Dest Port Any: 0
        UDP Dest Port Number of Single: 1
        UDP Dest Port Number of Range: 0
            Dest Port Single Port[1]: 68
        ICMP Custom Service Number with only Type defined: 0
        ICMP Custom Service Number with both Type and Code defined: 0
        Number of User Defined IP Protocol: 0
        ------------------------
```

13

IP Commands

Use these commands to configure IP settings on the ZyXEL Device.

13.1 Command Summary

The following table describes input values for some of the `ip` commands. Other values are discussed with the corresponding commands.

Table 29 IP Command Input Values

LABEL	DESCRIPTION
ip	An IP address in dotted decimal notation. For example, 192.168.1.3.
port	A protocol's port number.
interface	An interface on the ZyXEL Device. enif refers to an Ethernet interface. `enif0`: LAN `enif1`: WAN `enif2`: DMZ `wanif0`: PPPoE or PPPoA For some commands you can also add a colon and a 0 or 1 to specify an IP alias. This is only for the LAN and DMZ WLAN interfaces. For example, `enif0:0` specifies LAN IP alias 1 and `enif0:1` specifies LAN IP alias 2.
hostname	A domain name.
mask-bits	The number of bits in an address's subnet mask. To find the bit number, convert the subnet mask to binary and add all of the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1's in binary. There are three 255's, so add three eights together and you get the bit number (24).
num	The number of system report records to display. For example, if you specify 10, the top 10 report entries display.

The following section lists the IP commands.

Table 30 IP Commands

COMMAND	DESCRIPTION
`ip arp status [`*interface*`]`	Displays an interface's ARP table.
`ip des test`	Performs the DES/3DES hardware chip testing and displays the result.
`ip des reset`	Resets the DES/3DES hardware chip.
`ip dhcp <`*interface*`> client release`	Releases the specified interface's DHCP IP address. The interface must be a DHCP client to use this command.
`ip dhcp <`*interface*`> client renew`	Renews the specified interface's DHCP IP address. The interface must be a DHCP client to use this command.

Table 30 IP Commands (continued)

COMMAND	DESCRIPTION
ip dhcp <*interface*> mode <server|relay|none|client>	Sets the DHCP mode.
ip dhcp <*interface*> relay server <*ip*>	Sets the DHCP relay server's IP address.
ip dhcp <*interface*> reset	Resets the DHCP table.
ip dhcp <*interface*> server probecount <*num*>	Sets the DHCP probe counter.
ip dhcp <*interface*> server dnsserver <*ip-address1*> [*ip-address2*] [*ip-address3*]	Sets the DHCP DNS server IP address.
ip dhcp <*interface*> server winsserver <*wins-ip1*> [*wins-ip2*]	Sets the DHCP WINS server IP address.
ip dhcp <*interface*> server gateway <*gateway-ip*>	Sets the DHCP gateway IP address.
ip dhcp <*interface*> server hostname <*hostname*>	Sets the DHCP server name.
ip dhcp <*interface*> server initialize	Fills in DHCP parameters and initializes (for PWC purposes)
ip dhcp <*interface*> server leasetime <*period*>	Sets the DHCP leasetime.
ip dhcp <*interface*> server netmask <*subnet-mask*>	Sets the DHCP netmask
ip dhcp <*interface*> server pool <*start-ip*> <*size*>	Sets the DHCP IP pool size.
ip dhcp <*interface*> server renewaltime <*period*>	Sets the DHCP renew time.
ip dhcp <*interface*> server rebindtime <*period*>	Sets the DHCP rebind time.
ip dhcp <*interface*> server reset	Resets the DHCP table.
ip dhcp <*interface*> server server <*server-ip*>	Sets the DHCP relay server's IP address. Use this command only when you configure the DHCP mode as relay.
ip dhcp <*interface*> status	Displays the detailed DHCP status of the specified interface.
ip dhcp <*interface*> static delete <*index*|all>	Deletes the static DHCP entries.
ip dhcp <*interface*> static display	Displays static DHCP mac table
ip dhcp <*interface*> static update <*index*> <*mac-address*> <*ip-address*>	Adds a static DHCP entry. The IP should be available in the DHCP pool. *mac-address*: This is a 12-digit hexadecimal number separated by colons or dashes. For example, 00:13:49:00:00:0A or 00-13-49-00-00-0A.

Table 30 IP Commands (continued)

COMMAND	DESCRIPTION
ip dns query address <*ip-address*> [*timeout*]	Displays the domain name of an IP address. *timeout*: 0~255 seconds. This is the maximum number of seconds to wait for a response.
ip dns query debug [*level*]	Enables or disables DNS debug. 0 disables this function while other values enable it.
ip dns query name <*hostname*> [*timeout*]	Displays the IP address of a domain name. *timeout*: 0~255 seconds. This is the maximum number of seconds to wait for a response.
ip dns query table	Displays DNS query table.
ip dns server <*primary*> [*secondary*] [*third*]	Sets DNS server.
ip dns stats clear	Clears DNS statistics.
ip dns stats disp	Displays DNS statistics.
ip dns table	Displays DNS request table.
ip httpd debug [on|off]	Displays or sets the web configurator debug flag.
ip icmp status	Displays the ICMP statistics counter.
ip icmp discovery <*interface*> [on|off]	Turns ICMP discovery (ICMP type 10, RFC 1256) off or on for the specified interface.
ip icmp sourcequench	Displays whether the ignore Source Quench feature is enabled or not.
ip ifconfig [*interface*]	Displays all or the specified network interface settings.
ip ifconfig <*interface*> <*ip-address*[/<*mask-bits*>]> [broadcast <*address*>] [mtu <*value*>] [*dynamic*]	Configures a network interface. mtu <*value*>: Sets the Maximum Transmission Unit. *dynamic*: Sets the interface to get an IP address via DHCP.
ip igmp debug [0:off|1:normal|2:detailed]	Sets the IGMP (Internet Group Management Protocol) debug level.
ip igmp forwardall [on|off]	Activates or deactivates IGMP forwarding to all interfaces.
ip igmp querier [on|off]	Turns the IGMP stop query flag on or off.
ip igmp iface <*interface*> grouptm <260-2147483647>	Sets the IGMP group timeout (in seconds) for the specified interface.
ip igmp iface <*interface*> interval <125-2147483647>	Sets the IGMP query interval (in seconds) for the specified interface.
ip igmp iface <*interface*> join <*group-address*>	Adds the specified interface to the specified IGMP group.
ip igmp iface <*interface*> leave <*group-address*>	Removes the specified interface from the specified IGMP group.
ip igmp iface <*interface*> query	Sends an IGMP query on the specified interface.
ip igmp iface <*interface*> rsptime [100-255]	Sets the IGMP response time in tenths (1/10) of a second.
ip igmp iface <*interface*> start	Turns on IGMP on the specified interface.
ip igmp iface <*interface*> stop	Turns off IGMP on the specified interface.

Table 30 IP Commands (continued)

COMMAND	DESCRIPTION
ip igmp iface <*interface*> ttl <*0*-2147483647>	Sets the IGMP Time To Live threshold.
ip igmp iface <*interface*> v1compat [on|off]	Turns IGMP version 1 compatibility on or off for the specified interface.
ip igmp proxy [0|1]	Set 1 to send the IGMP leave message immediately while set 0 to wait a time interval (260 seconds) before sending the leave message.
ip igmp robustness [2-2147483647]	Sets the IGMP robustness variable.
ip igmp status	Displays the IGMP status.
ip mcastChan [0:both|1:LAN|2:WLAN]	Displays or controls whether the ZyXEL Device sends the multicast packets to the LAN or WLAN or both.
ip ping <*address*>	Pings a remote host IP address or domain name.
ip policyrouting set index <*set-number*> <*rule-number*>	Loads or allocates a working buffer to editing a policy route rule. You must apply this command first before you begin to configure the IP policy route rules. *set-number*: 1-12 *rule-number*: 1-6
ip policyrouting set name <*name*>	Sets the name of IP policy route set.
ip policyrouting set active <yes|no>	Enables or disables the IP policy route rule.
ip policyrouting set criteria protocol <0:don't care|1:ICMP|6:TCP|17:UDP>	Sets the IP policy route protocol ID.
ip policyrouting set criteria serviceType <0:don't care|1:normal|2:min delay|3:max thruput|4:max reliable|5:min cost>	This sets the Type of Service (TOS) values to prioritize the incoming network traffic. The values include normal service, minimize delay, maximize throughput, maximize reliability, or minimize cost.
ip policyrouting set criteria precedence <0-7|8:don't care>	Sets the IP policy route precedence.
ip policyrouting set criteria packetlength <*length*>	Sets the IP policy route packet length.
ip policyrouting set criteria lencomp <1:equal|2:not equal|3:less|4:greater|5:less or equal|6:greater or equal>	Sets the IP policy route criteria for the specified packet length above.
ip policyrouting set criteria srcip <*start-ip*> <*end-ip*>	Sets the IP policy route source IP address
ip policyrouting set criteria srcport <*start-port*> <*end-port*>	Sets the IP policy route source ports.
ip policyrouting set criteria destip <*start-ip*> <*end-ip*>	Sets the IP policy route destination IP addresses.

Table 30 IP Commands (continued)

COMMAND	DESCRIPTION
ip policyrouting set criteria destport <*start-port*> <*end-port*>	Sets the IP policy route destination ports.
ip policyrouting set action actmatch	Sets the criteria if a packet does not match the IP policy route rule for further action.
ip policyrouting set action actnomatch	Sets the criteria if a packet matches the IP policy route rule for further action.
ip policyrouting set action gatewaytype <1:WAN-remote-node |0:gateway-address>	Sets IP policy route gateway type.
ip policyrouting set action gatewayaddr <*ip-address*>	Sets the action the ZyXEL Device forwards the packet by the specified IP address.
ip policyrouting set action gatewaynode <1-8>	Sets the action the ZyXEL Device forwards the packet by the specified ZyXEL Device's WAN remote node.
ip policyrouting set action servicetype <0:don't care|1: normal|2:min delay|3: max thruput|4:max reliable|5:min cost>	Sets the action to change the service type or not.
ip policyrouting set action precedence <0~7|8:no change>	Sets the action to change the precedence or not.
ip policyrouting set action log <yes|no>	Sets the action to enable logging or not.
ip policyrouting set display <*set-number*> <*rule-number*>	Displays the specified IP routing policy rule setting.
ip policyrouting set save	Saves the IP policy route rule setting from working buffer to non-volatine memory.
ip policyrouting set freememory	Clears the IP policy route settings in the working buffer.
ip policyrouting set clear <*set-number*> [*rule-number*]	Deletes a IP policy route set or rule settings in the non-volatile memory.
ip policyrouting clear	Clears the IP policy route count.
ip policyrouting disp	Displays the IP policy route count.
ip policyrouting switch [on|off]	Switchs on or off the IP policy route count.
ip rip accept <*gateway*>	Drops an entry from the RIP (Routing Information Protocol) refusing list.
ip rip activate	Enables RIP.
ip rip merge [on|off]	Sets RIP merge flag.
ip rip refuse <*gateway*>	Adds an entry to the RIP refuse list.
ip rip request <*address*> [*port*]	Sends RIP request to some address and port.
ip rip reverse [on|off]	RIP Poisoned Reverse.
ip rip status	Displays RIP statistic counters.
ip rip trace [*number*]	Enables the RIP trace flag for debugging.

Table 30 IP Commands (continued)

COMMAND	DESCRIPTION
ip rip mode <*interface*> in [*mode*]	Sets the RIP direction to in for the specified interface. [*mode*]: This is a number. *0*: None. Don't follow any RIP standards. *1*: RIP-1 only. Only follows RIP version 1 standard. *2*: RIP-2 only. Only follows RIP version 1 standard. *3*: Both. Follows both RIP version 1 and version 2 standards.
ip rip mode <*interface*> out [*mode*]	Sets the RIP direction to out for the specified interface. [*mode*]: This is a number. *0*: None. Don't follow any RIP standards. *1*: RIP-1 only. Only follows RIP version 1 standard. *2*: RIP-1-compatible RIP-2. Follows both RIP version 1 and version 2 standards. *3*: RIP-2 only. Only follows RIP version 1 standard.
ip rip dialin_user <show|in|out|both|none>	Displays or sets the RIP direction. • When set to both or out, the ZyXEL Device will broadcast its routing table periodically. • When set to both or in, it will incorporate the RIP information that it receives. • When set to none, the ZyXEL Device doesn't send any RIP packets out and it also ignores any RIP packets received.
ip route add <*dest-ip*|default>[/<*mask-bits*>] <*gateway-ip*> <*metric*>	Adds a route. The route is runtime only (it is not kept in permanent memory).
ip route addiface <*dest-ip*>[/<*mask-bits*>] <*interface*> [*metric*]	Adds an entry to the routing table for the specified interface.
ip route addprivate <*dest-ip*|default>[/*mask-bits*] <*gateway-ip*> [*metric*]	Adds a private route.
ip route addrom index <*index*>	Adds a static route.
ip route addrom name <*name*>	Sets the name for a static route.
ip route addrom set <*dest-ip*>[/<*mask-bits*>] <*gateway-ip*> <*metric*>	Sets the static route settings.
ip route addrom active [on|off]	Activates or deactivates the static route.
ip route addrom private [yes|no]	Sets this route as private.
ip route addrom save	Saves the static route configuration.
ip route addrom clear [*index*]	Deletes the static route.
ip route addrom freememory	Clears working buffer.
ip route addrom display	Displays all static routes.
ip route drop <*ip-address*>[/*mask-bits*]	Drops a route.
ip route status [*interface*]	Displays the routing table.
ip smtp server [*address*]	Sets the smtp server address.

Table 30 IP Commands (continued)

COMMAND	DESCRIPTION
ip smtp destmail [*address*]	Sets the destination mail address.
ip smtp srcmail [*address*]	Sets the source mail address.
ip smtp sendmail	Sends a mail.
ip smtp addrlist	Lists the smtp server, destination and return addresses.
ip smtp addrreset	Resets the smtp server, destination and return addresses.
ip status	Displays IP statistics counters.
ip tcp status	Displays the TCP statistics counters.
ip telnet <*host-address*> [*port*]	Creates a Telnet connection to the specified host.
ip tftp support	Displays whether the ZyXEL Device supports TFTP.
ip tftp stats	Displays TFTP statistics coutners.
ip traceroute <*host*> [*ttl*] [*wait*] [*queries*]	Sends ICMP packets to trace the route of a remote host. *ttl*: Time to live in seconds (0-255). *wait*: Timeout in seconds (0-255). *queries*: The number of ICMP packets to use (1-5).
ip tredir active <on|off>	Enables or disables traffic redirect.
ip tredir checktime <*period*>	Sets the number of seconds (0-255) ZyXEL Device waits between attempts to connect to the target.
ip tredir disp	Displays the traffic redirect configuration.
ip tredir failcount <*count*>	Sets the number of times that ZyXEL Device can ping the target without a response before forwarding traffic to the backup gateway.
ip tredir partner <*ip-address*>	Sets the traffic redirect backup gateway IP address.
ip tredir save	Saves traffic redirect configuration.
ip tredir target <*ip-address*>	Sets the IP address that ZyXEL Device uses to test WAN accessibility.
ip tredir timeout <*timeout*>	Sets the maximum number of seconds (0-255) ZyXEL Device waits for a response from the target.
ip udp status	Displays UDP status.
ip urlfilter customize actionFlags act(1-7)<enable/disable>	Sets and displays the action flags.
ip urlfilter customize add [*string*] [trust|untrust|keyword]	Adds the trusted, untrusted, or a keyword block with the url string for filtering.
ip urlfilter customize delete [*string*] [trust|untrust|keyword]	Deletes the trusted, untrusted, or a keyword block with the url string for filtering.
ip urlfilter customize display	Displays settings for the URL filter.
ip urlfilter customize logFlags type<1-3> <enable|disable>	Sets and displays the logging flags. type1: for websites do not match either custom blocked or custom forwarded websites. type2: for custom blocked websites. type3: for custom forwarded websites.

Table 30 IP Commands (continued)

COMMAND	DESCRIPTION
`ip urlfilter customize reset`	Clears all customized filtering settings.
`ip urlfilter exemptZone actionFlags type <1-3> <enable|disable>`	Sets the exempt zone action flags.
`ip urlfilter exemptZone add <ip1> <ip2>`	Adds a range of IP addresses for which URL filtering is not conducted.
`ip urlfilter exemptZone delete <ip1> <ip2>`	Deletes the specified range of IP addresses for which URL filtering is not conducted.
`ip urlfilter exemptZone display`	Displays the range of IP addresses for which url filtering is not conducted.
`ip urlfilter exemptZone reset [type <1-3>][enable|disable]`	Resets the exempt zone action flags.
`ip urlfilter general enable <on|off>`	Enables or disables content filtering.
`ip urlfilter general display`	Displays all content filering settings.
`ip urlfilter general exemptZone display`	Displays the content filtering trusted zone settings.
`ip urlfilter general exemptZone actionFlags type<1-3> <enable|disable>`	Sets the exempt zone action flags.
`ip urlfilter general exemptZone add <ip1> <ip2>`	Adds a trusted user IP range.
`ip urlfilter general exemptZone delete <ip1> <ip2>`	Deletes a trusted user IP range.
`ip urlfilter general exemptZone reset`	Clears all content filtering trusted zone settings.
`ip urlfilter general reset`	Clears the content filtering settings.
`ip urlfilter general webFeature <block|nonblock> <activex|java|cookie|webproxy>`	Blocks or forwards the specified web features including ActiveX, JAVA, cookies, or web proxy.
`ip urlfilter general timeOfDay [always|from-time to-time]`	Sets the content filtering blocking schedule. *from-time*,*to-time*: Enter the format as "hh:mm".
`ip urlfilter general blockingText <text>`	Specifies a key word in a web site address you wish to block access.
`ip urlfilter webControl enable`	Enables content access control (CAC).
`ip urlfilter webControl display`	Displays the CAC settings.
`ip urlfilter webControl logAndBlock [log|block|both]`	Enables the action of logging , block or both for matched web site.
`ip urlfilter webControl category <block|forward> <1-55|all>`	Blocks or forwards the specified or all web categories. The command lists you all blocked web categories then. Refer to Table 31 on page 79 for the categories.
`ip urlfilter webControl serverList display`	Displays available CAC server list and their round trip time. You have to get the Internet access to use this command.
`ip urlfilter webControl serverList refresh`	Refreshs and adds the active CAC servers in the list.

Table 30 IP Commands (continued)

COMMAND	DESCRIPTION
`ip urlfilter webControl queryURL <url> <server|localcache>`	Checks with the CAC server or the ZyXEL Device's cache whether the specified URL is blocked or not.
`ip urlfilter webControl cache display`	Displays the ZyXEL Device's cache entries.
`ip urlfilter webControl cache delete [entry-number|All]`	Deletes one or all ZyXEL Device's cache entries.
`ip urlfilter webControl blockonerror <block|log> <on|off>`	Blocks or logs the websites when the CAC server is unavailable.
`ip urlfilter webControl unratedwebsite <block|log> <on|off>`	Blocks or logs unrated websites.
`ip urlfilter webControl waitingTime [second]`	Sets the waiting time in seconds before the CAC server responses.
`ip urlfilter webControl reginfo display`	Displays the CAC license key.
`ip urlfilter webControl reginfo licenseid <id>`	Registers the CAC service with the specified license key from the iCard and then displays the result.
`ip urlfilter webControl zssw`	Sets the CAC server's URL.

13.1.1 Content Filtering Categories

The following section lists the relationship between countries and country codes defined in the ZyXEL Device.

Table 31 Content Filtering Categories

TYPE NUMBER	CATEGORY NAME	TYPE NUMBER	CATEGORY NAME
type 1	Adult/Mature Content	type28	Web Communications
type 2	Pornography	type29	Job Search/Careers
type 3	Sex Education	type30	News/Media
type 4	Intimate Apparel/Swimsuit	type31	Personals/Dating
type 5	Nudity	type32	Reference
type 6	Alcohol/Tobacco	type33	Chat/Instant Messaging
type 7	Illegal/Questionable	type34	Email
type 8	Gambling	type35	Newsgroups
type 9	Violence/Hate/Racism	type36	Religion
type10	Weapons	type37	Shopping
type11	Abortion	type38	Auctions
type12	Arts/Entertainment	type39	Real Estate
type13	Business/Economy	type40	Society/Lifestyle
type14	Cult/Occult	type41	Gay/Lesbian
type15	Illegal Drugs	type42	Restaurants/Dining/Food

Table 31 Content Filtering Categories

TYPE NUMBER	CATEGORY NAME	TYPE NUMBER	CATEGORY NAME
type16	Education	type43	Sports/Recreation/Hobbies
type17	Cultural Institutions	type44	Travel
type18	Financial Services	type45	Vehicles
type19	Brokerage/Trading	type46	Humor/Jokes
type20	Games	type47	Streaming Media/MP3
type21	Government/Legal	type48	Software Downloads
type22	Military	type49	Pay to Surf
type23	Political/Activist Groups	type50	For Kids
type24	Health	type51	Web Advertisements
type25	Computers/Internet	type52	Web Hosting
type26	Hacking/Proxy Avoidance	type53	Unrated
type27	Search Engines/Portals		

13.1.2 IP Command Examples

The following example shows the ZyXEL Device's ARP table.

```
ras> ip arp status
received 11 badtype 0 bogus addr 0 reqst in 3 replies 2 reqst
out 11
cache hit 241 (85%), cache miss 42 (14%)
IP-addr         Type           Time  Addr              stat iface
210.200.128.6   None            0        [proxy]        25   NULL
192.168.1.33    10 Mb Ethernet 300   00:0f:fe:0a:2d:3b 41
enif0
192.168.1.255   10 Mb Ethernet 0     ff:ff:ff:ff:ff:ff 43   NULL
192.168.2.33    10 Mb Ethernet 290   00:19:cb:00:00:12 41
enif0:0
192.168.2.255   10 Mb Ethernet 0     ff:ff:ff:ff:ff:ff 43   NULL
192.168.3.255   10 Mb Ethernet 0     ff:ff:ff:ff:ff:ff 43   NULL
num of arp entries= 6
```

The following example shows LAN's ARP information.

```
ras> ip arp status enif0
received 27 badtype 0 bogus addr 0 reqst in 14 replies 1 reqst
out 61
cache hit 2669 (83%), cache miss 511 (16%)
IP-addr         Type           Time  Addr              stat iface
192.168.1.33    10 Mb Ethernet 300   00:0f:fe:0a:2d:3b 41
enif0
num of arp entries= 1
```

The following example shows LAN IP alias 1's ARP information.

```
ras> ip arp status enif0:0
received 11 badtype 0 bogus addr 0 reqst in 3 replies 2 reqst
out 11
cache hit 363 (89%), cache miss 42 (10%)
IP-addr         Type          Time  Addr              stat iface
192.168.2.33    10 Mb Ethernet 300   00:19:cb:00:00:12 41
enif0:0
num of arp entries= 1
```

The following commands configure the ZyXEL Device LAN's DHCP setting.

```
ras> ip dhcp enif0 mode server
ras> ip dhcp enif0 server dnsserver 168.95.1.1
ras> ip dhcp enif0 server winsserver 10.1.1.250
ras> ip dhcp enif0 server leasetime 655200
ras> ip dhcp enif0 server hostname TW-Server1
ras> ip dhcp enif0 server pool 192.168.1.33 2
ras> ip dhcp enif0 status
DHCP on iface enif0 is server
     Start assigned IP address: 192.168.1.33/24
     Number of IP addresses reserved: 2
     Hostname prefix: TW-Server1
     DNS server: 168.95.1.1 0.0.0.0
     WINS server: 10.1.1.250 0.0.0.0
     Domain Name :
     Default gateway: 192.168.1.1
     Lease time: 655200 seconds
     Renewal time: 129600 seconds
     Rebind time: 226800 seconds
     Probing count: 100
slot    state      timer   type  hardware address     hostname
   0  UNCERTAIN          0    0  00
   1  UNCERTAIN          0    0  00
Status:
     Packet InCount: 0, OutCount: 0, DiscardCount: 0
```

The following command has the ZyXEL Device ping IP address 172.16.1.202 five times.

```
ras> ip pingext 172.16.1.202 -n 5
Resolving 172.16.1.202... 172.16.1.202
      sent      rcvd    size     rtt     avg     max     min
         1         1      36       0       0       0       0
         2         2      36       0       0       0       0
         3         3      36       0       0       0       0
         4         4      36       0       0       0       0
         5         5      36       0       0       0       0

Extended Ping From device to 172.16.1.202:
   Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate Round Trip Times in milli-seconds:
   RTT: Average = 0ms, Maximum =  0ms, Minimum = 0ms
```

The following example configures the DNS server settings the ZyXEL Device assigns to LAN DHCP clients. In this case the first DNS server is the one assigned by ISP 1. The second DNS server is at IP address 192.168.1.5. No third DNS server is assigned.

```
ras> ip dns lan edit 0 0 1 1
ras> ip dns lan edit 1 1 192.168.1.5
ras> ip dns lan edit 2 3
ras> ip dns lan display
Router assigned DNS servers to host
===================================
First DNS server is from WAN_1, DNS server index 1
Second DNS server is user defined: 192.168.1.5
Third DNS server is none
```

This example does the following.

1. Inserts a new DNS address record named example for www.my-company.com.example for the WAN 1 interface.
2. Inserts a new DNS address record named example for a private DNS server for www.my-company-1.com.example.
3. Displays the system DNS server settings.

```
ras> ip dns system inserta -1 www.my-company.com.example 0 0 1
ras> ip dns system insertns -1 www.mycompany-2.com.example 2 10.0.0.5
ras> ip dns system display
System DNS HA and Proxy Service Configuration
=============================================

Rule Summary: A Record
001 | record type=A Record, ISP=WAN_1
    | FQDN       =www.my-company.com.example

Rule Summary: NS Record
001 | record type=NS Record, DNS server=10.0.0.5(private)
    | Domain Name=www.mycompany-2.com.example
```

The following example sets the WAN 1 interface to use IP address 172.16.1.203 and subnet mask 255.255.0.0.

```
ras> ip ifconfig enif1 172.16.1.203/16
enif1: mtu 1500 mss 1460
    inet 172.16.1.203, netmask 0xffff0000, broadcast 172.16.255.255
    RIP RX:None, TX:None,
    [InOctets        197396] [InUnicast       621] [InMulticast          982]
    [InDiscards          72] [InErrors          0] [InUnknownProtos       72]
    [OutOctets        89305] [OutUnicast      629] [OutMulticast           0]
    [OutDiscards          0] [OutErrors          0]
```

The following example displays the IGMP status.

```
ras> ip igmp status
Group           groupLink           ifaceLink           flags
224.0.0.12      [0102fd80 00c618c0] [0102fdc4 0102fdc4] 0003
224.0.0.9       [0102fd4c 0102fdb4] [0102fd90 0102fd90] 0001
224.0.0.2       [0102fd18 0102fd80] [0102fd5c 0102fd5c] 0001
224.0.0.1       [00c618c0 0102fd4c] [0102fd28 0102fd28] 0001

iface enif0 flags 00000000
  query interval 125 sec, max rsp time 100 1/10 sec, group timeout 260 sec,
  counter 0, query timer 0 sec, v1 host present timer 0 sec,
  ttl threshold 1
  multicast group:
------------------snip---------------------
iface enif5:1 flags 00000000
  query interval 0 sec, max rsp time 0 1/10 sec, group timeout 0 sec,
  counter 0, query timer 0 sec, v1 host present timer 0 sec,
  ttl threshold 0
  multicast group:
```

The following table describes the labels in this display.

Table 32 ip igmp status

LABEL	DESCRIPTION
Group	This field displays group multicast IP addresses.
groupLink ifaceLink flags	These fields are for debug purposes. Send a screenshot of this screen to customer support if there are problems with IGMP snooping on the ZyXEL Device.
iface	This is the ZyXEL Device interface.
flags	00000000
query interval	This is the time period between sending IGMP Host Membership Queries.
max rsp time	This is the IGMP maximum response time.
group timeout	The IGMP group timeout.
counter	The IGMP counter.
query timer	This is how long a mulicast router waits before deciding there is not another multicast router that should be the querier.
v1 host present timer	How long the ZyXEL Device waits to detect the presence of another IGMPv1 router.
ttl threshold	The IGMP group time to live threshold.
multicast group	This field lists any multicast groups to which the interface belongs.

The following example displays the ICMP status.

```
ras> ip icmp status
( 1)icmpInMsgs                  0     (14)icmpOutMsgs               1628
( 2)icmpInErrors                0     (15)icmpOutErrors                0
( 3)icmpInDestUnreachs          0     (16)icmpOutDestUnreachs          0
( 4)icmpInTimeExcds             0     (17)icmpOutTimeExcds             0
( 5)icmpInParmProbs             0     (18)icmpOutParmProbs             0
( 6)icmpInSrcQuenchs            0     (19)icmpOutSrcQuenchs            0
( 7)icmpInRedirects             0     (20)icmpOutRedirects             0
( 8)icmpInEchos                 0     (21)icmpOutEchos              1614
( 9)icmpInEchoReps              0     (22)icmpOutEchoReps              0
(10)icmpInTimestamps            0     (23)icmpOutTimestamps            0
(11)icmpInTimestampReps         0     (24)icmpOutTimestampReps         0
(12)icmpInAddrMasks             0     (25)icmpOutAddrMasks             0
(13)icmpInAddrMaskReps          0     (26)icmpOutAddrMaskReps          0
```

The following table describes the labels in this display.

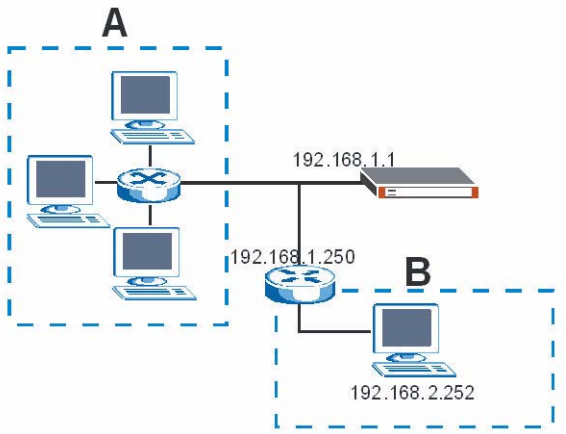
Table 33 ip icmp status

LABEL	DESCRIPTION
icmpInMsgs	The number of ICMP messages received on the interface.
icmpInErrors	The number of ICMP messages with an error received on the interface.
icmpInDestUnreachs	The number of ICMP Destination Unreachable messages received on the interface.
icmpInTimeExcds	The number of ICMP Time Exceeded messages received on the interface.
icmpInParmProbs	The number of ICMP Parameter Problem messages received on the interface.
icmpInSrcQuenchs	The number of ICMP Source Quench messages received on the interface.
icmpInRedirects	The number of ICMP Redirect messages received on the interface.
icmpInEchos	The number of ICMP Echo (request) messages received on the interface.
icmpInEchoReps	The number of ICMP Echo Reply messages received on the interface.
icmpInTimestamps	The number of ICMP Timestamp messages received on the interface.
icmpInTimestampReps	The number of ICMP Timestamp Reply messages received on the interface.
icmpInAddrMasks	The number of ICMP Address Mask Request messages received on the interface.
icmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received on the interface.
icmpOutMsgs	The number of ICMP messages received sent through the interface.
icmpOutErrors	The number of ICMP messages with an error sent through the interface.
icmpOutDestUnreach	The number of ICMP Destination Unreachable messages sent through the interface.
icmpOutTimeExcds	The number of ICMP Time Exceeded messages sent through the interface.
icmpOutParmProbs	The number of ICMP Parameter Problem messages sent through the interface.
icmpOutSrcQuench	The number of ICMP Source Quench messages sent through the interface.

Table 33 ip icmp status

LABEL	DESCRIPTION
icmpOutRedirects	The number of ICMP Redirect messages sent through the interface.
icmpOutEchos	The number of ICMP Echo (request) messages sent through the interface.
icmpOutEchoReps	The number of ICMP Echo Reply messages sent through the interface.
icmpOutTimestamps	The number of ICMP Timestamp messages sent through the interface.
icmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent through the interface.
icmpOutAddrMasks	The number of ICMP Address Mask Request messages sent through the interface.
icmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent through the interface.

The following example adds a policy route rule on the ZyXEL Device. The ZyXEL Device's LAN is in the network A (192.168.1.0/24) and its default gateway is 192.168.1.1. However, network admin would like to forward some computer's HTTP traffic that sends to 192.168.2.252 (in network B) through another router, 192.168.1.250.



We use following settings.

- The IP policy route set and rule numbers: set 1, rule 1
- The IP policy route set's name: Rule-1
- The criteria settings for the policy route rule:
  - The Protocol: TCP
  - The source IP: 192.168.1.2~192.168.1.254
  - The destination IP: 192.168.2.252
  - The destination port: 80
  - The checking if a packet matches the criterias or not: match
- The action settings for the policy route rule:
  - The gateway type: gateway address
  - The gateway address: 192.168.1.250

- Log: yes

```
ras> ip policyrouting set index 1 1
ras> ip policyrouting set name Rule-1
IPPR Name= Rule-1
ras> ip policyrouting set criteria protocol 6
the protocol =6
ras> ip policyrouting set criteria srcip 192.168.1.2
192.168.1.254
ras> ip policyrouting set criteria destip 192.168.2.252
ras> ip policyrouting set criteria destport 80
ras> ip policyrouting set active yes
ras> ip policyrouting set action actmatch
Action matched
ras> ip policyrouting set action gatewaytype 0
gateway type: gateway addr
ras> ip policyrouting set action gatewayaddr 192.168.1.250
ras> ip policyrouting set action log yes
ras> ip policyrouting set save
ras>
```

The following example displays the policy route rule on the ZyXEL Device.

```
ras> ip policyrouting set display 1 1
Set: 1 Rule: 1

Policy Set Name:Rule-1

 Active:yes
 IP Protocol :TCP
Type of Service: Don't care
Precedence : 0
Packet length=0
 Source:
 addr start=:192.168.1.2
 end start=:192.168.1.254
 port start=0
 port end=0
  Destination:
 addr start=:192.168.2.252
 end start=:192.168.2.252
 port start=80
 port end=80
  Action= Matched
  Gateway type   = Gateway addr
Type of Service: normal
Precedence =0
 Gateway addr=192.168.1.252
 Gateway node=0
 Log= Yes
ras>
```

The following example displays all content filtering categories.

```
ras> ip urlfilter webControl display
Web Control:
    Enable
Log and Access:
    Log and Block Access
Actions:
    Block when query error: off
Parameters:
    the packets max waiting time:10 (sec)
The Categories:
type 1        :Adult/Mature Content
type 2        :Pornography
type 3        :Sex Education
type 4        :Intimate Apparel/Swimsuit
....
```

The following example blocks or unblock content filtering categories. The command always displays all the blocked categories.

```
ras> ip urlfilter webControl category block
Usage: [block/forward][(1-55)/all]
ras> ip urlfilter webControl category block 1
Block Category:
type 1 :Adult/Mature Content
\as> ip urlfilter webControl category block 5
Block Category:
type 1 :Adult/Mature Content
type 5 :Nudity
ras> ip urlfilter webControl category forward 1
Block Category:
type 5 :Nudity
ras>
```

The following example queries the URL in the CAC server or the content filtering cache on the ZyXEL Device. The ZyXEL Device responds you the result.

```
ras> ip urlfilter webControl queryURL
Usage: [url][Server/localCache]
ras> ip urlfilter webControl queryURL www.playboy.com server
The url is blocked
ras> ip urlfilter webControl queryURL www.zyxel.com localcache
The url is forwarded
ras> ip urlfilter webControl queryURL www.openfind.com.tw
localcache
The url is not in local cache
ras>
```

The following example displays the entries in the content filtering cache on the ZyXEL Device.

```
ras> ip urlfilter webControl cache display
the total entries:3
idx block port URL
-----------------------------------------------
1   YES    80   www.espn.com/
2   NO     80   www.myzyxel.com/
3   YES    80   www.zyxel.com
ras>
```

14

IPSec Commands

Use these commands to configure IPSec settings on the ZyXEL Device.

14.1 Command Summary

The following section lists the commands for this feature.

Table 34 IPSec Commands

COMMAND	DESCRIPTION
`ipsec debug [on|off]`	Enables or disables the trace for IPSec debugging information.
`ipsec route dmz [on|off]`	After IPSec processes a packet that will be sent to the DMZ, this ZyXEL Device controls whether or not the packets can be forwarded to another IPSec tunnel.
`ipsec route lan [on|off]`	After IPSec processes a packet that will be sent to the LAN, this ZyXEL Device controls whether or not the packets can be forwarded to another IPSec tunnel.
`ipsec route wan [on|off]`	After IPSec processes a packet that will be sent to the WAN, this ZyXEL Device controls whether or not the packets can be forwarded to another IPSec tunnel.
`ipsec show_runtime sa`	Displays active IKE and IPSec SAs.
`ipsec show_runtime spd`	Displays the local and remote network address pairs used to differentiate the connected dynamic VPN tunnels.
`ipsec switch <on|off>`	Enables or disables all IPSec rules. The setting resets to off after the ZyXEL Device restarts.
`ipsec timer chk_my_ip <1~3600>`	Sets the interval (in seconds) for checking if the ZyXEL Device's WAN IP address has changed
`ipsec timer chk_conn <0~255>`	The ZyXEL Device disconnects a VPN tunnel if there is no reply traffic for this number of minutes. `0` disables the check.
`ipsec timer update_peer <0~255>`	For IPSec rules with a domain name as the local or remote gateway address, this command sets the interval (in minutes) for resolving the domain name and updating the rules. 0 disables the updates.
`ipsec timer chk_input <0~255>`	The ZyXEL Device disconnects any IPSec connection that has no inbound traffic for this number of minutes. `0` disables the check (this is the default setting).
`ipsec updatePeerIp`	If you use a domain name as the local or remote gateway address, this command forces the ZyXEL Device to resolve the domain name and update the IPSec rules right away.

Table 34 IPSec Commands (continued)

COMMAND	DESCRIPTION
`ipsec dial <rule-number>`	Dials the specified IPSec policy manually.
`ipsec display <rule-number>`	Displays the specified IPSec rule. Use `ipsec load` to load an IPSec rule before using this command.
`ipsec load <rule-number>`	Loads the specified IPSec rule for editing.
`ipsec save`	Saves the IPSec rule settings.
`ipsec config netbios active <on|off>`	Sets whether or not NetBIOS packets are allowed to pass through VPN tunnels.
`ipsec config name <name>`	Sets the rule's name (up to 32 characters).
`ipsec config active <Yes|No>`	Turns the rule on or off.
`ipsec config natTraversal <Yes|No>`	Turns NAT traversal on or off.
`ipsec config keepAlive <Yes|No>`	Turns keep alive on or off.
`ipsec config lcIdType <0:IP|1:DNS | 2:Email>`	Sets the local ID type.
`ipsec config lcIdContent <content>`	Sets the local ID content with the specified IP address, domain name, or e-mail address. Use up to 31 characters.
`ipsec config myIpAddr <ip-address>`	Sets the local VPN gateway with the specified IP address.
`ipsec config peerIdType <0:IP|1:DNS|2:Email>`	Sets the peer ID type.
`ipsec config peerIdContent <content>`	Sets the peer ID content with the specified IP address, domain name, or e-mail address. Use up to 31 characters.
`ipsec config secureGwAddr <ip-address|domain-name>`	Sets the remote gateway address with the specified IP address or domain name.
`ipsec config protocol <1:ICMP |6:TCP|17:UDP>`	Sets the traffic protocol that can trigger the VPN tunnel and be forwarded through it.
`ipsec config lcAddrType <0:single|1:range|2:subnet>`	Sets the address type for the local network.
`ipsec config lcAddrStart <ip-address>`	Sets the local network starting IP address.
`ipsec config lcAddrEndMask <ip-address>`	Sets the local network ending IP address for a range or the subnet mask for a subnet.
`ipsec config lcPortStart <port>`	Sets the starting port for local network traffic. Only traffic using the specified ports can go through the VPN tunnel.
`ipsec config lcPortEnd <port>`	Sets the ending port for local network traffic.
`ipsec config dynamicLocal <On|Off>`	Sets the local network IP address range to be dynamic (any).
`ipsec config rmAddrType <0:single|1:range|2:subnet>`	Sets the address type for the remote network.
`ipsec config rmAddrStart <ip-address>`	Sets the remote network starting IP address.
`ipsec config rmAddrEndMask <ip-address>`	Sets the remote network ending IP address for a range or the subnet mask for a subnet.
`ipsec config rmPortStart <port>`	Sets the starting port for remote network traffic. Only traffic using the specified ports can go through the VPN tunnel.
`ipsec config rmPortEnd <port>`	Sets the ending port for remote network traffic.
`ipsec config dynamicRemote <On|Off>`	Sets the remote network IP address range to be dynamic (any).

Table 34 IPSec Commands (continued)

COMMAND	DESCRIPTION
ipsec config dnsServer <*ip-address*>	Sets the DNS server IP address to assign to remote users.
ipsec config antiReplay <Yes|No>	Enables or disables the replay detection.
ipsec config keyManage <0:IKE|1:Manual>	Sets the rule to use IKE (ISAKMP) or manual key management.
ipsec config ike negotiationMode <0:Main | 1:Aggressive>	Sets the negotiation mode.
ipsec config ike authMethod <0:PreSharedKey|1:RSASignature>	Sets the authentication method.
ipsec config ike certificate <*certificate-name*>	Specifies the certificate the ZyXEL Device uses for authentication.
ipsec config ike preShareKey <*ascii*|0x*hex*>	Sets the pre-shared key. *ascii* | 0x*hex*: Enter characters in ASCII or in hexadecimal format. The minimum length is 8.
ipsec config ike p1EncryAlgo <0:DES|1:3DES|2:AES>	Sets the phase 1 encryption algorithm.
ipsec config ike p1EncryKeyLen <0:128|1:192|2:256	Sets the phase 1 encryption key length.
ipsec config ike p1AuthAlgo <0:MD5|1:SHA1>	Sets the phase 1 authentication algorithm.
ipsec config ike p1SaLifeTime <*seconds*>	Sets the phase 1 IPSec SA life time.
ipsec config ike p1KeyGroup <0:DH1|1:DH2>	Sets the phase 1 IKE SA key group.
ipsec config ike activeProtocol <0:AH|1:ESP>	Sets the active protocol.
ipsec config ike p2EncryAlgo <0:Null|1:DES|2:3DES|3:AES>	Sets the phase 2 encryption algorithm.
ipsec config ike p2EncryKeyLen <0:128|1:192|2:256	Sets the phase 2 encryption key length.
ipsec config ike p2AuthAlgo <0:MD5|1:SHA1>	Sets the phase 2 authentication algorithm.
ipsec config ike p2SaLifeTime <*seconds*>	Sets the phase 2 IPSec SA life time.
ipsec config ike encap <0:Tunnel|1:Transport>	Sets the encapsulation mode.
ipsec config ike pfs <0:None|1:DH1|2:DH2>	Sets Perfect Forward Secrecy for phase 2.
ipsec config manual activeProtocol <0:AH|1:ESP>	Sets the protocol the manual key rule uses.
ipsec config manual ah encap <0:Tunnel|1:Transport>	Sets the encapsulation mode when using AH protocol in the manual rule.
ipsec config manual ah spi <*decimal*>	Sets the SPI information when using AH protocol in the manual rule. *decimal*: The maximum length is 9.
ipsec config manual ah authAlgo <0:MD5|1:SHA1	Sets the authentication algorithm when using AH protocol in the manual rule.
ipsec config manual ah authKey <*ascii*>	Sets the authentication key when using AH protocol in the manual rule.

Table 34 IPSec Commands (continued)

COMMAND	DESCRIPTION
`ipsec config manual esp encap <0:Tunnel|1:Transport>`	Sets the encapsulation mode when using ESP protocol in the manual rule.
`ipsec config manual esp spi <decimal>`	Sets the SPI when using ESP protocol in the manual rule. *decimal*: The maximum length is 9.
`ipsec config manual esp encryAlgo <0:Null|1:DES|2:3DES>`	Sets the encryption algorithm when using ESP protocol in the manual rule.
`ipsec config manual esp encryKey <ascii>`	Sets the encryption key when using ESP protocol in the manual rule.
`ipsec config manual esp authAlgo <0:MD5|1:SHA1`	Sets the authentication algorithm when using ESP protocol in the manual rule.
`ipsec config manual esp authKey <ascii>`	Sets the authentication key when using ESP protocol in the manual rule.
`ipsec swSkipOverlapIp <on|off>`	Turn this on to send packets destined for overlapping local and remote IP addresses to the local network (you can access the local devices but not the remote devices). Turn this off to send packets destined for overlapping local and remote IP addresses to the remote network (you can access the remote devices but not the local devices.)
`ipsec adjTcpMss <off|auto|<1~1460>>`	The TCP packets are larger after VPN encryption. Packets larger than a connection's MTU (Maximum Transmit Unit) are fragmented. `auto`: Automatically set the Maximum Segment Size (MSS) of the TCP packets that are to be encrypted by VPN based on the encapsulation type. Recommended. `1-1460`: If fragmentation issues are affecting your network's throughput performance, you can manually specify a smaller MSS (in bytes).

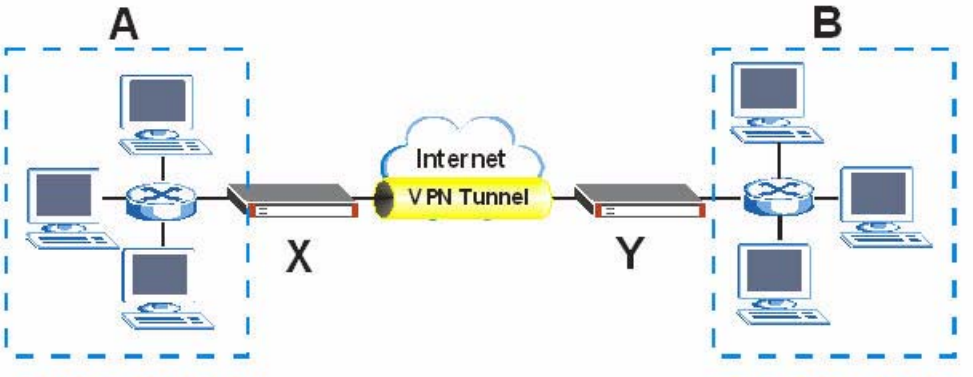
14.2 swSkipOverlapIp

Normally, you do not configure your local VPN policy rule's IP addresses to overlap with the remote VPN policy rule's IP addresses. For example, you usually would not configure both with 192.168.1.0. However, overlapping local and remote network IP addresses can occur in the following cases.

1 You configure a dynamic VPN rule for a remote site. (See Figure 1.)

For example, when you configure the ZyXEL Device X, you configure the local network as 192.168.1.0 and the remote network as any (0.0.0.0). The "any" includes all possible IP addresses. It will forward traffic from network A to network B even if both the sender (for example 192.168.1.8) and the receiver (for example 192.168.1.9) are in network A.

Figure 1 Dynamic VPN Rule I



Using the command `ipsec swSkipOverlapIp on` has ZyXEL Device X check if a packet's destination is also at the local network before forwarding the packet. If it is, the ZyXEL Device sends the traffic to the local network. Setting `ipsec swSkipOverlapIp` to `off` disables the checking for local network IP addresses.

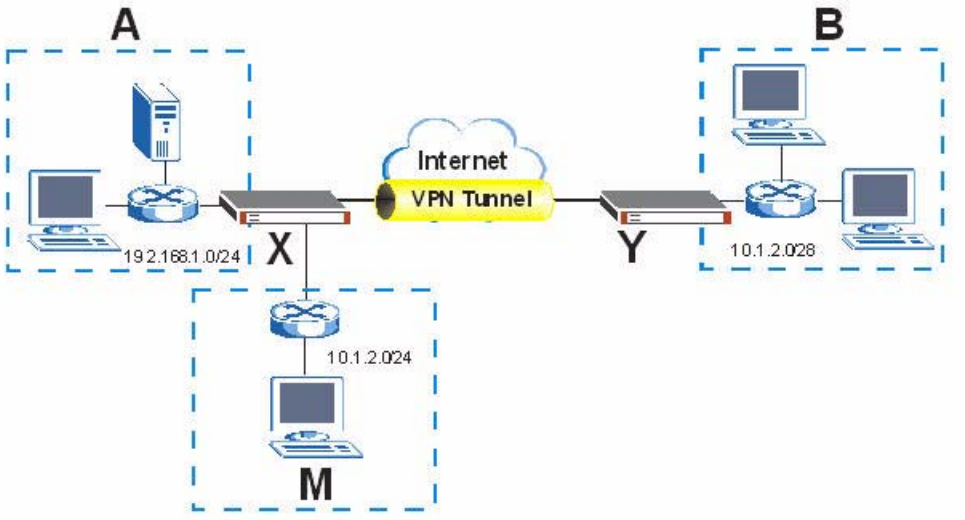
2 You configure an IP alias network that overlaps with the VPN remote network. (See Figure 2.)

For example, you have an IP alias network M (10.1.2.0/24) in ZyXEL Device X's LAN. For the VPN rule, you configure the VPN network as follows.

- Local IP address start: 192.168.1.1, end: 192.168.1.254
- Remote IP address start: 10.1.2.240, end: 10.1.2.254

IP addresses 10.1.2.240 to 10.1.2.254 overlap.

Figure 2 IP Alias



In this case, if you want to send packets from network A to an overlapped IP (ex. 10.1.2.241) that is in the IP alias network M, you have to set the `swSkipOverlapIp` command to `on`.

14.3 Command Examples

This example adds an IPSec rule as follows.

1. Load IPSec Rule Index: 2
2. Rule Name: VPN-ph1
3. Active
4. Local ID Type: IP
5. Local ID Content: 192.168.1.33
6. My IP Address: 10.1.1.1
7. Local Network Type: Range
8. Local Network Address Start: 192.168.1.33
9. Local Network Address End: 192.168.1.66
10. Secure Gateway Address: 10.1.1.2
11. Remote Network Type: Single
12. Remote Network Address Start: 172.16.1.3
13. Protocol: TCP
14. Key Management: IKE
15. Negotiation Mode: Main
16. Authentication Method: Pre-Shared Key
17. Pre-Shared Key: 12345678
18. Save

```
ras> ipsec load 2
ras> ipsec config name VPN-ph1
ras> ipsec config active Yes
ras> ipsec config natTraversal Yes
ras> ipsec config lcIdType IP
ras> ipsec config lcIdContent 192.168.1.33
ras> ipsec config myIpAddr 10.1.1.1
ras> ipsec config lcAddrType 1
ras> ipsec config lcAddrStart 192.168.1.33
ras> ipsec config lcAddrEndMask 192.168.1.66
ras> ipsec config secureGwAddr 10.1.1.2
ras> ipsec config rmAddrType 0
ras> ipsec config rmAddrStart 172.16.1.3
ras> ipsec config protocol 6
ras> ipsec config keyManage 0
ras> ipsec config ike negotiationMode 0
ras> ipsec config ike authMethod 0
ras> ipsec config ike preShareKey 12345678
ras> ipsec save
```

15

LAN Interface Commands

Use these commands to configure LAN interfaces on the ZyXEL Device.

15.1 Command Summary

The following section lists the commands for this feature.

Table 35 LAN Command Summary

COMMAND	DESCRIPTION
`lan active <yes|no>`	Enables or disables the LAN interface.
`lan clear`	Clears the working buffer for the specified configuration. Any unsaved changes are lost.
`lan dhcp mode <none|server|relay>`	Sets the DHCP mode.
`lan dhcp relay server <ip>`	Sets the IP address of the DHCP relay server.
`lan dhcp server dnsserver <dns-ip1> [<dns-ip2>]`	Sets the IP address of the DNS server assigned to DHCP clients on this interface.
`lan dhcp server gateway <ip>`	Sets the IP address of the default gateway assigned to DHCP clients on this interface.
`lan dhcp server leasetime <seconds>`	Specifies how long a device can use the same IP address before it needs to send a new request for an IP address.
`lan dhcp server netmask <netmask>`	Specifies the subnet mask assigned to DHCP clients by the ZyXEL Device.
`lan dhcp server pool <startip> <numip>`	Specifies the range of IP address for DHCP clients. *startip* - first IP address in the IP pool. *numip* - number of IP addresses in the IP pool.
`lan dhcp server rebindtime <seconds>`	Specifies the time interval from address assignment to the time the client transitions to rebinding state. A client in rebinding state broadcasts DHCP request messages.
`lan dhcp server renewaltime <seconds>`	Specifies the time interval from assigning an address assignment to the time the client transitions to renewing state. A client in renewing state can try to renew the IP address lease.
`lan display`	Displays the configuration details for the LAN interface being configured.
`lan filter <incoming|outgoing> <tcpip|generic> [1] [2] [3] [4]`	Applies the specified filter set to this interface. Filter sets can be configured via the `sys filter set` command. `1-4:` are the index numbers of filters configured via the `sys filter set` command.

Table 35 LAN Command Summary (continued)

COMMAND	DESCRIPTION
`lan index <interface>`	Sets the LAN interface for configuration. *interface*: type one of the following numbers • 1 - to select the main LAN interface; in CLI this interface is displayed as **enif0**. • 2 - to select IP Alias #1 interface; in CLI this interface is displayed as **enif0:0**. • 3 - to select IP Alias #2 interface; in CLI this interface is displayed as **enif0:1**. • 4 - to select the DMZ interface; in CLI this interface is displayed as **enif0:2**.
`lan ipaddr <ip> <mask>`	Sets the LAN interface's IP address and subnet mask.
`lan ippolicy <0-12>`	Applies the specified IP policy. “0” indicates no policy is applied. Policies can be configured via the `ip policyrouting set` command.
`lan multicast <none|igmpv1|igmpv2>`	Sets the multicast mode.
`lan rip <none|in|out|both> <rip1|rip2b|rip2m>`	Sets the RIP direction and mode.
`lan save`	Saves the LAN interface configuration in the working buffer to non-volatile memory. The working buffer is a volatile memory space. The settings in the working buffer are not applied to the ZyXEL Device until you execute this command.

15.2 Command Examples

This example sets the LAN IP address of the ZyXEL Device and specifies DHCP server settings on the LAN interface.

```
ras> lan index 1
enif0 is selected
ras> lan ipaddr 172.16.1.254 255.255.255.0
ras> lan dhcp mode server
ras> lan dhcp server gateway 172.16.1.254
ras> lan dhcp server pool 172.16.1.100 32
ras> lan dhcp server netmask 255.255.255.0
ras> lan dhcp server leasetime 3600
ras> lan display
Active: Yes
Interface: enif0
IP Address: 172.16.1.254
Subnet Mask: 255.255.255.0
RIP Direction: None
RIP Version: RIP-2B
Multicast: None
Protocol Filter Set:
Incoming:   0  0  0  0
Outgoing:   0  0  0  0
Device Filter Set:
Incoming:   0  0  0  0
Outgoing:   0  0  0  0
ras> lan save
lan: save ok
```

16

MyZyXEL.com Commands

Use these commands to configure user, product, or service registration settings on your ZyXEL Device. Your ZyXEL Device needs to connect to the registration server (the default is http://www.MyZyXEL.com).

Ensure your ZyXEL Device is connected to the Internet and the registration server before you use the following commands.

16.1 Command Summary

The following section lists the commands for this feature.

Table 36 sys myZyxelCom Commands

COMMAND	DESCRIPTION
`sys myZyxelCom checkUserName <username>`	Checks whether the specified user name exists or not in the myZyXEL.com database.
`sys myZyxelCom register <username> <password> <email> <countrycode>`	Sends the specified registration information to myZyXEL.com including user name, password, email, and country code. *<countrycode>*: This is a number that represents the country you are from. Refer to table Table 37 on page 100.
`sys myZyxelCom trialService <service>`	Activates the trial services to myZyXEL.com. *<service>*: 1: Content Filtering (CF)
`sys myZyxelCom serviceUpgrade <licence key>`	Registers a license key to myZyXEL.com.
`sys myZyxelCom serviceRefresh`	Gets up-to-date service status from the myZyXEL.com database.
`sys myZyxelCom display`	Displays the ZyXEL Device's registration information.
`sys myZyxelCom serviceDisplay`	Displays the service status (including the expiration date if the service is already activated).

16.2 Country Codes

The following section lists the relationship between countries and country codes defined in the ZyXEL Device.

Table 37 Country Codes

COUNTRY NAME	COUNTRY CODE
AFGHANISTAN	1
ALBANIA	2
ALGERIA	3
AMERICA	4
ANDORRA	5
ANGOLA	6
ANGUILLA	7
ANTARTICA	8
ANTIGUA_AND_BARBUDA	9
ARGENTINA	10
ARMENIA	11
ARUBA	12
ASCENSION_ISLAND	13
AUSTRALIA	14
AUSTRIA	15
AZERBAIJAN	16
BAHAMAS	17
BAHRAIN	18
BANGLADESH	19
BARBADOS	20
BELARUS	21
BELGIUM	22
BELIZE	23
BENIN	24
BERMUDA	25
BHUTAN	26
BOLIVIA	27
BOSNIA_AND_HERZEGOVINA	28
BOTSWANA	29
BOUVET_ISLAND	30
BRAZIL	31
BRITISH_INDIAN_OCEAN_TERRITORY	32
BRUNEI_DARUSSALAM	33
BULGARIA	34
BURKINA_FASO	35

Table 37 Country Codes (continued)

COUNTRY NAME	COUNTRY CODE
BURUNDI	36
CAMBODIA	37
CAMEROON	38
CANADA	39
CAPE_VERDE	40
CAYMAN_ISLANDS	41
CENTRAL_AFRICAN_REPUBLIC	42
CHAD	43
CHILE	44
CHINA	45
CHRISTMAS_ISLAND	46
COCOS_KEELING_ISLANDS	47
COLOMBIA	48
COMOROS	49
CONGO_DEMOCRATIC_REPUBLIC_OF_THE	50
CONGO_REPUB_IC_OF	51
COOK_ISLANDS	52
COSTA_RICA	53
COTE_D	54
CROATIA_HRVATSKA	55
CYPRUS	56
CZECH_REPUBLIC	57
DENMARK	58
DJIBOUTI	59
DOMINICA	60
DOMINICAN_REPUBLIC	61
EAST_TIMOR	62
ECUADOR	63
EGYPT	64
EL_SALVADOR	65
EQUATORIAL_GUINEA	66
ERITREA	67
ESTONIA	68
ETHIOPIA	69
FALKLAND_ISLANDS_MALVINA	70
FAROE_ISLANDS	71
FIJI	72
FINLAND	73

Table 37 Country Codes (continued)

COUNTRY NAME	COUNTRY CODE
FRANCE	74
FRANCE_METROPOLITAN	75
FRENCH_GUIANA	76
FRENCH_POLYNESIA	77
FRENCH_SOUTHERN_TERRITORIES	78
GABON	79
GAMBIA	80
GEORGIA	81
GERMANY	82
GHANA	83
GIBRALTAR	84
GREAT_BRITAIN	85
GREECE	86
GREENLAND	87
GRENADA	88
GUADELOUPE	89
GUAM	90
GUATEMALA	91
GUERNSEY	92
GUINEA	93
GUINEA_BISSAU	94
GUYANA	95
HAITI	96
HEARD_AND_MCDONALD_ISLANDS	97
HOLY_SEE_CITY_VATICAN_STATE	98
HONDURAS	99
HONG_KONG	100
HUNGARY	101
ICELAND	102
INDIA	103
INDONESIA	104
IRELAND	105
ISLE_OF_MAN	106
ITALY	107
JAMAICA	108
JAPAN	109
JERSEY	110
JORDAN	111

Table 37 Country Codes (continued)

COUNTRY NAME	COUNTRY CODE
KAZAKHSTAN	112
KENYA	113
KIRIBATI	114
KOREA_REPUBLIC_OF	115
KUWAIT	116
KYRGYZSTAN	117
LAO_PEOPLE's_DEMOCRATIC_REPUBLIC_OF	118
LATVIA	119
LEBANON	120
LESOTHO	121
LIBERIA	122
LIECHTENSTEIN	123
LITHUANIA	124
LUXEMBOURG	125
MACAU	126
MACEDONIA_FORMER_YUGOSLAV_REPUBLIC	127
MADAGASCAR	128
MALAWI	129
MALAYSIA	130
MALDIVES	131
MALI	132
MALTA	133
MARSHALL_ISLANDS	134
MARTINIQUE	135
MAURITANIA	136
MAURITIUS	137
MAYOTTE	138
MEXICO	139
MICRONESIA_FEDERAL_STATE_OF	140
MOLDOVA_REPUBLIC_OF	141
MONACO	142
MONGOLIA	143
MONTSERRAT	144
MOROCCO	145
MOZAMBIQUE	146
NAMIBIA	147
NAURU	148
NEPAL	149

Table 37 Country Codes (continued)

COUNTRY NAME	COUNTRY CODE
NETHERLANDS	150
NETHERLANDS_ANTILLES	151
NEW_CALEDONIA	152
NEW_ZEALAND	153
NICARAGUA	154
NIGER	155
NIGERIA	156
NIUE	157
NORFOLK_ISLAND	158
NORTHERN_MARIANA_ISLANDS	159
NORWAY	160
NOT_DETERMINED	161
OMAN	162
PAKISTAN	163
PALAU	164
PANAMA	164
PAPUA_NEW_GUINEA	166
PARAGUAY	167
PERU	168
PHILIPPINES	169
PITCAIRN_ISLAND	170
POLAND	171
PORTUGAL	172
PUERTO_RICO	173
QATAR	174
REUNION_ISLAND	175
ROMANIA	176
RUSSIAN_FEDERATION	177
RWANDA	178
SAINT_KITTS_AND_NEVIS	179
SAINT_LUCIA	180
SAINT_VINCENT_AND_THE_GRENADINES	181
SAN_MARINO	182
SAO_TOME_AND_PRINCIPE	183
SAUDI_ARABIA	184
SENEGAL	185
SEYCHELLES	186
SIERRA_LEONE	187

Table 37 Country Codes (continued)

COUNTRY NAME	COUNTRY CODE
SINGAPORE	188
SLOVAK_REPUBLIC	189
SLOVENIA	190
SOLOMON_ISLANDS	191
SOMALIA	192
SOUTH_AFRICA	193
SOUTH_GEORGIA_AND_THE_SOUTH_SANDWICH_ISLANDS	194
SPAIN	195
SRI_LANKA	196
ST_PIERRE_AND_MIQUELON	197
ST_HELENA	198
SURINAME	199
SVALBARD_AND_JAN_MAYEN_ISLANDS	200
SWAZILAND	201
SWEDEN	202
SWITZERLAND	203
TAIWAN	204
TAJIKISTAN	205
TANZANIA	206
THAILAND	207
TOGO	208
TOKELAU	209
TONGA	210
TRINIDAD_AND_TOBAGO	211
TUNISIA	212
TURKEY	213
TURKMENISTAN	214
TURKS_AND_CAICOS_ISLANDS	215
TUVALU	216
US_MINOR_OUTLYING_ISLANDS	217
UGANDA	218
UKRAINE	219
UNITED_ARAB_EMIRATES	220
UNITED_KINGDOM	221
UNITED_STATES	222
URUGUAY	223
UZBEKISTAN	224
VANUATU	225

Table 37 Country Codes (continued)

COUNTRY NAME	COUNTRY CODE
VENEZUELA	226
VIETNAM	227
VIRGIN_ISLANDS_BRITISH	228
VIRGIN_ISLANDS_USA	229
WALLIS_AND_FUTUNA_ISLANDS	230
WESTERN_SAHARA	231
WESTERN_SAMOA	232
YEMEN	233
YUGOSLAVIA	234
ZAMBIA	235
ZIMBABWE	236

16.3 Command Examples

This example displays your ZyXEL Device's registration information.

```
ras> sys myZyxelCom display

register server address : www.myzyxel.com
register server path : /register/registration?

username : aseawfasf
password : aaaaaa

email : aa@aa.aa.aa

sku : CFRT=1&CFST=319&ZASS=469&ISUS=469&ZAVS=469

country code : 204

register state 1

register MAC : 0000AA220765
CF expired day : 2008-05-26 14:58:19
2In1 expired day : 2008-10-23 14:58:19
Last update day : 2007-07-12 14:58:19
```

Table 38 sys myZyxelCom display Commands

FIELD NAME	DESCRIPTION
`register server address`	Displays the URL of the registration server.
`register server path`	Displays the path storing your ZyXEL Device's registration information on the registration server.
`username`	Displays the registered username.

Table 38 sys myZyxelCom display Commands

FIELD NAME	DESCRIPTION
password	Displays the registered password.
email	Displays the registered e-mail address.
sku	This is a string the registration server uses to validate your ZyXEL Device.
country code	Displays the registered country code.
register state	Displays whether the ZyXEL Device has completed the product registration. 1: Yes 0: No
register MAC	Displays the MAC address of the ZyXEL Device. This is also the unique MAC address used for product registration on the registration server.
CF expired day	Displays the due date that you can use the Content Filter service on this ZyXEL Device.
2In1 expired day	Displays the due date that you can use the Anti Virus service on this ZyXEL Device.
Last update day	Displays the most recent date that you updated the signatures for all services including CF and AV.

This example displays the detailed service registration information of your ZyXEL Device.

```
ras> sys myZyxelCom serviceDisplay
Content Filter Service :
Actived, Licenced, Trial, Expired : 2007-07-08 16:36:15
ras>
```

Table 39 sys myZyxelCom serviceD Commands

FIELD NAME	DESCRIPTION
Content Filter Service	This is the service name.
Actived Non-actived	Displays if the service is enabled or not. If the server has not activated yet, it just displays non-actived without further information as following fields.
Licence Expired	Displays the service status.
Trial Standard	Displays the service license type.
Expired : <date>	Displays the expiration date of the service.

17

Quality of Service (QoS)

Use these commands to configure QoS settings on the ZyXEL Device.

17.1 Command Summary

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

Table 40 QoS Command Input Values

LABEL	DESCRIPTION
interface	The QoS interface name includes `lan`, `wan`, `dmz`, and `wlan`. The interfaces to which you can apply QoS vary by ZyXEL Device model.
class-name	This is a class name. Enter a descriptive name of up to 20 alphanumeric characters, including spaces.
class-number	This is a class number (from 0 to 99).

The following section lists the commands for this feature.

Table 41 QoS Commands

COMMAND	DESCRIPTION
`qos active [on|off]`	Enables or disables QoS.
`qos class <`*interface*`> <add|mod> <`*class-number*`> [name <`*class-name*`>] [priority <0~7> | priority auto]`	Adds or modifies a class for the specified interface. `add|mod`: Add or modify the class. `priority`: Sets the class priority ranging from 0 (the lowest) to 7 (the highest). `priority auto`: Sets the ZyXEL Device to map the matched traffic to a queue according to the internal QoS mapping table.
`qos class <`*interface*`> del <`*class-number*`>`	Removes the specified class from the specified interface.
`qos config <save|load|clear>`	Loads, saves or clears QoS configuration from/to the permanent memory.

Table 41 QoS Commands (continued)

COMMAND	DESCRIPTION
qos filter <*interface*> add <*class-number*> [service <*service-type*>] [dip [not] <*dst-ip*> <*dst-ip-mask*>] [dport [not] <*dst-port-start*> <*dst-port-end*>] [sip [not] <*src-ip*> <*src-ip-mask*>] [sport [not] <*src-port-start*> <*src-port-end*>] [proto [not] <*protocol*>] [dscp [not] <*dscp*>] [size [not] <*min-ip-length*> <*max-ip-length*>] [dmac [not] <*dst-mac*> <*dst-mac-mask*>] [smac [not] <*src-mac*> <*src-mac-mask*>] [vid [not] <*vlan-id*>] [vpri [not] <*priority*>] [portid [not] <*lan-port-id*>] [pvcid [not] <*pvc-id*>]	Adds a new QoS filter for the specified interface. *service-type*: Sets the type of application (**sip** or **ftp**). *dst-ip*: Enters the destination IP address. *dst-ip-mask*: Enters the destination subnet mask. *dst-port-start*: Enters the first of the contiguous port number of the destination. *dst-port-end*: Enters the last of the contiguous port number of the destination. *src-ip*: Enters the source IP address. *src-ip-mask*: Enters the source subnet mask. *src-port-start*: Enters the first of the contiguous port number of the source. *src-port-end*: Enters the last of the contiguous port number of the source. *protocol*: Enters the number of the protocol type (the protocol field in the IP header). For example 1 for ICMP, 6 for TCP, and 17 for UDP. *dscp*: Specifies a DSCP number between 0 and 63. *min-ip-length*: Enters the minimum packet length (from 28 to 1500). *max-ip-length*: Enters the maximum packet length (from 28 to 1500). *dst-mac*: Enters destination MAC address. *dst-mac-mask*: Types the mask for the MAC address. *src-mac*: Enters the source MAC address. *src-mac-mask*: Types the mask for the MAC address. *vlan-id*: Specifies a VLAN ID number between 2 and 4094. *priority*: Sets the class priority ranging from 0 (the lowest) to 7 (the highest). *lan-port-id*: Enters a LAN port number. *pvc-id*: Enters a remote node number.
qos filter <*interface*> del <*class-number*>	Deletes a filter for class # in the specified interface.
qos filter <*interface*> <enable|disable> <*class-number*>	Disables or enables a filter for class # in the specified interface.
qos filter <*interface*> order <*class-number*> <*new-order*>	Changes the QoS filter ordering. The ordering of your rules is important as rules are applied in turn.
qos filter <*interface*> index <*class-number*> <*save-index*>	Changes the index number of a QoS filter in TR-069. *save-index*: Enters the new index number from 1 to 30.
qos filter show	Displays all filters settings.
qos policer <*index*> <enable|disable>	Disables or enables the specified policer. *index*: Enters the index number (from 1 to 10) of the policer.
qos policer <*index*> set <*bandwidth* (kbps)> [<*size (bytes)*> <*meter-type*> <*conforming-act*> <*non-conforming-act*>]	Sets the bandwidth policer settings.
qos policer <*index*> show	Displays the specified policer settings.
qos policer show	Displays all policers settings.

Table 41 QoS Commands (continued)

COMMAND	DESCRIPTION
qos policy <*interface*> <*class-number*> [clear] [dscp <same|auto> | dscp mark <*dscp*>] [vlan <same|auto|remove> | vlan <mark|add> <*vlan-id*> <*priority*>] [route rn <*remote-node-number*> | route gw <*gateway-ip*>] [policer <*policer-number*>]	Sets a QoS policy for the specified interface and class.
qos priq <*interface*> <enable|disable>	Turns on or off the auto priority mapping on the specified interface.
qos priq <*interface*> mon	Displays the specified QoS packet statistics. Enter this command again to stop it.
qos priq <*interface*> set <0|1> <0|1> <0|1>	Sets whether the ZyXEL Device assigns priority to unmatched traffic based on the IEEE 802.1p priority level, IP precedence and/or packet length.
qos priq <*interface*> show	Displays auto priority mapping settings on the specified interface.
qos queue <*index*> <enable|disable>	Disables or enables the specified queue. *index*: Enters the index number (from 1 to 24) of the QoS queue.
qos queue <*index*> reset inerface <lan|wlan|wan> [drop <dt|red>] [priority <*priority*>] [weight <*weight*>] [rate <*rate kbps*>] [size <*burst-size bytes*>] [redt <*red threshold (%)*>] [redp <*red percentage (%)*>]	Changes the specified queue settings.
qos queue <*index*> show	Displays the specified queue settings.
qos queue show	Displays all queue settings.
qos show class <*interface*> <*class-number*>	Displays QoS class settings for the specified class in the specified interface.
qos show filter <*interface*>	Displays filter settings for the specified interface.
qos tbr <*interface*> <enable|disable>	Disables or enable TBR (Token Bucket Regulator) in the specified interface.
qos tbr <*interface*> set <*bandwidth*> [<*size*>]	Changes the specified interface's TBR settings. *bandwidth*: Sets the bandiwdth (in kbps) from 1 to 100M. *size*: Sets the burst size (in bytes) from 0 to 100kB.
qos tbr <*interface*> show	Displays Token Bucket Regulator settings for the specified interface.

17.2 Command Examples

This example configures QoS at the interface level. It does the following.

1. Turns on QoS on the ZyXEL Device.
2. Enable auto priority mapping on the WLAN interface.
3. Sets the ZyXEL Device to assign priority to unmatched traffic based on the IEEE 802.1p priority level, IP precedence and packet length on the WLAN interface.

4 Displays the WLAN interface's auto priority mapping settings.

```
ras> qos active on
ras> qos priq wlan enable
ras> qos priq wlan set 1 1 1
ras> qos priq wlan show
================================================================================
Interface:   WLAN               [Enabled]
     Auto priority mapping
     1. Ethernet Priority:      [ ON]
     2. IP Precedence:          [ ON]
     3. Packet Size:            [ ON]
================================================================================
ras>
```

This example adds one WLAN class using the following settings (and then displays it).

- Class number: 1
- Class name: WLAN-class1
- Priority: auto

```
ras> qos class wlan mod 1 name WLAN-class1 priority auto
Class setting is done.
ras> qos show class wlan 1
================================================================================
 Class 1          Name: WLAN-class1
              Priority: AUTO
          Route policy: NONE
           DSCP policy: NONE
           VLAN policy: NONE
            BW policer: NONE
        Filter setting: NONE
================================================================================
ras>
```

This example adds a filter on the WLAN class using the following settings.

- Class number: 1
- Service: FTP
- Destination address: 172.16.1.208
- Source port: Any
- Source address: Any
- Destination address: Any
- Destination port: Any

- Protocol: Any.

```
ras> qos filter wlan add 1 service ftp dip 172.16.1.208 255.255.255.0
Filter setting is done.
ras> qos show filter wlan 1
================================================================================
        Class  1                WLAN-class1
        Filter Enabled:         Yes
        Classification Order:   0
        Classification Index:   1
        Special for Service:    FTP
        Destination IP/Mask:    172.16.1.208/255.255.255.0
        Class Queue:            AUTO
================================================================================
ras>
```

This example adds and enables a bandwidth policer on the ZyXEL Device using the following settings.

- Class number: 1
- Bandwidth: 10 Mbps

This example also adds a policy on the WLAN class using the following settings, applies the pre-configured bandwidth policer to this policy, and then displays the class and filter settings.

- Class number: 1
- 802.1q tagging: keep the priority setting and VLAN ID of the frames.
- Bandwidth policer number: 1

```
ras> qos policer 1 set bandwidth 10000
ras> qos policer 1 enable
ras> qos policy wlan 1 vlan same policer 1
tpModifyClassPolicy is completed.
ras> qos show filter wlan 1
================================================================================
        Class  1                WLAN-class1
        Filter Enabled:         Yes
        Classification Order:   0
        Classification Index:   1
        Special for Service:    FTP
        Destination IP/Mask:    172.16.1.208/255.255.255.0
        Class Queue:            AUTO
        VLAN policy:            MARK    VLAN ID: 123    Priority: 1
        Bandwidth policer:      1
================================================================================
ras> qos show class wlan 1
================================================================================
 Class 1          Name: WLAN-class1
              Priority: AUTO
          Route policy: NONE
           DSCP policy: NONE
           VLAN policy: MARK    VLAN ID: 123    Priority: 1
            BW policer: 1
        Filter setting: YES
================================================================================
ras>
```

18

RADIUS Commands

Use these commands to view RADIUS authentication or accounting configuration settings on the ZyXEL Device. See the `wlan radius` commands in Chapter 22 on page 175 for configuration details.

18.1 Command Summary

The following section lists the commands for this feature.

Table 42 radius Command Summary

COMMAND	DESCRIPTION
`radius auth`	Displays current RADIUS authentication server configuration.
`radius acct`	Displays current RADIUS accounting server configuration.

18.2 Command Examples

This example displays the RADIUS authentication server settings configured on the ZyXEL Device.

```
ras> radius auth
authentication server:   non-active
                IP   :   172.16.1.201
                Port :   1844
                Key  :   asdfkjas123
```

19

System Commands

Use these commands to configure system related settings on the ZyXEL Device.

19.1 Command Summary

The following section lists the commands for this feature.

The following table describes input values for some of the `sys` commands. Other values are discussed with the corresponding commands.

Table 43 sys Command Input Values

LABEL	DESCRIPTION
community	The SNMP community (or password).
compare-type	Describes the result of a comparison of a packet field with that specified in a rule. There are four possible values: `0:None` -Do not compare the packet field with that specified in the rule. `1:Equal` -The packet field value is the same as that specified in the rule. `2:NotEqual` -The packet field value is not the same as that specified in the rule. `3:Less` -The packet field value is less than that specified in the rule. `4:Greater` -The packet field value is greater than that specified in the rule.
filter-action	Sets the action when a filter set is checking a packet. The options are: `forward:` This forwards the packet to its destination. `drop:` This drops the packet. `checknext:` Sets the filter to check the next rule. Use this option if the packet must be checked against more than one rule.
groupid	The number of a tripleplay port-interface group mapping policy.
interface	An interface on the ZyXEL Device. These are usually as follows: `enif0`: LAN `enif1`: WAN `wanif0`: PPPoE If the device supports WLAN then: `enif1`: WLAN `enif2`: WAN
mail-address	An e-mail address
password	<32 ASCII characters
ports	A list of port numbers.
protocol#	0 = ICMP, 6 = TCP, 17 = UDP

Table 43 sys Command Input Values (continued)

LABEL	DESCRIPTION
rule#	Each set contains 6 rules. Rules are either TCP/IP or generic. A TCP/IP based rule contains the following subfields: Active: <yes|no> IP Protocol: <*protocol#*> IP Source Route: <yes|no> Destination IP Address: <*dest-ip*> Destination IP Mask: <*dest-mask*> Destination port: <*dest-port*> Destination port compare type: <*compare-type*> Source IP Address: <*dest-ip*> Source IP Mask: <*dest-mask*> Source port: <*dest-port*> Source port compare type: <*compare-type*> TCP/IP estab: <yes|no> More: <yes|no> Log: [none|match|notmatch|both] Action Matched: <*filter-action*> Action Not Matched: <*filter-action*> A generic rule contains the following subfields: Active: <yes|no> Offset: <*offset*> Length: <*length*> Mask: <*data-mask*> Value: <*value*> More: <yes|no> Log:[none|match|notmatch|both] Action Matched: <*filter-action*> Action Not Matched: <*filter-action*>
service	telnet|ftp|http|https|snmp|dns|icmp
session#	Refers to Temporarily Open Sessions (TOS).
set#	There are 12 filter sets.
ssid	The SSID of a wireless network.
timeout	This is a number between 1-65535 seconds.

Table 44 sys Commands

COMMAND	DESCRIPTION
sys adjtime	Retrieves the date and time from the Internet.
sys adminPassword <*password*>	Changes the administrator password.
sys atmu	Shows the multi-boot version.
sys atsh	Displays system information, including hardware and firmware details.
sys countrycode [*country-code*]	Sets or displays the country code. See Table 37 on page 100 for the country codes.
sys cpu display	Displays the CPU utilization.
sys date	Sets or displays the current date in year/month/date format.
sys datetime period [*day*]	Sets or displays the time period (in days) for how often the ZyXEL Device synchronizes with the time server.
sys ddns config active [0|1]	Activates or deactivates dynamic DNS.

Table 44 sys Commands (continued)

COMMAND	DESCRIPTION
`sys ddns config emailaddress <mail-address>`	Sets your email address. First allocate memory by using `sys ddns config load.`
`sys ddns config hostname <domain-name>`	Sets the domain name provided by your ISP. First allocate memory by using `sys ddns config load.`
`sys ddns config load`	Loads dynamic DNS to the working buffer for configuration and use.
`sys ddns config password <password>`	Sets the password. (This command may not be supported in your ZyXEL Device.) First allocate memory by using `sys ddns config load.`
`sys ddns config save`	Saves the dynamic DNS settings to non-volatile memory.
`sys ddns config username <username>`	Sets the DDNS user name (<32 ASCII characters). This command may not be supported in your ZyXEL Device.
`sys ddns debug <level>`	Enables or disables DDNS debug mode.
`sys ddns display <interface>`	Displays DDNS information for the specified interface, including DDNS status and connection details.
`sys ddns logout <interface>`	This logs out DDNS on the specified interface. This should be a WAN interface.
`sys ddns restart <interface>`	Restarts DDNS on the specified interface. This should be a WAN interface.
`sys default`	Resets the device to its default values, except for LAN settings which are reserved. If default LAN settings are also required, use `sys romreset`.
`sys diag`	Displays the system version, CPU usage, and mbuf status. mbuf is the memory buffer used to store network packets.
`sys display`	Displays system information on the hostname, location and system modes.
`sys domainname [domain-name]`	Sets or displays the domain name.
`sys edit <file-name>`	Edits the system preset text files such as autoexec.net.
`sys feature`	Displays information on available features.
`sys filter clear`	Remove the filter statistics.
`sys filter disp`	Shows the filter statistics.
`sys filter netbios config <0|1|2|3|4><on|off>`	Turns the netbios filter on or off for the specified traffic. 0:Between LAN and WAN 1:Between LAN and DMZ 2:Between WAN and DMZ 3:IPSec passthrough 4:Trigger Dial For options 1-3, on = `block`, `off` = `forward.` For option 4, `on` = `enable`, `off` = `disable.` If your device does not support DMZ then options 1 and 2 will not be available.
`sys filter netbios display`	Displays the netbios filter status.
`sys filter set actmatch [filter-action]`	Sets the action to be performed when a packet matches the set description.
`sys filter set actnomatch [filter-action]`	Sets the action to be performed when a packet does not match the set description.

Table 44 sys Commands (continued)

COMMAND	DESCRIPTION
`sys filter set clear [set#]`	This clears the specified set entry.
`sys filter set destip [dest-ip][mask]`	Sets the destination IP address and subnet mask of the set description. TCP/IP rules only.
`sys filter set destport [dest-port][compare-type]`	Sets the destination port and compare type. TCP/IP rules only.
`sys filter set disable`	Disables the rule. You need to specify which set to disable by first using `sys filter set index [set#][rule#]`.
`sys filter set display`	Displays buffer information.
`sys filter set display [set#] [rule#]`	Displays filter set information on the specified rule.
`sys filter set enable`	Enables a rule. You need to specify which set to enable by first using `sys filter set index [set#][rule#]`.
`sys filter set freememory`	Discards changes and frees the working buffer. Use this command before specifying a set to configure using `sys filter set index [set#][rule#]`.
`sys filter set index [set#][rule#]`	Sets the index of the filter set rule to be configured. You need to do this before configuring a rule.
`sys filter set length [length]`	Sets the length value for the generic filter. Use `sys filter set type generic` to set the set type to generic first before applying this rule. *length*: This value describes the number of sequential bits in a packet to be examined for pattern-matching as specified in a rule. The range for this value is 0-8. Use `sys filter set offset [offset]` to specify the first bit to be examined. Generic rules only.
`sys filter set log [none|match|notmatch|both]`	Sets a log depending on whether a packet matches the set description. `none:` No packets will be logged. `match:` Only packets that match the rule will be logged. `notmatch:` Only packets that do not match the rule will be logged. `both:` All packets will be logged.
`sys filter set mask [data-mask]`	Sets the mask to be applied to the packet data (delimited by the offset and length values) before comparing it with the generic rule. *data-mask:* Enter this value in hexadecimal notation. Generic rules only.
`sys filter set more [yes|no]`	Sets the filter to check the next rule or not. If this is enabled then `sys filter actmatch` and `sys filter actnomatch` commands are ignored.
`sys filter set name [set#][set-name]`	Sets the name of a filter set.
`sys filter set offset [offset]`	Sets the offset value for the generic filter. Use `sys filter set type generic` to set the set type to generic first before applying this rule. *offset:* This value describes after which bit in a packet the filter begins to search for a sequence of bits as specified in a rule. For example, enter “2” to begin pattern matching at the third bit. The range for this value is 0-255. Generic rules only.

Table 44 sys Commands (continued)

COMMAND	DESCRIPTION
`sys filter set protocol [protocol#]`	Sets the rule to match a specified protocol. 0 sets the rule to match any protocol. TCP/IP rules only.
`sys filter set save`	Saves the set's configuration.
`sys filter set sourceroute [yes|no]`	Enables or disables the filtering of packets based on whether their sourceroute option is enabled or not. TCP/IP rules only.
`sys filter set srcip [source-ip][mask]`	Sets the source IP address and subnet mask of the set. TCP/IP rules only.
`sys filter set srcport [source-port][compare-type]`	Sets the source port and compare type. TCP/IP rules only.
`sys filter set tcpestab [yes|no]`	`yes` sets the rule to match packets that request a TCP/IP connection. `no` sets the rule to ignore this behavior. TCP/IP rules only.
`sys filter set type [tcpip|generic]`	Sets the type of filter rule. `tcpip`: Choose TCP/IP filtering to filter packets based on source and destination IP address, destination port and protocol. `generic`: Choose generic filtering to filter packets based on bit pattern matching.
`sys filter set value [value]`	Sets the value of the data to be compared with the packet data delimited by the offset and length values. *value*: Enter this three byte value in hexadecimal notation, e.g., F:F:F. Generic rules only.
`sys filter sw`	Turns on or off the filtering counter switch.
`sys firewall`	See Chapter 12 on page 67 for details on the these commands.
`sys general bridge <on|off>`	Enables or disables system bridging.
`sys general contactname [contact-name]`	Sets the contact person's name.
`sys general display`	Displays general system configuration information, including hostname. domain name. location, contact details and system mode.
`sys general domainname [domain-name]`	Sets the domain name.
`sys general hostname [host-name]`	Sets the system name.
`sys general load`	Loads general system information into the buffer.
`sys general location [location]`	Sets the geographical location of your device.
`sys general routip <on|off>`	Enables or disables system routing.
`sys general save`	Saves general information to non-volatile memory.
`sys hostname [hostname]`	Sets or displays the system hostname.
`sys logs category 8021.x [0:none|1:log]`	Activates or deactivate logging for IEEE 802.1X authentication requests.
`sys logs category access [0:none|1:log|2:alert|3:both]`	Sets whether a log and/or an alert is made for requests for access.
`sys logs category anyip [0:none|1:log]`	Enables or disables recording of AnyIP logs and/or sending an alert.

Table 44 sys Commands (continued)

COMMAND	DESCRIPTION
`sys logs category attack [0:none|1:log|2:alert|3:both]`	Enables or disables recording of firewall attack logs and/or sending an alert.
`sys logs category display`	Displays the log settings for the categories of logs. Log settings for Blocked Java can only be configured via the GUI.
`sys logs category error [0:none|1:log|2:alert|3:both]`	Enables or disables recording system errors and/or sending an alert.
`sys logs category fsm [0:none|1:log]`	Enables or disables recording VoIP related FSM (Finite State Machine) logs.
`sys logs category ike [0:none|1:log|2:alert|3:both]`	Enables or disables recording IKE logs and/or sending an alert.
`sys logs category ipsec [0:none|1:log|2:alert|3:both]`	Enables or disables recording IPSec logs and/or sending an alert.
`sys logs category mten [0:none|1:log]`	Enables or disables recording system maintenance logs.
`sys logs category pki [0:none|1:log|2:alert|3:both]`	Enables or disables recording certificate logs and/or sending an alert. [0:hides show debug type|1:shows debug type]
`sys logs category sip [0:none|1:log]`	Enables or disables recording SIP logs.
`sys logs category tls [0:none|1:log|2:alert|3:both]`	Enables or disables recording TLS (HTTPS) logs and/or sending an alert.
`sys logs category traffic [0:none|1:log]`	Enables or disables recording traffic logs. This command is not available in the P-2602HWL Series.
`sys logs category upnp [0:none|1:log]`	Enables or disables recording UPnP logs.
`sys logs category urlblocked [0:none|1:log|2:alert|3:both]`	Enables or disables recording blocked web access logs and/or sending an alert.
`sys logs category urlforward [0:none/1:log]`	Enables or disables recording web forward logs.
`sys logs clear`	Clears all logs.
`sys logs display [access|attack|error|ipsec|ike|javablocked|pki|mten|tls|urlblocked|urlforward|upnp]`	Displays all logs or specific categories of logs.
`sys logs errlog clear`	Clears error logs.
`sys logs errlog display`	Displays error logs.
`sys logs errlog online`	Enables or disables the error log online display.
`sys logs load`	Loads the log setting buffer. Use this command before you configure the log settings. Use `sys logs save` after you configure the log settings.
`sys logs mail alertAddr [`*`mail-address`*`]`	Sets the email address to which the ZyXEL Device sends alerts.
`sys logs mail auth <0:enable|1:disable>`	Enables or disables SMTP (Simple Mail Transfer Protocol) authentication.
`sys logs mail display`	Displays the settings for e-mailing logs, including the SMTP server, and e-mail and identification details.

Table 44 sys Commands (continued)

COMMAND	DESCRIPTION
`sys logs mail logAddr [mail-address]`	Sets or displays the e-mail address to send logs to.
`sys logs mail passwd [smtp-user-password]`	Sets the SMTP authentication password.
`sys logs mail port [port]`	Sets the port number for sending log e-mails.
`sys logs mail schedule display`	Displays the log email schedule, including day and time and whether an immediate alert is required.
`sys logs mail schedule hour <0-23>`	Sets the hour to send the logs.
`sys logs mail schedule minute <0-59>`	Sets the minute to send the logs.
`sys logs mail schedule policy <0:full|1:hourly|2:daily|3:weekly|4:none>`	Sets how often the ZyXEL Device sends log e-mails.
`sys logs mail schedule week <0:sun|1:mon|2:tue|3:wed|4:thu|5:fri|6:sat>`	Sets the day of the week to send the e-mail log.
`sys logs mail sendmail`	Immediately sends a log by e-mail.
`sys logs mail server <domain-name|ip-address>`	Specifies the server name or the IP address of the mail server for the e-mail address specified as the mail sender.
`sys logs mail subject <mail-subject>`	Specifies the title in the subject line of the diagnostic e-mail message that the ZyXEL Device sends.
`sys logs mail user [smtp-username]`	Specifies (or displays) the user name (up to 31 characters) for the e-mail account the ZyXEL Device uses for e-mailing logs.
`sys logs save`	Saves the log settings to long term memory.
`sys logs syslog active [0:no|1:yes]`	Enables or disables the UNIX syslog.
`sys logs syslog display`	Displays the syslog settings, including status, syslog IP address and log facility.
`sys logs syslog facility [local-id]`	Logs the messages to different files located on the syslog server. `local-id`: The number of files available depends on the syslog utility used. For example, the Kiwilog supports seven files.
`sys logs syslog server [domain-name|ip-address]`	This sets the domain name and IP address for the syslog server to send the logs.
`sys password <new-password>`	Sets the system administrator password.
`sys pwderrtm [minute]`	Sets or displays the password error blocking timeout value in minutes. Not devices support this command.
`sys qe acl add <ila> <ilp> <oga> <ogp> <proto> <direction>`	Adds an ACL rule in the QE (quick engine) ACL table. `ila`: Enters the inside local address, that is the source or destination address of packets on the LAN. `ilp`: Enters the inside local port. `oga`: Enters the outside global address, that is the source or destination address of packets on the WAN. `ogp`: Enters the outside global port. `proto`: Specifies the protocol type. 1: TCP, 0: UDP `direction`: Specifies the traveling direction of the packets. 1: outgoing, 0: incoming

Table 44 sys Commands (continued)

COMMAND	DESCRIPTION
sys qe acl delete <*index*>	Removes an ACL rule from the QE (quick engine) ACL table.
sys qe acl display	Shows the QE (quick engine) ACL table.
sys qe acl reset [on|off]	Refreshes the QE (quick engine) ACL table.
sys qe active [on|off]	Enables or disables quick engine.
sys qe arp add <*target-ip*> ether <*target-mac*> interface <*interface-ip*> chann <*channel-mac*>	Adds an ARP (Address Resolution Protocol) entry in the QE (quick engine) ARP table.
sys qe arp delete <*target-ip*> <*hw-type*>	Removes an ARP entry from the QE (quick engine) ARP table.
sys qe arp display [on|off]	Shows the QE (quick engine) ARP table.
sys qe arp reset	Refreshes the QE (quick engine) ARP table.
sys qe arp search <*ip-address*> <*hw-type*>	Searchs for a specified ARP entry in the QE (quick engine) ARP table.
sys qe arp starttimer	Starts the ARP timer that sets how often the ZyXEL Device updates the QE ARP entries.
sys qe arp stoptimer	Stops the ARP timer that sets how often the ZyXEL Device updates the QE ARP entries.
sys qe bridge add <*src-mac*> <*id*>	Adds a bridge entry in the QE bridge table. *src-mac*: Enters the source MAC address. *id*: Enters the channel ID.
sys qe bridge bltlookup <*src-mac*> <*id*>	Looks up the bridge local type in the QE bridge table.
sys qe bridge delete <*target-mac*>	Removes a bridge entry from the QE bridge table.
sys qe bridge display	Displays the QE bridge table.
sys qe bridge search <*src-mac*>	Searchs for a specified bridge entry in the QE bridge table
sys qe bridge reset [on|off]	Refreshes the QE (quick engine) bridge table.
sys qe config [0: off | flags]	Sets the features supported in QE, such as quick route.
sys qe debug [on|off]	Displays or sets the QE debug flag.
sys qe NFAIFlag	Activates NAT Fragment Anti-idiot.
sys qe poe active [on|off]	Turns on or off QE for PPPoE.
sys qe poe display	Displays the current status of QE PPPoE.
sys qe route add <*dest-ip*>[/<*bits*>] <*gateway-ip*> <*interface-ip*> [<*metric*>]	Adds a routing entry in the QE routing table.
sys qe route delete <*ip-address*>[/<*bits*>]	Removes a routing entry in the QE routing table.
sys qe route display	Displays the QE routing table.
sys qe route reset [on|off]	Refreshes the QE routing table.
sys qe route search <*target-ip*>	Searchs for a specified routing entry in the QE routing table.

Table 44 sys Commands (continued)

COMMAND	DESCRIPTION
`sys qe session add <ila> <ilp> <iga> <igp> <oga> <ogp> <protocol>`	Adds a session to the QE session table.
`sys qe session display`	Displays the QE session table.
`sys qe session reset [on|off]`	Resets the QE session table.
`sys qe state`	Displays the channel profile and encapsulation type of quick engine.
`sys reboot`	Restarts the ZyXEL Device.
`sys romreset`	Restores the default romfile (configuration).
`sys routeip <on|off>`	Turns on or off IP routing.
`sys save`	Avoid using this command as it may result in system instability.
`sys server access <service><0:all|1:None|2:LAN only|3:WAN only>`	Enables or disables the server access on the specified interface using the specified protocol. Use `sys server load` before configuring server access.
`sys server auth_client <https> [on|off]`	Specifies whether the ZyXEL Device authenticates the client for the specified service's sessions.
`sys server certificate <https|ssh>[certificate-name]`	Sets the server certificate the ZyXEL Device uses to identify itself for the specified service's sessions.
`sys server display`	Display's the ZyXEL Device's server access settings.
`sys server load`	Loads server information. Use this first in order to be able to configure the server settings.
`sys server port <service><port>`	Sets the server port number and protocol.
`sys server save`	Saves the server settings.
`sys server secureip <service><ip-address>`	Sets the IP address of a "trusted" computer that is allowed to access the ZyXEL Device by remote management using this service.
`sys snmp clear`	Resets SNMP related fields to default values.
`sys snmp discard`	Discards any changes made to your ZyXEL Device SNMP configuration and returns to the previous settings.
`sys snmp display`	Displays the status of the SNMP Get, Set and Trap Community, and the Trusted Host's and Trap Host's IP address.
`sys snmp get <community>`	Sets the SNMP Get Community.
`sys snmp save`	Saves any changes made to your ZyXEL Device SNMP configuration to non-volatile memory.
`sys snmp set <community>`	Sets the SNMP Set Community.
`sys snmp trap community <community>`	Sets the SNMP Trap Community.
`sys snmp trap destination <ip-address>`	Sets the IP address of the station to send SNMP traps to.
`sys snmp trusthost <ip-address>`	Sets the IP address of the SNMP trusted host. If an SNMP trusted host is specified, the ZyXEL Device will respond only to SNMP messages from this IP address. If this field is left blank, the ZyXEL Device will respond to all SNMP messages it receives, regardless of their source.

Table 44 sys Commands (continued)

COMMAND	DESCRIPTION
`sys socket`	Displays the system socket's ID number, type, control block address (PCB) (this is a memory address), IP address and port number of the peer device connected to the socket (Remote Socket) and task control block (Owner).
`sys stdio [minute]`	Sets the management session inactivity timeout value.
`sys tcconsole`	This function is disabled.
`sys time hour [min[sec]]`	Sets or displays the current system time.
`sys tos cache`	Displays TOS in the cache.
`sys tos currentTOSNum`	Displays current TOS number.
`sys tos display`	Shows all runtime TOS.
`sys tos historicalCHigh`	Displays the historical concurrent high number.
`sys tos historicalHigh`	Displays the historical high.
`sys tos listPerHost`	Displays the session count for each host.
`sys tos sessPerHost <session#>`	Sets the temporary open sessions per host limit.
`sys tos tempTOSDisplay`	Displays the TOS records.
`sys tos tempTOSTimeout [timeout]`	Sets or displays the timeout value in seconds. *timeout*: 1-2147483647 seconds
`sys tos timeout ah <timeout>`	Sets the AH-session idle-timeout value in seconds (used in IP Sec).
`sys tos timeout display`	Displays all TOS timeout information.
`sys tos timeout esp <timeout>`	Sets the ESP-session idle-timeout value in seconds (used in IP Sec).
`sys tos timeout gre <timeout>`	Sets the GRE-session idle-timeout value in seconds.
`sys tos timeout icmp <timeout>`	Sets the ICMP session idle timeout value in seconds.
`sys tos timeout igmp <timeout>`	Sets the IGMP session idle timeout value in seconds.
`sys tos timeout mail <timeout>`	Sets the e-mail session idle-timeout value in seconds.
`sys tos timeout others <timeout>`	Sets the idle-timeout value for other sessions in seconds.
`sys tos timeout tcp <timeout>`	Sets the TCP session idle timeout value in seconds.
`sys tos timeout tcpfin <timeout>`	Sets the TCP FIN session idle timeout value in seconds.
`sys tos timeout tcpsyn <timeout>`	Sets the SYN TCP session idle timeout value in seconds.
`sys tos timeout udp <timeout>`	Sets the UDP-session idle-timeout value in seconds.
`sys tripleplay igmpsnp disable`	Disables IGMP Snooping on tripleplay services.
`sys tripleplay igmpsnp display`	Displays tripleplay's IGMP Snooping settings, including status, group count, maximum response time, query interval and robustness.
`sys tripleplay igmpsnp enable`	Enables IGMP Snooping on tripleplay services. IGMP snooping limits the forwarding of redundant packets to LAN ports in a multicast flood. It only tries to deliver traffic to a specified LAN port in a multicast group. Use this command to start or configure tripleplay IGMP Snooping, as well as after making changes to max response time, query interval or robustness.

Table 44 sys Commands (continued)

COMMAND	DESCRIPTION
`sys tripleplay igmpsnp maxresptime [tenthsofasecond]`	Displays or sets the maximum response time for a IGMP membership query in tenths of a second. This is used to determine the total group timeout value. IGMP Group Timeout = (Robustness x Query Interval) + (Max Response Time/10) + Time Value.(default = 2).
`sys tripleplay igmpsnp queryinterval [seconds]`	Displays or sets the IGMP query interval time in seconds. This is used to determine the query timeout value. IGMP Query Timeout = (Robustness x Query Interval) + (Max Response Time/20) + Time Value (default = 2).
`sys tripleplay igmpsnp robust [robustness]`	Displays or sets the level of robustness. *robustness*: This variable represents the level of expected packet loss on the subnet. The range is 2-255. This is used to determine the leave timeout: IGMP Leave Timeout = Robustness x Max Response Time/100 + 3
`sys tripleplay portbase disable`	Disables port-based tripleplay services.
`sys tripleplay portbase display`	Displays the permanent virtual circuit (PVC) to port mappings for tripleplay services such VoIP or video.
`sys tripleplay portbase enable`	Enables port-based tripleplay services.
`sys tripleplay portbase groupadd [groupid][LAN[ports]][PVC[ports]][WLAN[ssid]]`	Adds ports and/or interfaces to a group mapping policy.
`sys tripleplay portbase groupdel [groupid][LAN[ports]][PVC[ports]][WLAN[ssid]]`	Deletes the whole group or individual members.
`sys tripleplay portbase groupset [groupid][LAN[ports]][PVC[ports]][WLAN[ssid]]`	Sets a group port to PVC mapping policy, with up to eight PVCs allowed. WLAN may only belong to one group. If a product supports multiple SSID, each one will be treated as if it were a port.
`sys tripleplay portbase save`	Saves the port mappings to non-volatile memory.
`sys tripleplay portbase set <port><pvcid|disable>`	Sets a single port to single PVC mapping policy. *pvcid*: The number of the PVC, between 1-8.
`sys upnp active [0:no|1:yes]`	Activates or deactivates the saved UPnP settings.
`sys upnp config [0:deny|1:permit]`	Allows users to make configuration changes through UPnP.
`sys upnp display`	Displays the UPnP configuration.
`sys upnp firewall [0:deny|1:pass]`	Allows UPnP to pass through the firewall.
`sys upnp load`	Loads the UPnP setting buffer. Use this command to be able to configure the settings. Use `sys upnp save` after you configure the settings.
`sys upnp reserve [0:deny|1:permit]`	Retains UPnP created NAT rules even after restarting.
`sys upnp save`	Saves the UPnP settings to the long term memory.
`sys userPassword <password>`	Changes the user password. This command may not be supported in your ZyXEL Device.
`sys version`	Displays the firmware and bootbase versions.

Table 44 sys Commands (continued)

COMMAND	DESCRIPTION
`sys view <filename>`	Displays the specified text file.
`sys wdog cnt [value]`	Sets or displays the current watchdog count. This value represents the time interval at which the system is checked for normal operation. If watchdog detects a system crash the system is restarted. Use `sys wdog switch` to activate watchdog before configuring. *value:* This is a value from 0-34463.
`sys wdog switch [on|off]`	Turns the watchdog firmware protection feature on or off.
`sys xmodemmode [crc|checksum]`	Changes the console port xmodem mode.

The following table shows a list of default values.

Table 45 sys Default Values

VARIABLE	DEFAULT VALUE
`sys ddns config active [0|1]`	0
`sys filter netbios config <0|1|2|3|4><on|off>`	0:Between LAN and WAN: Off/Forward 3:IPSec passthrough: off/forward 4:Trigger Dial: off/disable
`sys general routip <on|off>`	on
`sys general bridge <on|off>`	off
`sys logs syslog active [0:no|1:yes]`	0
`sys snmp trap community <community>`	public
`sys stdio [minute]`	5
`sys tos sessPerHost <session#>`	512
`sys tos tempTOSTimeout [timeout]`	5
`sys tos timeout gre <timeout>`	9000
`sys tripleplay igmpsnp maxresptime [tenthsofasecond]`	100
`sys tripleplay igmpsnp queryinterval [seconds]`	125
`sys tripleplay igmpsnp robust [robustness]`	2
`sys upnp active [0:no|1:yes]`	0
`sys wdog cnt [value]`	180
`sys wdog switch [on|off]`	on
`sys xmodemmode [crc|checksum]`	crc

19.2 Command Example

The following examples show you first how to configure logs and then how to display them.

19.2.1 Configuring Logging

1. Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the ZyXEL Device is to record.
2. Use `sys logs category` to view a list of the log categories.

Figure 3 Displaying Log Categories Example

```
ras> sys logs category
access          attack          display         error
mten            upnp            urlblocked      urlforward
anyip
ras>
```

3. Use `sys logs category` followed by a log category to display the parameters that are available for the category.

Figure 4 Displaying Log Parameters Example

```
ras> sys logs category access
Usage: [0:none/1:log/2:alert/3:both]
ras>
```

4. Use `sys logs category` followed by a log category and a parameter to decide what to record.

   Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category. Not every parameter is available with every category.
5. Use the `sys logs save` command to store the settings in the ZyXEL Device (you must do this in order to record logs).

19.2.2 Displaying Logs

- Use the `sys logs display` command to show all of the logs in the ZyXEL Device's log.
- Use the `sys logs category display` command to show the log settings for all of the log categories.
- Use the `sys logs display [log category]` command to show the logs in an individual ZyXEL Device log category.
- Use the `sys logs clear` command to erase all of the ZyXEL Device's logs.

19.2.3 Log Command Example

This example shows how to set the ZyXEL Device to record the access logs and alerts and then view the results.

```
ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access

#  .time                 source                 destination            notes

    message
  0|06/08/2004 05:58:21 |172.21.4.154         |224.0.1.24           |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  1|06/08/2004 05:58:20 |172.21.3.56          |239.255.255.250      |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  2|06/08/2004 05:58:20 |172.21.0.2           |239.255.255.254      |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  3|06/08/2004 05:58:20 |172.21.3.191         |224.0.1.22           |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  4|06/08/2004 05:58:20 |172.21.0.254         |224.0.0.1            |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  5|06/08/2004 05:58:20 |172.21.4.187:137     |172.21.255.255:137   |ACCESS
BLOCK
    Firewall default policy: UDP (W to W/ZW)
```

20

VoIP Commands

Use these commands to configure VoIP settings on the ZyXEL Device.

20.1 VoIP RTP Commands

Use these commands to configure Real-time Transport Protocol settings on the ZyXEL Device.

Table 46 RTP Command Summary

COMMAND	DESCRIPTION
`voice config rtp index <index>`	Selects an RTP (Real-time Transport Protocol) index for configuration.
`voice config rtp packetsize <index> g711 <0:10ms|1:20ms|2:30ms> g729 <0:10ms|1:20ms|2:30ms>`	Specifies the transmit period of RTP packets for G.711 and G.729 codecs.
`voice config rtp rtcpinterval <index> <miliseconds>`	Specifies the RTCP (RTP Control Protocol) interval. This is the time interval at which the ZyXEL Device sends control packets during calls.
`voice config rtp save <index>`	Saves the RTP configuration iin the working buffer to non-volatile memory. The working buffer is a volatile memory space. The settings in the working buffer are not applied to the ZyXEL Device until you execute this command.
`voice config rtp display <index>`	Displays the saved values for the specified RTP configuration.
`voice config rtp dumpCfg`	Displays the configured values in the working buffer for the specified configuration.
`voice config rtp free`	Clears the working buffer for the specified configuration. Any unsaved changes are lost.

20.1.1 VoIP RTP Command Examples

This example displays the RTP settings configured on the ZyXEL Device.

```
ras> voice config rtp display 1
       RTP[1] Display
==========================================
Sort Buffer Size ms :10
RTCP Interval ms :0
G711 voice Packet Length ms :20
G729 voice Packet Length ms :20
ras>
```

The following table describes the labels in this screen.

Table 47 `voice config rtp display`

LABEL	DESCRIPTION
Sort Buffer Size ms	Specifies the size of the sorting buffer for processing RTP packets.
RTCP Interval	Displays the RTCP interval. The interval between RTP control packets being sent during calls.
G711 voice Packet Length ms	Displays the length of speech duration encapsulated in RTP packets for G.711 codec.
G729 voice Packet Length ms	Displays the length of speech duration encapsulated in RTP packets for G.729 codec.

20.2 VoIP Relay to PSTN Commands

Use these commands to specify PSTN prefix numbers. The PSTN prefix numbers tells the ZyXEL Device when to use the PSTN line to make calls.

Table 48 Relay to PSTN Numbers Command Summary

COMMAND	DESCRIPTION
`voice config pstn index <index>`	Specifies which PSTN prefix number you want to configure. *index*: 1-10; Index number 1 represents the PSTN prefix number or the number a user has to dial to use the PSTN line. Index numbers 2-9 represent relay to PSTN numbers.
`voice config pstn phonebook <index> <prefix-nr>`	Sets the PSTN prefix number for the specified PSTN prefix entry. *prefix-nr*: Allowed characters are numbers (0-9), asterisks (*), and pound characters (#). This can be up to 32 digits long. Leaving this parameter blank clears the PSTN prefix entry.
`voice config pstn prefixcode <index> <1:enable|0:disable>`	Disables or enables the prefixcode for the specified PSTN prefix entry.
`voice config pstn active <index> <1:active|0:in-active>`	Enables or disables the PSTN prefix entry.
`voice config pstn save <index>`	Saves the PSTN prefix configuration in the working buffer to non-volatile memory. The working buffer is a volatile memory space. The settings in the working buffer are not applied to the ZyXEL Device until you execute this command.
`voice config pstn display`	Displays the saved values for the PSTN prefix numbers.
`voice config pstn dumpCfg <index>`	Displays the configured values in the working buffer for the specified configuration.
`voice config pstn free`	Clears the working buffer for the specified configuration. Any unsaved changes are lost.

20.2.1 VoIP Relay to PSTN Command Examples

This example displays the PSTN prefix numbers configured on the ZyXEL Device.

```
ras> voice config pstn display
   index   PhoneNumber                          flags

-------------------------------------------
     1    7878  7
     2    3434  4
     3      0
     4      5
     5      0
     6      0
     7      0
     8      0
     9      0
    10      0
```

he following table describes the labels in this screen.

Table 49 `voice config pstn display`

LABEL	DESCRIPTION
index	This is the number of a PSTN prefix number entry.
PhoneNumber	This is the prefix number associated with the entry.
flags	This field displays one of the following entries • 0 - if this index entry has not been configured. • 7 - if the prefix code is turned on, phone number activated and configured. • 4 - if the prefix code is turned off, phone number not activated or configured.

20.3 VoIP SIP Account Commands

Use these commands to configure SIP accounts on the ZyXEL Device.

Table 50 SIP Account Command Summary

COMMAND	DESCRIPTION
`voice config signal index <index>`	Specifies the SIP account you want to configure.
`voice config signal active <index> <0:off|1:on>`	Activates (`1`) or deactivates (`0`) this SIP account.
`voice config signal registertimeout <index> <seconds>`	Sets the SIP registration timeout value for this SIP account. (default 3600 sec)
`voice config signal registerresendtime <index> <seconds>`	Sets the number of seconds the ZyXEL Device waits to resend a registration request if a previous request failed or there was no response.
`voice config signal sessiontimerActive <index> <0:off|1:on>`	Activates (`1`) or deactivates (`0`) a SIP session timer for this SIP account.
`voice config signal sessiontimeout <index> <30-3600>`	Sets the number of seconds a conversation can last before the call is automatically disconnected. (default 300 sec)

Table 50 SIP Account Command Summary

COMMAND	DESCRIPTION
`voice config signal minse <index> <20-1800>`	Sets the minimum number of seconds the ZyXEL Device accepts for a session expiration time when it receives a request to start a SIP session.
`voice config signal serveraddress <index> <ip>`	Sets the SIP server address for this SIP account.
`voice config signal serverport <index> <1024-65535>`	Sets the SIP server's listening port for this SIP account.
`voice config signal registeraddress <index> <ip>`	Sets the SIP register server address for this SIP account.
`voice config signal registerport <index> <1024-65535>`	Sets the SIP register server's listening port for this SIP account.
`voice config signal userid <index> <username>`	Sets the SIP username for this SIP account.
`voice config signal password <index> <password>`	Sets the SIP password for this SIP account.
`voice config signal urltype <index> <sip|tel>`	Sets the SIP URL type for this SIP account. `sip`: SIP messages are sent to domain name or IP address. `tel`: SIP messages are sent to addresses represented as telephone numbers.
`voice config signal port <index> <1024-65535>`	Sets the ZyXEL Device's SIP listening port for this SIP account.
`voice config signal phonenumber <index> <0-32>`	Sets the SIP number for this SIP account.
`voice config signal domain <index> <domain>`	Sets the SIP service domain name. *domain*: 1-128 alphanumeric characters.
`voice config signal dtmf <index> <rfc2833|pcm|sipinfo|rfc2833like>`	Sets the method for sending the tones created by pressing buttons on your phones keypad. `rfc2833`: sends DTMF tones in RTP packets. `pcm`: sends DTMF tones in voice data stream. `sipinfo`: sends DTMF tones in SIP messages. `rfc2833like`: Sends the information in SIP messages with an RTP payload.
`voice config signal pri_compression <index> <0:G711mu|8:G711A|18:G729>`	Sets the primary compression (voice codec) type for this SIP account.
`voice config signal sec_compression <index> <0:G711mu|8:G711A|18:G729>`	Sets the secondary compression (voice codec) type for this SIP account.
`voice config signal portrange <index> <start-port> <end-port> (40000~65535)`	Sets the port range for RTP/RTCP communication.
`voice config signal transport <index> <udp|tcp>`	Sets the protocol for sending SIP messages.
`voice config signal callerid <index> <disable|enable>`	Enables or disables the caller ID feature for this SIP account.
`voice config signal autoredialpstn <index> <disable|enable>`	Enables or disables the auto-redial feature for this SIP account.

Table 50 SIP Account Command Summary

COMMAND	DESCRIPTION
`voice config signal phoneselect <index> <phone-port|0:All> <0:No|1:Yes>`	Sets the physical FXS port mapping to this SIP account for incoming calls. In other words, specifies which analog phone rings when a call is received for this SIP account. *phone-port*: this is an FXS port on the ZyXEL Device. Enter 0 to select all FXS ports.
`voice config signal vlantag <index> <disable|enable>`	Enables or disables VLAN tags in VoIP packets.
`voice config signal tpid_vlantag <index> <tpid>`	Sets the value of the TPID (Tag Protocol Identifier) in the VLAN tag header of VoIP packets.
`voice config signal vid_vlantag <index> <vlan-id>`	Sets the VLAN ID of VoIP packets sent via this SIP account.
`voice config signal priority_vlantag <index> <priority:0-7>`	Sets the VLAN priority value of outgoing VoIP packets.
`voice config signal diffservrtp <index> <0-255>`	Sets the DiffServ value in the IP header of outgoing RTP packets for this SIP account.
`voice config signal diffservsip <index> <0-255>`	Sets the DiffServ value in the IP header of outgoing SIP packets for this SIP account.
`voice config signal mwiactive <index> <0:off|1:on>`	Enables or disables the message waiting indication.
`voice config signal mwitimeout <index> <minutes>`	Sets the MWI time out value.
`voice config signal rfc3325 <index><1: privacy call using RFC3325, 0: privacy call using draft-01>`	Enables or disables the sending of identity information between SIP devices as described in RFC 3325.
`voice config signal prack <index> <0:off|1:on>`	Enables or disables sending of PRACK messages as described in RFC 3262 for this SIP account.
`voice config signal fakesipactive <index> <0:off|1:on>`	Enables a fake SIP service for this SIP account. This feature is used by ZyXEL Devices which are behind a NAT router that does not support SIP ALG. If a ZyXEL Device has a private IP address on its WAN interface, then it may have to provide a public IP address along with a listening port of the Internet gateway (for example a DSL modem) to which it is connected. This fake IP address and port number ensure that SIP packets are successfully routed back to the ZyXEL Device from the Internet.
`voice config signal fakesipservaddr <index> <ip>`	Sets a fake SIP server address for this SIP account.
`voice config signal fakesipservport <index> <port>`	Sets a fake SIP server port for this SIP account.
`voice config signal outboundactive <index> <0:off|1:on>`	Enables or disables a SIP outbound proxy configuration for this SIP account.
`voice config signal outboundaddr <index> <ip>`	Sets the address of the SIP outbound proxy server.
`voice config signal outboundport <index> <port>`	Sets the port number of the SIP outbound proxy server.
`voice config signal outboundkaactive <index> <0:off|1:on>`	Enables or disables NAT keep alive service.

Table 50 SIP Account Command Summary

COMMAND	DESCRIPTION
`voice config signal outboundkaintvl <index> <seconds>`	Sets how often (seconds) the ZyXEL Device sends SIP notify messages to the SIP server to let the server know that a session is ongoing.
`voice config signal stunactive <index> <0:off|1:on>`	Enables or disables STUN.
`voice config signal stunservaddr <index> <ip>`	Sets the STUN server IP Address.
`voice config signal stunservport <index> <port>`	Sets the STUN server port number.
`voice config signal ringbackactive <index> <0:off|1:on>`	Disables or enables early media.
`voice config signal ringbacktone <index> <tone>`	Sets an early media tone.
`voice config signal musiconholdactive <index> <0:off|1:on>`	Disables or enables music on hold.
`voice config signal musiconholdtone <index> <tone>`	Sets the music on hold tone.
`voice config signal callfwd <index> <1-2>`	Specifies the call forwarding table.
`voice config signal mixermode <index> <0:Local|1:Remote>`	Sets the 3-way conference mixermode.
`voice config signal transafterconf <index> <0:off|1:on>`	Enables or disables transferring of calls from
`voice config signal rfc3263 <index> <0:off|1:on>`	Disables or enables support for RFC 3263 for this SIP account. RFC 3263 specifies how SIP proxy servers use DNS to find remote (located in another domain) SIP proxy server to complete SIP calls.
`voice config signal featuresdisable <index> <0|1>`	Disables or enables call forwarding for this SIP account. Enter 1 to disable call forwarding or enter 0 to enable call forwarding.
`voice config signal save <index>`	Saves the SIP configuration in the working buffer to non-volatile memory. The working buffer is a volatile memory space. The settings in the working buffer are not applied to the ZyXEL Device until you execute this command.
`voice config signal display <index>`	Displays the saved values for the SIP account.
`voice config signal dumpCfg`	Displays the configured values in the working buffer for the specified configuration.
`voice config signal free`	Clears the working buffer for the specified configuration. Any unsaved changes are lost.

20.3.1 VoIP SIP Account Command Examples

This example does the following:

- specifies not to ring phone 2 when receiving a call by SIP 1 account.
- specified to ring phone 1 when receiving an coming call by SIP 1 account.

- displays the mapping to only phone port 1 for SIP 1 account.

```
ras> voice config signal index 1
ras> voice config signal phoneselect 1 2 0
ras> voice config signal phoneselect 1 1 1
ras> voice config signal save 1
ras> voice config signal display 1
     Mapping phone port: 1
```

20.4 Analog Phone Commands

Use these commands to configure analog phone features on the ZyXEL Device.

Table 51 Analog Phone Command Summary

COMMAND	DESCRIPTION
`voice config fxs index <index>`	Specifies the analog phone port for configuration.
`voice config fxs echocancellation <index> <enable|disable>`	Disables or enables echo cancellation.
`voice config fxs jittersize <index> <0-90>`	Sets the jitter buffer size in miliseconds.
`voice config fxs vad <index> <enable|disable>`	Disables or enables the VAD (Voice Activity Detection).
`voice config fxs dialshortinterval <index> <interval>`	Sets the dialshortinterval value. This is the time interval (in seconds) that the ZyXEL Device waits between digits being dialed when making a call. If time between dialed digits exceeds this value the ZyXEL Device considers the dialing to be completed and calls the number entered. Enter a value between 0-256.
`voice config fxs diallonginterval <index> <interval>`	Sets the diallonginterval value. This is the time interval (in seconds) that the ZyXEL Device waits until the first digit is dialed when making a call. If no digit is dialed in this time period the ZyXEL Device sends a busy signal. Enter a value between 0-256.
`voice config fxs flashmaxinterval <index> <interval>`	Sets the flash key maximum interval (in miliseconds). If the flash key is pressed for a longer period, then it will be ignored. Users must press the flash key for a period of time smaller than the flash key maximum interval but greater than the flash key minimum interval for it to be recognized by the system. Enter a value between 0~65535.
`voice config fxs flashmininterval <index> <interval>`	Setup flash key minimum interval. If the flash key is pressed for a shorter period, then it will be ignored. Enter a value between 0~65535.
`voice config fxs inputvolume <index> <volume>`	Sets the input volume level. The level can be in the range -14 to 14.
`voice config fxs outputvolume <index> <volume>`	Sets the output volume level. The level can be in the range -14 to 14.
`voice config fxs sipselect <index> <phone-port|0:All> <0:no|1:yes>`	Configures an analog phone to SIP account mapping and enables the specified SIP account.

Table 51 Analog Phone Command Summary

COMMAND	DESCRIPTION
`voice config fxs fax <index> <0|1>`	Sets how the ZyXEL Device handles fax messages. 0: The ZyXEL Device uses G.711 to send fax messages. 1: The ZyXEL Device sends fax messages as UDP or TCP/IP packets through IP networks. This method is also referred to as T.38 relay.
`voice config fxs callwaitingtime <index> <time>`	Sets the call waiting time.
`voice config fxs cidtype <index> <0:During Ring |1: Prior Ring>`	Sets whether the ZyXEL Device displays the caller ID priror to or during ringing when calls come in.
`voice config fxs cidfirsttastype <index> <0|1|2|3>`	Sets the first TAS (Terminal Alerting Signal) parameter. TAS specifies the method to alert the receiver that data is forthcoming. The possible methods are: • 0: NULL • 1: DT-AS (Dual Tone Alerting Signal) • 2: RP-AS (Ringing Pulse Alrting Signal) • 3: Line reversal followed by DT-AS This command executes automatically when a countrycode is selected. It adjusts the settings for caller ID to work in different geographic locations.
`voice config fxs cidsecondtastype <index> <0:NULL|1:DT-AS|2:RP-AS>`	Sets the second TAS parameter. This command executes automatically when a countrycode is selected. It adjusts the settings for caller ID to work in different geographic locations.
`voice config fxs cidpayload <index> <0:FSK|1:DTMF>`	Sets the DTMF payload type. This command executes automatically when a countrycode is selected. It adjusts the settings for caller ID to work in different geographic locations.
`voice config fxs firsttastoint <index> <0~65535>`	Sets the first TAS timeout interval. This command executes automatically when a countrycode is selected. It adjusts the settings for caller ID to work in different geographic locations.
`voice config fxs sectastoint <index> <0~65535>`	Sets the second TAS timeout interval. This command executes automatically when a countrycode is selected. It adjusts the settings for caller ID to work in different geographic locations.
`voice config fxs firstringtoint <index> <0~65535>`	Sets the CID ring timeout interval. This command executes automatically when a countrycode is selected. It adjusts the settings for caller ID to work in different geographic locations.
`voice config fxs cidringtimeout <index> <0~65535 msec>`	Sets call id ring timeout. This command generates extra 200 ms delay. For example, if you set the value to 0 ms, the actual value is 200 ms and if you set the value to 200 ms, then the actual value is 400 ms. This command executes automatically when a countrycode is selected. It adjusts the settings for caller ID to work in different geographic locations.
`voice config fxs ciddtasacktimeout <index> <100~500>`	Sets the TAS acknowledgement time out value (in miliseconds). This command executes automatically when a countrycode is selected. It adjusts the settings for caller ID to work in different geographic locations.

Table 51 Analog Phone Command Summary

COMMAND	DESCRIPTION
`voice config fxs featuresdisable <index> <0~7>`	Disables or enables analog phone features. ras> voice config fxs featuresdisable 1 h Use this command to configure the debug settings. This command allows you to disable or enable the following features: • Call Waiting • Call Conference • Call Transfer • PSTN Outgoing • ISDN Outgoing This is a binary data field with each bit representing a parameter, so you can control the parameters by entering decimal (base-10) numbers that correspond to binary numbers. The first bit controls the Call Waiting parameter, the second bit controls Call Conference, and so on. A binary value of 1 turns a parameter on, and a binary value of 0 turns it off. Thus, if you enter 6 (00110 in binary), the following displays: Call Waiting(bit 0) disabled Call Conference(bit 1) enabled Call Transfer(bit 2) enabled PSTN Outgoing(bit 3) disabled ISDN Outgoing(bit 4) disabled
`voice config fxs autodialenable <index> <enable|disable>`	Disables or enables the auto dial feature. When auto dial is enabled a user can press the pound key and the ZyXEL Device will try to connect to the dialed number (the ZyXEL Device does not wait for the dialing interval to timeout.)
`voice config fxs autodialnumber <index> <phone number>`	Sets a phone number for auto dialing. When the last digit of the number entered via this command is dialed the ZyXEL Device will try to connect to this number immediately and not wait for the dialing interval timeout.
`voice config fxs save <index>`	Saves the analog phone configuration in the working buffer to permanent memory. The working buffer is a volatile memory space. The settings in the working buffer are not applied to the ZyXEL Device until you execute this command.
`voice config fxs display <index>`	Displays the saved values for the SIP account.
`voice config fxs dumpCfg`	Displays the configured values in the working buffer for the specified configuration.
`voice config fxs free`	Clears the working buffer for the specified configuration. Any unsaved changes are lost.

20.4.1 Analog Phone Command Examples

This example configures the settings for the analog phone port **1** on the ZyXEL Device. It sets the ZyXEL Device the volume it sends to the analog phone to the maximum **14** and it sets the volume it sends out from this analog phone to **13**.

```
ras> voice config fxs index 1
ras> voice config fxs inputvolume 1 14
ras> voice config fxs outputvolume 1 13
ras> voice config fxs save 1
```

20.5 VoIP Speed Dial Commands

Use these commands to configure speed dial entries on the ZyXEL Device.

Table 52 Speed Dial Command Summary

COMMAND	DESCRIPTION
`voice config phbook index <index>`	Specifies the speed dial entry index for configuration.
`voice config phbook active <index> <1:active|0:inactive>`	Enables or disables this speed dial entry.
`voice config phbook orignum <index> <0~32>`	Sets the SIP number that the ZyXEL Device dials when the speed dial number is entered.
`voice config phbook forcesipuri <index> <1-128>`	Sets the ZyXEL Device to use an IP address or URI to complete this speed dial call. This is used for peer-to-peer calls or calls that use a different SIP server from the ones defined in the SIP accounts.
`voice config phbook speednum <index> <0~32>`	Sets the speed dial number for this speed dial entry. This is the number callers must dial to perform this speed dial call.
`voice config phbook name <index> <name>`	Sets a name for this speed dial entry.
`voice config phbook type <index> <0:Proxy|1:NonProxy>`	Specifies whether this entry should use an existing SIP account (proxy) or whether it should be a call to a SIP server not specifed in the SIP accounts configured on the ZyXEL Device (non-proxy).
`voice config phbook save <index>`	Saves the speed dial entry in the working buffer to non-volatile memory. The working buffer is a volatile memory space. The settings in the working buffer are not applied to the ZyXEL Device until you execute this command.
`voice config phbook display <index>`	Displays the saved values for the speed dial entry.
`voice config phbook dumpCfg <index>`	Displays the configured values in the working buffer for the specified configuration.
`voice config phbook free`	Clears the working buffer. Any unsaved changes are lost.

20.5.1 VoIP Speed Dial Command Examples

This example configures a speed dial entry for a peer-to-peer call with an IP phone located at the IP address **172.16.1.201**, with the SIP number **12345**. Users will have to dial **#01** to reach this speed dial entry.

```
ras> voice config phbook index 1
ras> voice config phbook active 1 1
PhoneBook active on
ras> voice config phbook orignum 1 12345
ras> voice config phbook forcesipuri 1 172.16.1.201
ras> voice config phbook type 1 1
ras> voice config phbook speednum 1 #01
ras> voice config phbook name 1 Andre
ras> voice config phbook save 1
ras> voice config phbook display 1
================================================
origNumber: 12345
forceSipURI: 172.16.1.201
speedNumber: #01
name: Andre
flags: active
type: non-Proxy
```

20.6 VoIP Common Settings Commands

Use these commands to configure IVR (Interactive Voice Response), PSTN fallback and other common settings on the ZyXEL Device.

Table 53 Common Settings Command Summary

COMMAND	DESCRIPTION
`voice config common index <index>`	Specifies the common settings entry index for configuration.
`voice config common ivrsyspermit <index> <0|1>`	Enables (`1`) or disables (`0`) changing the IVR settings.
`voice config common specialFlag <index> <special flag|h:for help>`	This is a command which tests SIP communication. It is a 2-bit binary flag. Bit 0 specifies when to send RTP traffic. If bit 0 is set to 0, then send RTP after sending 200OK message, otherwise send RTP after receiving ACK message. Bit 1 specifies when to send 200OK message. If set to 0, then send 200OK message when receive NOTIFY message, otherwise follow RFC3265.
`voice config common ivrcodec <index> <codec>`	Sets the voice codecs to be used by the ZyXEL Device. Type one of the following: • 0 to enable G.711 µ • 4 to enable G.723 • 8 to enable G.711 A • 18 to enable G.729 - This setting is recommended. • 97 to enable G.726 24K • 98 to enable G.726 32K

Table 53 Common Settings Command Summary

COMMAND	DESCRIPTION
`voice config common ivrlanguage <index> <0~2>`	Specifies the language for IVR. The languages supported on your ZyXEL Device differ by model. This command allows you to specify one of the languages supported.
`voice config common pstnfallback <index> <0:Disable PSTN Fallback|1:Enable PSTN Fallback>`	Enables or disables the PSTN fallback function. When this function is enabled the ZyXEL Device uses the PSTN line to complete calls if a SIP account is unregistered.
`voice config common sipfallback <index> <0:Disable SIP Fallback|1:Enable SIP Fallback>`	Enables or disables the SIP fallback function. When this function is enabled the ZyXEL Device uses a SIP line to complete calls if the PSTN line is not receiving a signal.
`voice config common dialmethod <index> <0:European|1:USA>`	Sets whether the ZyXEL Device uses the European dialing method or dialing method based on the American system.
`voice config common forcedialtone <index><0:Busytone when SIP/PSTN Not Registered|1:Dialtone when SIP/PSTN Not Registered>`	Sets the ZyXEL Device to provide a dial tone even if there are no SIP lines registered on the ZyXEL Device.
`voice config common removepound <index> <0:not removed|1:removed pound>`	Enables removing the pound (#) key as part of the dialed digits. If this function is not activated then the pound key is sent along with the dialed digits when making a call.
`voice config common countrycode <index> <countrycode|h:for help>`	Sets the country code for the ZyXEL Device. Enter h as the country parameter to view the countries supported by your ZyXEL Device.
`voice config common webdisable <index><0:1>`	Enables or disables configuring the call forwarding feature in the web configurator.
`voice config common save <index>`	Saves the common settings entry in the working buffer to non-volatile memory. The working buffer is a volatile memory space. The settings in the working buffer are not applied to the ZyXEL Device until you execute this command.
`voice config common display <index>`	Displays the saved values for the common settings entry.

20.6.1 VoIP Common Settings Command Examples

This example shows the country codes supported by the ZyXEL Device and selects Poland as the location of the ZyXEL Device.

```
ras> voice config common index 1
ras> voice config common countrycode 1 h
Please input 0 or 42 to select country!254:Default. 255: MRD
0:USA | 1:JAPAN | 2:TAIWAN | 3: AUSTRIA | 4:BELGIUM
5:BULGARIA | 6:CZECH | 7:DENMARK | 8: FINLAND | 9:FRANCE
10:HUNGARY | 11:ICELAND | 12:ITALY | 13: LUXEMBOURG
14:NETHERLAND | 15:NORWAY | 16:POLAND | 17: PORTUGAL
18:SLOVAKIA | 19: SPAIN | 20:SWEDEN | 21:SWITZERLAND
22:UK | 23:GERMANY | 24:GREECE | 25:Australia | 26:New Zealand
27:Hong Kong | 28:Singapore | 29:Morocco | 30:Ireland | 31:Malaysia
32:Russia | 33:Thailand | 34:Israel | 35:UAE | 36:China | 37:Ukraine
38:South Africa | 39:Korea | 40:Philippine | 41:India | 42:Turkey
254:Default | 255:Issue sys default countrycode
ras> voice config common countrycode 1 16
ras> voice config common save 1
```

20.7 VoIP Auto-Provisioning Commands

Use these commans to configure auto-provisioning on the ZyXEL Device.

Table 54 Auto-Provisioning Command Summary

COMMAND	DESCRIPTION
`voice config autopro index <index>`	Specifies the auto-provisioning entry for configuration.
`voice config autopro active <index> <0:off|1:on>`	Enables or disables this auto-provisioning entry.
`voice config autopro servaddr <index> <ip>`	Sets the auto-provisioning server IP address.
`voice config autopro timeout <index> <seconds>`	Sets the auto-provisioning time out value. This is the amount of time that the ZyXEL Device waits for a response from the auto-provisioning.
`voice config autopro retry <index> <seconds>`	Sets the auto-provisioning retry interval. This is the interval at which the ZyXEL Device will try to resend messages to the auto-provisioning server if it fails to get an acknowledgement response.
`voice config autopro protocol <index> <0:TFTP|1:HTTP|2:HTTPS>`	Sets the protocol for sending the auto-provisioning configuration files.
`voice config autopro method <index> <0:Common|1:Bluewin|2:Pincode>`	Sets the method for sending auto-provisioning configuration files.
`voice config autopro phonenumber <index> <phonenumber>`	Sets the phone number identfiying the auto-provisioning request. This is only necessary if the auto-provisioning server requires a phone number to authenticate an auto-provisioning request.
`voice config autopro pincode <index> <pincode>`	Sets the PIN code for this auto-provisioning request. This is only necessary if the auto-provisioning server requires a PIN code to authenticate an auto-provisioning request.

Table 54 Auto-Provisioning Command Summary

COMMAND	DESCRIPTION
`voice config autopro save <index>`	Saves the speed dial entry in the working buffer to non-volatile memory. The working buffer is a volatile memory space. The settings in the working buffer are not applied to the ZyXEL Device until you execute this command.
`voice config autopro display <index>`	Displays the saved values for the speed dial entry.
`voice config autopro dumpCfg <index>`	Displays the configured values in the working buffer for the specified configuration.

20.7.1 VoIP Auto-Provisioning Command Examples

This example enables auto-provisioning on the ZyXEL Device. Specifies the IP address of the auto-provisioning server (**172.16.1.201**). Sets auto-provisioning to use HTTPS to transmit data and specifies which auto-provisioning file to receive by providing the phone number associated with the configuration file.

```
ras> voice config autopro index 1
ras> voice config autopro active 1 1
ras> voice config autopro servaddr 1 172.16.1.210
ras> voice config autopro protocol 1 2
ras> voice config autopro phonenumber 1 5555555
ras> voice config autopro save 1
```

20.8 VoIP PSTN Line Commands

Use these commands to configure the PSTN line on the ZyXEL Device.

Table 55 PSTN Line Command Summary

COMMAND	DESCRIPTION
`voice config fxo index <index>`	Selects a PSTN line index for configuration.
`voice config fxo fxolongdial <index> <long-dial-interval>`	Sets the diallonginterval value. This is the time interval (in seconds) that the ZyXEL Device waits until the first digit is dialed when making a call. If no digit is dialed in this time period the ZyXEL Device sends a busy signal. Enter a value between 0-256.
`voice config fxo dtmfpausedur <index> <short-dial-interval>`	Sets the dialshortinterval value. This is the time interval (in seconds) that the ZyXEL Device waits between digits being dialed when making a call. If time between dialed digits exceeds this value the ZyXEL Device considers the dialing to be completed and calls the number entered. Enter a value between 0-256.
`voice config fxo dtmfdigitdur <index> <dtmf-duration>`	Sets the duration of time that the ZyXEL Device sends DTMF signals through the FXO interface. If this setting is set to 0, then the duration becomes 500 ms.

Table 55 PSTN Line Command Summary

COMMAND	DESCRIPTION
`voice config fxo fxoflashmin <index> <flash-min-interval>`	Sets the fxo flash key min interval value (miliseconds). The flash key being pressed is only recognized by the ZyXEL Device if it is pressed for a longer period than the flash key min interval but a shorter period than the flash key max interval.
`voice config fxo fxoflashmax <index> <flash-max-interval>`	Sets the fxo flash key max interval value (miliseconds). The flash key being pressed is only recognized by the ZyXEL Device if it is pressed for a longer period than the flash key min interval but a shorter period than the flash key max interval.
`voice config fxo fxophselect <index> <phone-port|0:All><0:No|1:Yes>`	Specifies which telephones should receive calls via the PSTN line.
`voice config fxo save <index>`	Saves the PSTN line configuration entry in the working buffer to non-volatile memory. The working buffer is a volatile memory space. The settings in the working buffer are not applied to the ZyXEL Device until you execute this command.
`voice config fxo display`	Displays the saved values for the PSTN line configuration entry.
`voice config fxo dumpCfg`	Displays the configured values in the working buffer for the specified configuration.

20.8.1 VoIP PSTN Line Command Examples

This example sets all telephones connected to the ZyXEL Device to receive calls via the PSTN line.

```
ras> voice config fxo index 1
ras> voice config fxo fxophselect 1 0 1
ras> voice config fxo save 1
```

20.9 VoIP Call Forwarding Commands

Use these commands to configure call-forwarding rules on the ZyXEL Device.

Table 56 Call-forwarding Command Summary

COMMAND	DESCRIPTION
`voice config forward index <index>`	Specifies the call-forwarding table you want to configure.
`voice config forward unconditional <index> <phone-number>`	Specifies the phone number to which the ZyXEL Device forwards all incoming calls.
`voice config forward busy <index> <phone-number>`	Specifies the phone number to which the ZyXEL Device forwards incoming calls when the phone port is busy.
`voice config forward noanswer <index> <phone-number>`	Specifies the phone number to which the ZyXEL Device forwards incoming calls when the call goes unanswered for a period of time you specify in the `voice config forward noanstime` command.
`voice config forward noanstime <index> <seconds>`	Sets the amount of time the ZyXEL Device waits before it considers a call unanswered.

Table 56 Call-forwarding Command Summary

COMMAND	DESCRIPTION

`voice config forward table <index> <entry-id> <caller> <dest> <0:unconditional 1:busy 2:noanswer 3:block 4: accept>`	Sets a call-forwarding rule based on the incoming call number. You can specify the type of call forwarding.
	`0:unconditional`
	`1:busy`
	`2:noanswer`
	`3:block` - drops calls from the specified phone number.
	`4: accept` - this setting overrides general forwarding rules.

`voice config forward clear <index> <entry|uncond|busy|noans|all> <entry_id>`	Deletes a call-forwarding rule.
`voice config forward save <index>`	Saves the call-forwarding rule configuration in the working buffer to permanent memory. The working buffer is a volatile memory space. The settings in the working buffer are not applied to the ZyXEL Device until you execute this command.
`voice config forward display <index>`	Displays the saved values for the specified call forwarding table.
`voice config forward free`	Clears the working buffer for the specified configuration. Any unsaved changes are lost.

20.9.1 VoIP Call Forwarding Command Examples

This example configures the following call forwarding rules:

- If phone is busy, forward to **555-5555**.
- If no Answer within **10** seconds, forward to **555-5555**.

- Forward all calls from telephone number **111-1111** to telephone number **444-4444**.

```
ras> voice config forward index 1
ras> voice config forward busy 1 5555555
ras> voice config forward noanstime 1 10
ras> voice config forward noanswer 1 5555555
ras> voice config forward table 1 1 1111111 4444444 0
ras> voice config forward save 1
ras> voice config forward display 1
       Call Forward Table[1] Display
================================================
SIP forwarding is enabled
unconditional   :
busy   :5555555
no answer   :5555555
no answer time   :10

 Num    caller    dest    type
================================================
 1    1111111    4444444    Unconditional
 2            Unconditional
 3            Unconditional
 4            Unconditional
 5            Unconditional
 6            Unconditional
 7            Unconditional
 8            Unconditional
 9            Unconditional
10            Unconditional
```

20.10 VoIP View RTP Commands

Use these commands to configure RTP settings on the ZyXEL Device.

Table 57 View RTP Command Summary

COMMAND	DESCRIPTION
`voice rtp table`	Displays all the current active RTP session.
`voice rtp usage`	Display all active RTP ports.
`voice rtp statistics <index>`	Displays the RTP statistics.
`voice rtp linktime <index>`	Displays the RTP linktimes.

20.10.1 VoIP View RTP Command Examples

This example views the active RTP ports.

```
ras> voice rtp usage
The used RTP ports are as follows
 50001  50000
```

20.11 VoIP Auto-Provision Commands

Use these commands to execute auto-provisioning functions on the ZyXEL Device.

Table 58 Execute Auto-Provisioning Command Summary

COMMAND	DESCRIPTION
`voice autopro active`	Enables or disables autoprovision of VoIP related settings.
`voice autopro startnow`	Initiates the auto-provisioning process.
`voice autopro terminate`	Stops the auto-provisioning process.
`voice autopro start`	Initiates the autoprovisioning process.
`voice autopro status`	Displays auto-provisioning status. `AUTO_PRO_TRY_NONE`: auto-provision has not been tried. `AUTO_PRO_TRY_ONCE`: auto-provision attempted to run one time, there is no timer running. `AUTO_PRO_TRY_N_SUCCESS`: auto-provision tried to run and succeeded, the timer is set. `AUTO_PRO_TRY_N_FAIL`: auto-provision attempted to run and failed, the timer is set. `AUTO_PRO_ON_PROGRESS`: auto-proviosion is currently running.

20.12 VoIP Dial Plan Commands

Use these commands to configure the dial plan on the ZyXEL Device.

20.12.1 VoIP Dial Plan Overview

One of the first VoIP planning steps is setting up the dial plan that defines how long phone numbers are, which gateways are used to complete calls and whether any manipulation of the numbers dialed should take place.

Dial plans contain specific dialing patterns so that users can reach a particular telephone number. Access codes, area codes, specialized codes, and combinations of the numbers of digits dialed are all a part of any particular dial plan. Dial plans used with voice-capable routers essentially describe the process of determining which and how many digits to store in each of the configurations. If the dialed digits match the number and patterns, the call is processed for forwarding.

All telephony networks require a dial plan that describes what happens when you dial which numbers. In the U.S., for example, there is the North American Numbering Plan, which is why we put a "011" before international calls and "1" before an area code and phone number. These kinds of things are all specified in a dial plan.

20.12.1.1 Dial Rules

The dial plan specifies how to interpret digit sequences dialed by users, and how to convert those sequences into an outbound dial string.

When a user dials a series of digits, each sequence in the dial plan is tested as a possible match. The matching sequences form a set of candidate digit sequences. As more digits are entered by the user, the set of candidates diminishes until only one or none are valid.

Any one of a set of terminating events triggers the device to either accept the user-dialed sequence and transmit it to initiate a call, or else reject it as invalid. The terminating events are:

1. No candidate sequences remain: the number is rejected.
2. Only one candidate sequence remains, and it has been matched completely: the number is accepted and transmitted after any transformations indicated by the dial plan, unless the sequence is rejected by the dial plan.
3. A timeout occurs: the digit sequence is accepted and transmitted as dialed if incomplete, or transformed as per the dial plan if complete.

White space is ignored in dial plans, and may be used for readability. The following table contains rules for creating dial plans:

Table 59 Dial Rule Syntax

SYNTAX	DESCRIPTION
( )	The collection of sequences is enclosed in parentheses.
|	Used to separate multiple dial plan rules.
x	The letter is used as a wildcard, matching any one numeric digit ('0' - '9').
[ ]	A subset of keys within brackets. (e.g. [389] means '3' or '8' or '9'.) - Numeric ranges are allowed within the brackets. (e.g. [2-9] means '2' or '3' or …. or '9'.) - Ranges can be combined with other keys. (e.g. [235-8*] means '2' or '3' or '5' or '6' or '7' or '8' or '*'.)
.	Any element can be repeated zero or more times by appending '.' to the element. For example, "01." matches "0","01", "011", "0111", …… etc.) Note that the command can be used only at the end of a dial plan rule and all digits (0-9,*,#) following '.' will be ignored.
<dialed-subsequence**:** transmitted-subsequence**>**	A subsequence of keys (possible empty) can be automatically replaced with a different subsequence using an angle bracket notation. (e.g. "<8:1650>xxxxxxx" would match "85551212" and transmit to "16505551212".) Note that the command can be used only at the start of a dial plan rule.
!	A sequence can be rejected by placing '!' at the end of the sequence. For example, "1900xxxxxxx!" automatically rejects all 900 area code numbers from being dialed.)
@	A termination character. When the termination character is at the end of the dial sequence, the dial string will be sent immediately. For example, "911@" will send "911" immediately, in other words no delay for any timeout value occurs. Note: The digits following @ will be ignored.
=gwX=	This syntax means "if you match this dial plan listed, dial out this gateway". gw0 is special and means "dial out the default VoIP port". The setting of **gw0** means VoIP gateway, **gw1** means PSTN gateway, **gw2** means ISDN gateway, and **gw3** is reserved for future use. The default setting is VoIP gateway. If there is a setting **gw2** for a dial sequence, the ZyXEL Device will check if ISDN line exists when matching this sequence. If it does not exist, then the ZyXEL Device will dial out via PSTN line. If both ISDN/PSTN line do not exist, the dial number is blocked.

20.12.2 VoIP Dial Plan Command Summary

The following section lists the commands for this feature.

Table 60 Dial Plan Command Summary

COMMAND	DESCRIPTION
`voice dialplan clear`	Clears the dial plan in memory.
`voice dialplan dial <phone-number>`	Simulates dialing digits for dial plan parsing.
`voice dialplan load`	Loads the dial plan from permanent memory and overwrites the dial plan in runtime memory.
`voice dialplan save`	Saves the dial plan to permanent memory.
`voice dialplan set <dial-plan>`	Sets up a dial plan rule. *dial-plan*: You can specify multiple dial plan sequences. The collection of sequences must be enclosed in paranthesis **()**.
`voice dialplan show`	Displays dial plan details.
`voice dialplan switch <0:off|1:on>`	Enables or disables the dial plan.
`voice dialplan debug`	Enables or disables the dial plan debug mode.

20.12.3 VoIP Dial Plan Command Examples

This example configures a dial plan which only allows US-style (1 + area code + local number) dialing sequences.

```
ras> voice dialplan set (1 xxx xxxxxxx)
ras> voice dialplan save
```

This example creates a dial plan that also allows 7-digit US-style dialing, and automatically inserts a 1 + 212 (local area code) in the transmitted number.

```
ras> voice dialplan set (1 xxx xxxxxxx | <:1212> xxxxxxx)
ras> voice dialplan save
```

This example creates a dial plan which requires a user to dial 8 as a prefix for local calls and 9 as a prefix for long distance.

```
ras> voice dialplan set (<9:> 1 xxx xxxxxxx | <8:1212> xxxxxxx)
ras> voice dialplan save
```

This example creates a dial plan which allows US-style long distances, but blocks 9xx area codes.

```
ras> voice dialplan set (1 [2-8]xx [2-9]xxxxxx)
ras> voice dialplan save
```

In this example, the dial plan implements 002 & 003 area code calls being sent out via different gateways.

```
ras> voice dialplan set (1 002 xxxxxxx =gw0= | 1 003 xxxxxxx =gw1=)
ras> voice dialplan save
```

The next example illustrates a more complex dial plan:

- If one dials 3433334545, system will dial out 3434545 via default VoIP network (gateway 0).
- If one dials 3434444545, system will dial out 4443434444545 via ISDN network (gateway 2).
- If one dials 54321, system will dial out 54321 via default PSTN network (gateway 1).

```
ras> voice dialplan set (xx<333:>x. | <:444>[1-3]x. =gw2= | x. =gw1=)
ras> voice dialplan save
```

21

WAN Commands

Use these commands to configure the ZyXEL Device's WAN settings.

21.1 wan adsl Commands

Use these commands to configure the ZyXEL Device's ADSL interface settings.

Table 61 wan adsl Commands

COMMAND	DESCRIPTION
`wan adsl chandata`	Shows the ADSL channel data and line rate.
`wan adsl close`	Closes the ADSL line.
`wan adsl coinfo`	Displays information on the current modem status.
`wan adsl fwversion`	Displays the current DSL firmware version.
`wan adsl linedata far`	Shows ADSL far end noise margin and carrier load information.
`wan adsl linedata near`	Shows ADSL near end noise margin and carrier load information.
`wan adsl open`	Opens the ADSL line.
`wan adsl opencmd <adsl2|adsl2+|gdmt|multimode>`	Opens the ADSL line with the specified standard.
`wan adsl opmode`	Shows the ADSL operational mode (standard).
`wan adsl perfdata`	Shows performance information such as the CRC, FEC, error seconds.
`wan adsl rateadap <on|off>`	Activates or deactivates rate adaption.
`wan adsl reset`	Resets the ADSL modem to the saved configuration.
`wan adsl status`	Displays ADSL status (up, down or initializing).
`wan adsl targetnoise <target_noise_margin>`	Sets the target noise margin. *target_noise_margin*: -31 ~ 32.
`wan adsl version`	Displays the ADSL firmware version.

21.1.1 wan adsl Examples

The following example:

- Resets the ADSL modem.
- Displays the firmware version.

- Opens the ADSL line in ADSL2+ mode.
- Activates rate adaption.
- Displays the ADSL operation mode.
- Displays ADSL status.

```
ras> wan adsl reset
.....................................................................
.
.............ras>
ras> wan adsl version
ADSL Chipset Vendor: TI AR7 06.00.04.00
ras> wan adsl open adsl2+
ras> wan adsl rateadap on
ras> wan adsl opmode
DSL standard: NORMAL
ras> wan adsl status
current modem status: down
ras>
```

21.2 wan atm Commands

Use these commands to configure the ZyXEL Device's ATM (Asynchronous Transfer Mode) settings.

Table 62 wan atm Commands

COMMAND	DESCRIPTION
`wan atm vchunt active <yes|no>`	Enables or disables the virtual circuit (VC) auto-hunting feature.
`wan atm vchunt add <node-id> <vpi> <vci> <service-bit-hex>`	Configures a virtual circuit hunting pool entry. <*node-id*> : input the remote node index 1-8 <*vpi*>: VPI value <*vci*>: VCI value <*service-bit-hex*>: This is a six-bit field which controls the services the ZyXEL Device searches. The bits control the following services: Bit 0 (1): PPPoE/VC Bit 1 (2): PPPoE/LLC Bit 2 (4): PPPoA/VC Bit 3 (8): PPPoA/LLC Bit 4 (16): Enet/VC Bit 5 (32): Enet/LLC You must enter the parameter value in hexadecimal format. For example, if you want to enable PPPoA/VC (4 in decimal) and Enet/LLC (32 in decimal), enter "24" (4 + 32 = 36 in decimal = 24 in hexadecimal). Note: Use the `wan atm vchunt save` command to add the entry to the hunt pool.

Table 62 wan atm Commands (continued)

COMMAND	DESCRIPTION
`wan atm vchunt clear`	Clears the virtual circuit configuration working buffer.
`wan atm vchunt display`	Displays the virtual circuit hunt pool (the group of parameters the ZyXEL Device checks for an active VC).
`wan atm vchunt remove <node#> <vpi> <vci>`	Removes the entry with the specified profile number, VPI and VCI from the hunt pool. <*node#*>: input the remote node index 1-8 <*vpi*>: VPI value <*vci*>: VCI value
`wan atm vchunt result`	Displays the VC hunt result.
`wan atm vchunt save`	Saves the current setting in the virtual circuit hunt pool working buffer to the permanent memory. Note: Changes to the configuration in the working buffer are not saved or used until you enter this command.
`wan atm vchunt send`	Manually starts the VC auto-hunt.
`wan atm vchunt timer <seconds>`	Sets the length of time the ZyXEL Device waits before checking the virtual circuit hunt result.
`wan atm vchunt webRedirDis <1|0>`	Enables or disables web redirection. Enter 1 to disable web redirection, or enter 0 to disable it.

21.2.1 wan atm Examples

The following example:

- Enables VC hunting.
- Configures VC hunting to hunt remote node 1 with a VPI of 30 and a VCI of 33.
- Sets the ZyXEL Device to search all services.
- Displays the VC hunt parameters.

- Saves the current configuration.

```
ras> wan atm vchunt active yes
ras> wan atm vchunt add 2 30 33 63
ras> wan atm vchunt display
(1) Configure Buffer
Flags: Active
 RN VPI   VCI   service
----------------------
  1  30  33   63H
(2) RemoteNode (Read Only)
 RN VPI   VCI | RN VPI   VCI | RN VPI   VCI | RN VPI   VCI |
-------------------------------------------------------------
  1   8    35 |  2   0     0 |  3   0     0 |  4   0     0 |
  5   0     0 |  6   0     0 |  7   0     0 |  8   0     0 |
  9   0     0 |
(3) VC Hunt Table: (User setting)
 Flags: Active(1)
 RN VPI   VCI serv| RN VPI   VCI serv| RN VPI   VCI serv| RN VPI  VCI serv
-------------------------------------------------------------------------
  1   0  33   3fH|  1   0  35   3fH|  1   1  35   3fH|  1   8  32   3fH|
  1   0 101   3fH|  1   0  50   3fH|  1   0  32   3fH|  1  14  24   3fH|
  1   0  38    4H|  0   0   0    0H|
(4) WebRedirect: Enable
ras> wan atm vchunt save
ras>
```

21.3 wan backup Commands

Use these commands to configure the ZyXEL Device's WAN backup settings.

Table 63 wan backup Commands

COMMAND	DESCRIPTION
`wan backup 1checkip <ip-address>`	Specifies the first IP address to check for connectivity (when `icmp` checking is activated).
`wan backup 2checkip <ip-address>`	Specifies the second IP address to check for connectivity (when `icmp` checking is activated).
`wan backup 3checkip <ip-address>`	Specifies the third IP address to check for connectivity (when `icmp` checking is activated).
`wan backup checkmech <icmp|dsllink>`	Specifies the method the ZyXEL Device uses to check the DSL connection. `icmp`: periodically ping the `checkip` IP addresses. `dsllink`: check the connection to the DSLAM.
`wan backup dialbackup active <0:off|1:on>`	Activates or deactivates dial up backup.
`wan backup dialbackup ATcommand answer <command>`	Sets the AT command used to answer a call.
`wan backup dialbackup ATcommand dial <command>`	Sets the AT command used to make a call.
`wan backup dialbackup ATcommand drop <command>`	Sets the AT command used to end a call.

Table 63 wan backup Commands (continued)

COMMAND	DESCRIPTION
`wan backup dialbackup ATresponse callid <call-id>`	Specifies the keyword preceding the dialed number.
`wan backup dialbackup ATresponse clid <clid>`	Sets the keyword preceding the Calling Line Identification in the AT response
`wan backup dialbackup ATresponse speed <speed>`	Specifies the keyword preceding the connection speed.
`wan backup dialbackup callctl callbackdelay <seconds>`	Sets the number of seconds the ZyXEL Device waits between dropping a callback request call and dialing the corresponding callback call.
`wan backup dialbackup callctl dialtimeout <seconds>`	Sets the number of seconds the ZyXEL Device tries to make a call before timing out.
`wan backup dialbackup callctl droptimeout <seconds>`	Sets the number of seconds the ZyXEL Device waits before dropping the DTR signal if it does not receive a positive disconnect confirmation.
`wan backup dialbackup callctl retrycount <metric>`	Sets the number of times the ZyXEL Device tries a busy or no-answer phone number before blacklisting it.
`wan backup dialbackup callctl retryinterval <seconds>`	Sets the number of seconds the ZyXEL Device waits before calling a busy or unanswered number again.
`wan backup dialbackup dropDTR <0:no|1:yes>`	Activates or deactivates the dropping of the Data Terminal Ready (DTR) signal after the `wan backup dialbackup ATcommand drop <command>` string is issued.
`wan backup dialbackup init <command>`	Sets the AT command used to initialize the WAN device connected to the dial backup port.
`wan backup dialbackup portspeed <1:9600|2:19200|3:38400|4:57600|5:115200|6:230400>`	Sets the speed of the connection between the dial backup port and the external device.
`wan backup display`	Shows the WAN backup information currently stored in the memory buffer.
`wan backup free`	Clears the WAN backup information in the working buffer. Note: Use this command before working on another WAN backup profile.
`wan backup icmptimeout <seconds>`	Sets the timeout in seconds for an ICMP ping.
`wan backup load`	Loads the WAN backup configuration into the working buffer.
`wan backup recovery <seconds>`	Sets the number of seconds the ZyXEL Device waits, when using a WAN backup connection, before trying to reconnect using the higher priority connection.
`wan backup save`	Saves the current setting in the WAN backup working buffer to the permanent memory. Note: Changes to the configuration in the working buffer are not saved or used until you enter this command.

Table 63 wan backup Commands (continued)

COMMAND	DESCRIPTION
`wan backup tolerance <0~9>`	Sets the number of failed responses the ZyXEL Device may receive when pinging the `checkip` IP addresses before switching to a WAN backup connection.
`wan backup trafficredirect active <0:no|1:yes>`	Activates or deactivates traffic redirection to a backup gateway.
`wan backup trafficredirect backIp <address>`	Sets the backup gateway's IP address for traffic redirection.
`wan backup trafficredirect metric <number>`	Specifies the metric value for traffic redirection.

21.3.1 wan backup Examples

The following example:

- Loads the WAN backup configuration information.
- Specifies the following IP addresses to check: 192.168.1.100, 192.168.1.150, 192.168.1.175
- Sets the ZyXEL Device to periodically ping the IP addresses.
- Sets the timeout in seconds for an ICMP ping to 5.
- Sets the tolerance to 5.
- Sets the recovery interval to 60.
- Activates dial backup.
- Sets the AT command used to answer a call to "A0".
- Sets the number of seconds the ZyXEL Device tries to make a call before timing out to 20.
- Sets the number of times the ZyXEL Device tries a busy or no-answer phone number before blacklisting it to 10.
- Sets the dial backup port speed to 9600.
- Saves the current setting in the WAN backup working buffer to the permanent memory.

- Displays the WAN backup configuration.

```
ras> wan backup load
ras> wan backup 1checkip 192.168.1.100
ras> wan backup 2checkip 192.168.1.150
ras> wan backup 3checkip 192.168.1.175
ras> wan backup checkmech icmp
ras> wan backup icmp 10
ras> wan backup tolerance 5
ras> wan backup recovery 60
ras> wan backup dialbackup active 1
ras> wan backup dialbackup ATcommand answer A0
ras> wan backup dialbackup callctl dialtimeout 20
ras> wan backup dialbackup callctl retrycount 10
ras> wan backup dialbackup portspeed 1
ras> wan backup save

save ok.
ras> wan backup display

------Wan Backup Setup-----
                      Check Mechanis:  ICMP
                Check WAN IP Address1:  192.168.1.100
                Check WAN IP Address2:  192.168.1.150
                Check WAN IP Address3:  192.168.1.175
             KeepAlive Fail Tolerance:  5
               Recovery Interval(sec):  60
                    ICMP Timeout(sec):  10
------Traffic Redirect Setup-----
                     traffic Active::   No
          Backup Gateway IP Address::   0.0.0.0
                              Metric::   15
-------Dial Backup Setup-------
                          dial Active:   Yes
                    dial Port Speed::   9600
                                Init::   at&fs0=0
AT Command Strings:
                                Dial::   atd
                                Drop::   ~~+++~~ath
                              Answer::   A0
              Drop DTR When Hang Up::   No
AT Response Strings:
                                CLID::   NMBR =
                           Called Id::
                               Speed::   CONNECT
Call Control:
                  Dial Timeout(sec)::   20
                        Retry Count::   10
                 Retry Interval(sec)::   10
                   Drop Timeout(sec)::   20
                Call Back Delay(sec)::   15
ras>
```

21.4 wan callsch Commands

Use these commands to configure call scheduling on the ZyXEL Device.

Table 64 wan callsch Commands

COMMAND	DESCRIPTION
`wan callsch action <0:force on|1:force down|2:enable dial-on-demand|3:disable dial-on-demand>`	Sets the type of action performed by the previously-specified call schedule.
`wan callsch active <yes|no>`	Activates or deactivates the previously-specified call schedule.
`wan callsch clear`	Resets the configuration of the previously-specified call schedule to its default values.
`wan callsch display`	Displays the current configuration of the previously-specified call schedule.
`wan callsch duration <hour> <minute>`	Sets the length of time the previously-specified call schedule should remain active.
`wan callsch freeMemory`	Clears the call schedule information in the working buffer. Note: Use this command before working on another call schedule profile.
`wan callsch index <set#>`	Specifies the call scheduling profile number to work with. Note: Use this command to specify the call schedule profile before using other `wan callsch` commands.
`wan callsch name <set-name>`	Sets the name of the previously-specified call schedule.
`wan callsch oncedate <year> <month> <day>`	Sets a single date on which the previously-specified call schedule should be in effect.
`wan callsch save`	Saves the configuration of the previously-specified call schedule. Note: Changes to the configuration in the working buffer are not saved or used until you enter this command.
`wan callsch startdate <year> <month> <day>`	Sets the date on which the previously-specified call schedule starts.
`wan callsch starttime <hour> <minute>`	Sets the time of day at which the previously-specified call schedule should become active.
`wan callsch weeklyday <Monday|Tuesday|Wednesday|Thursday|Friday|Satudray|Sunday> <0:inactive|1:active>`	Sets the day(s) of the week on which the previously-specified call schedule should be active.

21.4.1 wan callsch Examples

The following example:

- Clears the call schedule information from the working buffer.
- Specifies call schedule set 1.
- Sets the name to be "Schedule1".
- Sets the action to be forced off.
- Sets the call schedule to take effect on the first of January 2010 at three o'clock in the afternoon.
- Sets the call schedule to remain in effect for 23 hours and 59 minutes.
- Sets the call schedule to be in effect on Mondays and Tuesdays only.
- Activates the schedule.
- Displays the schedule configuration.

```
ras> wan callsch clear
ras> wan callsch index 1
ras> wan callsch name Schedule1
ras> wan callsch action 1
ras> wan callsch startdate 2010 01 01
ras> wan callsch starttime 15 00
ras> wan callsch weeklyday Monday 1
ras> wan callsch weeklyday Tuesday 1
ras> wan callsch duration 23 59
ras> wan callsch active yes
ras> wan callsch display

Schedule Set# = 1
Set name:Schedule1
Active= Yes
Start Date(yyyy-mm-dd)= 2010-01-01
How Often=Weekly
Once:
  Date(yyyy-mm-dd)= N/A
Weekdays:
  Sunday   =No
  Monday   =Yes
  Tuesday  =Yes
  Wednesday=No
  Thursday =No
  Friday   =No
  Saturday =No
Start Time(hh:mm)=  15 : 00
Duration(hh:mm)=  23 : 59
Action= Forced Down
ras>
```

21.5 wan hwsar Commands

Use these commands to see SAR (Segmentation And Reassembly) and HAL (Hardware Abstraction Layer) statistics, and conduct ATM tests.

Table 65 wan hwsar Commands

COMMAND	DESCRIPTION
`wan hwsar clear`	Resets SAR and HAL incoming and outgoing packet counters.
`wan hwsar disp`	Displays SAR (Segmentation And Reassembly) and HAL (Hardware Abstraction Layer) incoming and outgoing packet statistics.
`wan hwsar driver config`	Displays SAR and HAL configuration information.
`wan hwsar driver dischan <channel>`	Discards the specified channel.
`wan hwsar driver oammode mode:<0|1>`	Sets the Operation, Administration, and Maintenance (OAM) mode. `0`: firmware OAM mode. `1`: host OAM mode.
`wan hwsar driver test <vpi> <vci> <count> <0|1>`	Performs an ATM test on the specified connection. `0`: send packet. `1`: internal loopback.

21.5.1 wan hwsar Examples

The following example:

- Displays SAR and HAL packet statistics.
- Selects firmware mode OAM.
- Performs an internal loopback test.

```
ras> wan hwsar disp
SAR Driver Counters Display:
inPkts        = 0x00000000, inDiscards    = 0x00000000
outPkts       = 0x00000000, outDiscards   = 0x00000000
inF4Pkts      = 0x00000000, outF4Pkts     = 0x00000000
inF5Pkts      = 0x00000000, outF5Pkts     = 0x00000000
openChan      = 0x00000000, closeChan     = 0x00000000
txRate(Bps)   =          0, rxRate(Bps)   =          0

HAL Stats Display Ch 0:
Rx Total      = 0x00000000, Tx Total      = 0x00000000
Rx Peak       = 0x00000000, TxH Peak      = 0x00000000
TxL Peak      = 0x00000000, CrcErr        = 0x00000000
LenErr        = 0x00000000, DmaLenErr     = 0x00000000
AbortErr      = 0x00000000, StarvErr      = 0x00000000
TxH MisQ Cnt  = 0x00000000, TxL MisQ Cnt  = 0x00000000
Rx MisQ Cnt   = 0x00000000, Tx DMA Busy   = 0x00000000
Rx EOQ Cnt    = 0x00000000, TxH EOQ Cnt   = 0x00000000
TxL EOQ Cnt   = 0x00000000, Rx Pkts       = 0x00000000
TxH Pkts      = 0x00000000, TxL Pkts      = 0x00000000
ras> wan hwsar driver oammode 0
ras> wan hwsar driver test 30 33 2 1
```

21.6 wan node Commands

Use these commands to configure the WAN ISP and backup nodes.

Table 66 wan node Commands

COMMAND	DESCRIPTION
`wan node backup <enable|disable>`	Activates or deactivates the backup WAN node. Note: Use the `wan node index 9` command to specify the backup WAN node.
`wan node backup filter <incoming|outgoing> <profile>`	Sets the filter action and profile to be used by the previously-specified WAN backup node. `incoming`: the filter applies to traffic coming from the WAN to the LAN. `outgoing`: the filter applies to traffic coming from the LAN to the WAN. *`profile`*: profile number 1 ~ 4. Use the `sys filter set` commands to configure filter profiles.
`wan node backup idletimeout <seconds>`	Sets the idle timeout for the previously-specified WAN backup node.
`wan node backup ispname <name>`	Sets the ISP name for the previously-specified WAN backup node.
`wan node backup metric <metric>`	Sets the metric value (number of transmission hops) for the previously-specified WAN backup node.
`wan node backup multicast <none|igmpv1|igmpv2>`	Sets the multicast mode of the previously-specified WAN backup node.
`wan node backup nailedup <on|off>`	Activate or deactivate a nailed-up (always on) connection for the previously-specified WAN backup node.
`wan node backup nat <off|sua|full <address mapping rule #>>`	Sets the Network Address Translation (NAT) mode of the previously-specified WAN backup node. `<off>`: NAT is not active `<sua>`: Use Single User Account only (if you have just one public WAN IP address for your ZyXEL Device). `<full>` : Use full-feature NAT (if you have multiple public WAN IP addresses for your ZyXEL Device). *`<address mapping rule #>`* : When you choose full-feature NAT, specify the address mapping rule to apply. Use the `ip nat addrmap rule` command to configure address mapping rules.
`wan node backup ppp authen <chap|pap|both>`	Sets the authentication method for the backup WAN node (use the `wan node index 9` command to specify the backup WAN node).
`wan node backup ppp idletime <seconds>`	Sets the PPP idle timeout for the previously-specified backup WAN node.
`wan node backup ppp password <password>`	Sets the password for the previously-specified backup WAN node.
`wan node backup ppp username <name>`	Sets the username for the backup WAN node (use the `wan node index 9` command to specify the backup WAN node).

Table 66 wan node Commands (continued)

COMMAND	DESCRIPTION
`wan node backup pppopt com <yes|no>`	Activates or deactivates PPP compression on the previously-specified WAN backup node.
`wan node backup pppopt encap <std|cisco>`	Sets the PPP encapsulation mode of the previously-specified WAN backup node. `std`: standard PPP encapsulation. `cisco`: Cisco PPP encapsulation.
`wan node backup priph <primary-phone#>`	Specifies the phone number the ZyXEL Device should call in order to make a connection to the previously-specified backup WAN node.
`wan node backup private <yes|no>`	Specifies whether the previously-specified WAN backup node is private or not.
`wan node backup remoteip <ip-address> <subnet mask>`	Sets the remote gateway IP address and subnet mask of the previously-specified WAN backup node.
`wan node backup rip <none|in|out|both>`	Sets the Routing Information Protocol (RIP) mode and type of the previously-specified WAN backup node.
`wan node backup script set <1~6> <expect> <send>`	Configures the specified PPP chat script to transmit the defined *send* string when it receives the defined *expect* string. For example, the command: `wan node backup set 2 123 456` sets script 2 to transmit “456” when it receives “123”. Note: Use the `wan node index 9` command to specify the backup WAN node.
`wan node backup secph <secondary-phone#>`	Specifies the backup phone number the ZyXEL Device should call in order to make a connection to the previously-specified backup WAN node. The ZyXEL Device calls this number if the primary phone number is busy or does not answer.
`wan node backup wanip <static <ip-address>|dynamic>`	Sets the WAN IP address and mode (static or dynamic) of the previously-specified WAN backup node.
`wan node bridge <on|off>`	Activates or deactivates bridge mode on the previously-specified WAN node profile.
`wan node bridgetimeout <minutes>`	Type the time (in minutes) for the ZyXEL Device to retain the Ethernet address information in its internal tables while the line is down. If this information is retained, your ZyXEL Device will not have to recompile the tables when the line comes back up.
`wan node callsch <set#1> <set#2> <set#3> <set#4>`	Sets the call scheduling profile(s) used by the previously-specified WAN node profile. Use the `wan callsch` commands to configure call scheduling profiles.
`wan node clear`	Returns the WAN node you previously specified with the `wan node index <node#>` command to its defaults.
`wan node disable`	Deactivates the previously-specified WAN node profile.

Table 66 wan node Commands (continued)

COMMAND	DESCRIPTION
`wan node display`	Displays configuration details of the previously-specified WAN node currently in the working buffer.
`wan node enable`	Activates the previously-specified WAN node profile.
`wan node encap <1483|pppoa|pppoe|enet>`	Sets the encapsulation method used by the previously-specified WAN node profile. `<1483>`: RFC1483 `<pppoa>`: Point-to-Point Protocol over ATM `<pppoe>`: Point-to-Point Protocol over Ethernet `<enet>`: Ethernet encapsulation.
`wan node filter <incoming|outgoing|call> <tcpip|generic> <profile>`	Specifies the filter action, type and profile to be used for traffic to or from the previously-specified WAN node profile. `incoming`: the filter applies to traffic coming from the WAN to the LAN. `outgoing`: the filter applies to traffic coming from the LAN to the WAN. `call`: determines whether a packet should be allowed to trigger a call. `tcpip`: filters IP packets only. `generic`: filters based on a packet's MAC address. *`profile`*: profile number 1 ~ 4. Use the `sys filter set` commands to configure filter profiles.
`wan node freememory`	Clears the WAN node information in the working buffer. Note: Use this command before working on another WAN node profile.
`wan node index <node#>`	Sets the node pointer to the specified WAN node profile. • 1 is the ISP node profile. • 9 is the backup node profile. Note: Use this command to specify the node profile before using other `wan node` commands.
`wan node ippolicy <profile#>`	Sets the IP policy profile to be used by the previously-specified WAN node profile. *`profile#`*: profile number 0 ~ 12.
`wan node ispname <name>`	Sets the ISP name for the node you previously specified with the `wan node index <node#>` command.
`wan node mbs <mbs>`	Sets the Maximum Burst Size (MBS) of the previously-specified WAN node profile.
`wan node metric <metric>`	Sets the metric value (number of transmission hops) of the previously-specified WAN node profile.
`wan node mtu <512~1500>`	Sets the Maximum Transmission Unit (MTU) to define the size of the largest packet allowed on the specified WAN node.

Table 66 wan node Commands (continued)

COMMAND	DESCRIPTION
`wan node multicast <none|igmpv1|igmpv2>`	Sets the multicast mode of the previously-specified WAN node profile.
`wan node mux <vc|llc>`	Sets the multiplexing protocol used by the previously-specified WAN node profile. <vc>: virtual circuit-based <llc>: logical link control-based
`wan node nailedup <on|off>`	Activates or deactivates a nailed-up (always on) connection for the previously-specified WAN node profile.
`wan node nat <none|sua|<full <rule#>>`	Sets the Network Address Translation (NAT) method of the previously-specified WAN node profile. <off>: NAT is not active <sua>: Use Single User Account only (if you have just one public WAN IP address for your ZyXEL Device). <full> : Use full-feature NAT (if you have multiple public WAN IP addresses for your ZyXEL Device). <*rule#*> : When you choose full-feature NAT, specify the address mapping rule to apply. Use the `ip nat addrmap rule` command to configure address mapping rules.
`wan node pcr <pcr>`	Sets the Peak Cell Rate (PCR) of the previously-specified WAN node profile.
`wan node ppp authen <pap|chap|both>`	Sets the PPP authentication method for the previously-specified WAN node profile.
`wan node ppp idletime <seconds>`	Sets the PPP idle timeout.
`wan node ppp password <password>`	Sets the PPP password for the previously-specified WAN node profile
`wan node ppp username <username>`	Sets the PPP user name for the previously-specified WAN node profile
`wan node private <yes|no>`	Specifies whether the previously-specified WAN node is private or not. This command determines whether or not the ZyXEL Device includes the route to this remote node in its RIP broadcasts. If you select `yes`, this route is not included in RIP broadcast. If you select `no`, the route to this remote node is propagated to other hosts through RIP broadcasts.
`wan node qos <ubr|cbr|vbr_nrt|vbr_rt>`	Sets the QoS (Quality of Service) type used by the previously-specified WAN node profile. <ubr>: Unspecified Bit Rate <cbr>: Constant Bit Rate <vbr_nrt>: Variable Bit Rate (Non-Real-Time) <vbr_rt>: Variable Bit Rate (Real-Time)
`wan node remoteip <ip-address> <subnet>`	Sets the remote gateway IP address of the previously-specified WAN node profile.
`wan node rip <none|in|out|both> <rip1|rip2b|rip2m>`	Sets the Routing Information Protocol (RIP) mode and type of the previously-specified WAN node profile.

Table 66 wan node Commands (continued)

COMMAND	DESCRIPTION
`wan node routeip <on|off>`	Activates or deactivates IP routing on the previously-specified WAN node profile.
`wan node save`	Saves configured information about the WAN node you previously specified with the `wan node index` <*node#*> command to the permanent memory. Note: Changes to the configuration in the working buffer are not saved or used until you enter this command.
`wan node scr <scr>`	Sets the Sustainable Cell Rate (SCR) of the previously-specified WAN node profile.
`wan node service <name>`	Sets the PPPoE service name of the previously-specified WAN node profile.
`wan node vci <vci>`	Sets the VCI (Virtual Channel Identifier) of the previously-specified WAN node profile.
`wan node vpi <vpi>`	Sets the VPI (Virtual Path Identifier) of the previously-specified WAN node profile.
`wan node wanip <<static> <ip>>|<dynamic>`	Sets the WAN IP address of the previously-specified WAN node profile.

21.6.1 wan node Examples

The following example:

- Sets the active node profile to node 1 (the ISP node profile).
- Sets the profile name to "ISP1".
- Sets the multicast mode to IGMP version 2.
- Sets the NAT mode to SUA only.
- Sets the PPP authentication method to CHAP.
- Sets the PPP username to "User1".
- Sets the PPP password to "Pass1".
- Sets the PPP idle timeout to 240 seconds.
- Sets the remote gateway IP address to 192.168.1.254, with a subnet mask of 255.255.255.0.
- Activates IP routing.
- Sets the service name to "ISPservice".
- Sets the VPI to 30 and the VCI to 33.
- Sets the WAN IP address to be dynamic.
- Saves the settings.
- Sets the active node profile to node 2 again.

- Displays the configuration.

```
ras> wan node index 1
ras> wan node ispname ISP1
ras> wan node multicast igmpv2
ras> wan node nat sua
ras> wan node ppp authen chap
ras> wan node ppp username User1
ras> wan node ppp password Pass1
ras> wan node ppp idletime 240
ras> wan node remoteip 192.168.1.254 255.255.255.0
ras> wan node routeip on
ras> wan node service ISPservice
ras> wan node vpi 30
ras> wan node vci 33
ras> wan node wanip dynamic
ras> wan node save
wan node: save ok
ras> wan node index 1
ras> wan node display
WAN node index = 1
Active = yes
Route IP = on
Bridge = off
Name = ISP1
Encapsulcation <2:PPPoE|3:RFC1483|4:PPPoA|5:Enet Encap> = 5
Mux <1:LLC|2:VC> = 1
VPI/VCI = 30 / 33
PPPoE service name = ISPservice
PPP username = User1
PPP password = Pass1
PPP authentication <1:PAP|2:CHAP|3:BOTH> = 2
SUA/NAT is enabled, NAT lookupset = 255
Dynamic IP address
WAN IP address            = 0.0.0.0
Remote IP address         = 0.0.0.0
Remote IP subnet mask = 0.0.0.0
Idle timeout = 240
Call scheduling set =   0  0  0  0
Nailed-up connection = off
QOS Type <2:CBR|3:UBR|4:VBR_nRT|5:VBR_RT> = 3
QOS PCR/SCR/MBS =     0,    0,    0
RIP direction <0:none|1:both|2:in|3:out>= 0
RIP version <0:RIP-1|1:RIP-2B|2:RIP-2M> = 0
Multicast <0:IGMP-v2|1:IGMP-v1|2:none>  = 0
Incoming protocol filter set =   0  0  0  0
Incoming device filter set       =   0  0  0  0
Outgoing protocol filter set =   0  0  0  0
Outgoing device filter set       =   0  0  0  0
Call protocol filter set =   0  0  0  0
Call device filter set   =   0  0  0  0
ras>
```

21.7 wan tr069 Commands

Use these commands to configure the ZyXEL Device's TR-069 auto-configuration settings.

Table 67 wan tr069 Commands

COMMAND	DESCRIPTION
`wan tr069 acsUrl <url>`	Specifies the URL of the TR-069 auto-configuration server.
`wan tr069 active <0:no|1:yes>`	Activates or deactivates remote management via TR-069 on the WAN.
`wan tr069 debug <on|off>`	Activates or deactivates TR-069 debugging.
`wan tr069 display`	Shows the current TR-069 configuration.
`wan tr069 dump dbglog`	Displays TR-069 logs.
`wan tr069 dump notification`	Shows the TR-069 notification parameter table.
`wan tr069 dump parameters [name] [NextLevel] [flag]`	Shows a list of TR-069 notification parameters.
`wan tr069 gateway active <0:no|1:yes>`	Enables or disables remote management through a NAT router.
`wan tr069 gateway display`	Shows the current TR-069 gateway status.
`wan tr069 gateway notifylimit <seconds>`	Sets the time interval at which the gateway notifies the ACS when a Device entry is added to or removed from the ManageableDevice table. The gateway is a NAT router between the ZyXEL Device and the ACS.
`wan tr069 informInterval <seconds>`	Sets the frequency with which the ZyXEL Device sends information to the auto-configuration server.
`wan tr069 informTime <yyyy>-<mm>-<dd>T<hh>:<mm>:<ss>`	Sets the date and time at which the ZyXEL Device sends information to the auto-configuration server.
`wan tr069 load`	Loads the TR-069 configuration.
`wan tr069 password <password>`	Sets the TR-069 password for authentication with the auto-configuration server.
`wan tr069 periodicEnable <0:disable|1:enable>`	Enables or disables the periodic sending of information to the auto-configuration server.
`wan tr069 reqpassword <password>`	Sets the TR-069 connection request password. When the auto-configuration server makes a connection request to the ZyXEL Device, this password is used to authenticate the auto-configuration server.
`wan tr069 reqport <1001 ~ 65535>`	Sets the port number of the TR-069 connection request.
`wan tr069 requsername <username>`	Sets the TR-069 connection request user name. When the auto-configuration server makes a connection request to the ZyXEL Device, this user name is used to authenticate the auto-configuration server.
`wan tr069 reset`	Resets the TR-069 configuration to its factory defaults.
`wan tr069 routeRN <0 ~ 7>`	Sets the remote node through which the ZyXEL Device routes the TR-069 connection requests.

Table 67 wan tr069 Commands (continued)

COMMAND	DESCRIPTION
`wan tr069 save`	Saves the TR-069 configuration. Note: Changes to the configuration in the working buffer are not saved or used until you enter this command.
`wan tr069 status`	Displays the TR-069 status.
`wan tr069 stun active <0:no|1:yes>`	Enables or disables the use of TR-069 STUN. STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) allows the ZyXEL Device to find the presence and types of NAT routers and/or firewalls between it and the public Internet. STUN also allows the ZyXEL Device to find the public IP address that NAT assigned, so the ZyXEL Device can embed it in the data stream.
`wan tr069 stun display`	Shows the STUN settings.
`wan tr069 stun notifylimit <seconds>`	Sets the time interval at which the ZyXEL Device sends the STUN binding requests.
`wan tr069 stun srvaddr`	Sets the IP address of the STUN server.
`wan tr069 stun srvport`	Sets the STUN server port.
`wan tr069 stun username <username>`	Sets the user name for registration with the STUN server.
`wan tr069 stun password`	Sets the password for registration with the STUN server.
`wan tr069 stun maxkeepperiod`	Sets the maximum keep alive period for which the NAT binding is maintained.
`wan tr069 stun minkeepperiod`	Sets the minimum keep alive period for which the NAT binding is maintained.
`wan tr069 username <username>`	Sets the TR-069 user name for authentication with the auto-configuration server.

21.7.1 wan tr069 Examples

The following example:

- loads the TR-069 configuration.
- Sets the auto-configuration server address to 192.168.1.151.
- Sets the inform interval to 3600 seconds.
- Enables periodic sending of information to the auto-configuration server.
- Sets the connection request password to be "ConnReq1001".
- Sets the connection request username to be "ConnReqUser1".
- Sets the username to be "ACSauth1"
- Sets the password to be "ACSauthpass1"
- Activates TR-069.
- Displays the configuration.

- Saves the configuration.

```
ras> wan tr069 load
ras> wan tr069 acsUrl 192.16.1.151

Auto-Configuration Server URL: http://192.168.1.151
ras> wan tr069 informInterval 3600

TR069 Informinterval 3600
ras> wan tr069 periodicEnable 1
ras> wan tr069 reqpassword ConnReq1001

ConnectionRequestPassword: ConnReq1001
ras> wan tr069 requsername ConnReqUser1

ConnectionRequestUserName: ConnReqUser1
ras> wan tr069 username ACSauth1

Username: ACSauth1
ras> wan tr069 password ACSauthpass1

Password: ACSauthpass1
ras> wan tr069 active 1
ras> wan tr069 display

                        TR069 Active:  Yes
       Auto-Configuration Server URL:  http://192.168.1.151
                 PeriodicInformEnable:  Enabled
              PeriodicInformInterval:  3600
                  PeriodicInformTime:  2009-11-11T22:30:00
                         TR069 Debug:  Disable
                            Username:  ACSauth1
                            Password:  ACSauthpass1
           ConnectionRequestUsername:  ConnReqUser1
           ConnectionRequestPassword:  ConnReq1001
ras> wan tr069 save
ras>
```

21.8 wan zeroCfg Commands

Use these commands to configure the ZyXEL Device's zero configuration settings.

Table 68 wan zeroCfg Commands

COMMAND	DESCRIPTION
`wan zeroCfg <on|off>`	Enables or disables zero configuration.
`wan zeroCfg debug <0:off|1:on>`	Enables or disables zero configuration debugging.

Table 68 wan zeroCfg Commands (continued)

COMMAND	DESCRIPTION

`wan zeroCfg flag <0~7>`	Use this command to configure the zero configuration settings.
	This command allows you to configure three parameters:
	`zeroCfh`: zero configuration.
	`auto-hunt`: VPI/VCI auto-hunting.
	`password`: user password.
	This is a binary data field with three bits, so you can control the three parameters by entering decimal (base-10) numbers that correspond to 3-bit binary numbers. The first bit controls `zeroCfh`, the second bit controls `auto-hunt`, and the third bit controls `password`.
	For the `auto-hunt` and `password` parameters, a binary value of 1 turns the parameter on, and a binary value of 0 turns it off.
	However, for the `zeroCfh` parameter, a binary value of 0 turns the feature on, and a binary value of 1 turns it off.
	Thus, if you enter “6” (110 in binary), the following displays:
	`==========`
	`zeroCfgFlag = 6`
	`-- zero-configure is enable now`
	`-- had checked auto-hunt`
	`-- check password of PPPoE/PPPoA is correct`
	`no page need to redirect ..`
	`Auto hunt is enable`
	`Debug mode is disable`

`wan zeroCfg status`	Displays current zero configuration information.

21.8.1 wan tr069 Examples

The following example:

- Turns zero configuration on.
- Turns zero configuration debugging on.
- Sets the zero configuration flag to turn zero configuration on, and auto-hunting and user password off.

- Displays the zero configuration status.

```
ras> wan zeroCfg on
ras> wan zeroCfg debug on
ras> wan zeroCfg flag 0
ras> wan zeroCfg status

 ====================================
 zeroCfgFlag = 0
   -- zero-configure is enable now
   -- check auto-hunt not yet
   -- password of PPPoE/PPPoA is fail or not check
 no page need to redirect ..
 Auto hunt is enable
 Debug mode is disable

ras>
```

22

Wireless LAN Commands

Use these commands to configure the ZyXEL Device's wireless LAN settings.

22.1 Command Summary

The following section lists the commands for this feature.

Table 69 General Wireless Commands

COMMAND	DESCRIPTION
`wcfg macfilter <1 ~ 8> action <deny |allow>`	Sets the action of the specified MAC filtering policy.
`wcfg macfilter <1 ~ 8> clear`	Removes the specified MAC filtering policy.
`wcfg macfilter <1 ~ 8> description <entry-id> <description>`	Sets the descriptive name of an entry in the specified MAC filtering policy.
`wcfg macfilter <1 ~ 8> macAddr <entry-id> <mac-address>`	Sets the MAC address of an entry in the specified MAC filtering policy.
`wcfg macfilter <1 ~ 8> name <policy-name>`	Sets the name of the specified MAC filtering policy.
`wcfg macfilter <1 ~ 8> save`	Saves the specified MAC filtering policy.
`wcfg macfilter <1 ~ 8> show`	Displays the specified MAC filtering policy settings.
`wcfg macfilter display [1 ~ 8]`	Displays the staus of all MAC filtering policies or the specified MAC filtering policy.
`wcfg macfilter saveall`	Saves all MAC filtering policies.
`wcfg macfilter spdisplay [1 ~ 8]`	Displays settings of all MAC filtering policies or the specified MAC filtering policy before saving.
`wcfg radius <1 ~ 8> backupacct <IP> <port-number> <shared-secret> <enable|disable>`	Sets the backup RADIUS accounting server settings.
`wcfg radius <1 ~ 8> backupauth <IP> <port-number> <shared-secret> <enable|disable>`	Sets the backup RADIUS authentication server settings.
`wcfg radius <1 ~ 8> clear`	Deletes the specified RADIUS policy.
`wcfg radius <1 ~ 8> name <profile-name>`	Sets the descriptive name of the specified RADIUS policy.
`wcfg radius <1 ~ 8> primaryacct <IP> <port-number> <shared-secret> <enable|disable>`	Sets the primary RADIUS accounting server settings.

Table 69 General Wireless Commands (continued)

COMMAND	DESCRIPTION
`wcfg radius <1 ~ 8> primaryauth <IP> <port-number> <shared-secret> <enable|disable>`	Sets the primary RADIUS authentication server settings.
`wcfg radius <1 ~ 8> save`	Saves the specified RADIUS policy.
`wcfg radius <1 ~ 8> show`	Displays the specified RADIUS policy settings.
`wcfg radius display [1 ~ 8]`	Displays the staus of all RADIUS policies or the specified RADIUS policy.
`wcfg radius saveall`	Saves all RADIUS policies.
`wcfg radius spdisplay [1 ~ 8]`	Displays settings of all RADIUS policies or the specified RADIUS policy before saving.
`wcfg security <1 ~ 8> clear`	Removes the specified security profile.
`wcfg security <1 ~ 8> groupkeytime <10 ~ 65535>`	Sets the rate at which the AP or RADIUS server sends a new group key out to all clients
`wcfg security <1 ~ 8> idletime <10 ~ 65535>`	Sets the time interval before the ZyXEL Device automatically disconnects a wireless client from the wired network after a period of inactivity.
`wcfg security <1 ~ 8> mode <security-mode>`	Sets the security mode of the specified security profile. *security-mode*: `none | wep | wpa | wpapsk | wpa2 | wpa2mix | wpa2psk | wpa2pskmix`
`wcfg security <1 ~ 8> name <policy-name>`	Sets the name of the specified security profile.
`wcfg security <1 ~ 8> passphrase <passphrase>`	Sets the passphrase for the `wpapsk`, `wpa2psk`, and `wpa2pskmix` security modes. *passphrase*: Types a pre-shared key from 8 to 63 case-sensitive ASCII characters.
`wcfg security <1 ~ 8> reauthtime <10 ~ 65535>`	Sets how often wireless stations have to re-send usernames and passwords in order to stay connected.
`wcfg security <1 ~ 8> save`	Saves the specified security profile.
`wcfg security <1 ~ 8> show`	Displays the specified security profile settings.
`wcfg security <1 ~ 8> wep auth <shared|auto>`	Sets the WEP authentication method for this security profile.
`wcfg security <1 ~ 8> wep <key1 ~ key4> <key-string>`	Sets the WEP key used to encrypt data for this security profile. *key-string*: Enters any 5, 13 or 16 characters (ASCII string) or 10, 26 or 32 hexadecimal characters ("0-9", "A-F") for a 64-bit, 128-bit or 152-bit WEP key respectively.
`wcfg security <1 ~ 8> wep keyindex <1 ~ 4>`	Sets a default WEP key to use for data encryption.
`wcfg security <1 ~ 8> wep keysize <64|128|152> <ascii|hex>`	Sets the size and type of the WEP key(s) in this security profile.
`wcfg security display [1 ~ 8]`	Displays the staus of all security profiles or the specified security profile.
`wcfg security saveall`	Saves all security profiles.

Table 69 General Wireless Commands (continued)

COMMAND	DESCRIPTION
`wcfg security spdisplay [1 ~ 8]`	Displays settings of all security profiles or the specified security profile before saving.
`wcfg ssid <1 ~ 8> clear`	Deletes the specified SSID profile.
`wcfg ssid <1 ~ 8> hidenssid <enable |disable>`	Enables or disables hiding the SSID in the outgoing beacon frame.
`wcfg ssid <1 ~ 8> intrabss <enable |disable>`	Enables or disables traffic between wireless clients in the same BSS using the specified SSID profile.
`wcfg ssid <1 ~ 8> l2isolation <enable|disable> <l2isolation-policy-name>`	Enables or disables an L2 isolation policy in the specified SSID profile.
`wcfg ssid <1 ~ 8> name <profile-name>`	Sets the name of the specified SSID profile.
`wcfg ssid <1 ~ 8> qos <qos-mode>`	Sets the QoS mode of the specified SSID profile. *qos-mode*: 0 : WLANQOS_MODE_NONE 1 : WLANQOS_MODE_WMM 2 : WLANQOS_MODE_WMM_VO 3 : WLANQOS_MODE_WMM_VI 4 : WLANQOS_MODE_WMM_BE 5 : WLANQOS_MODE_WMM_BK
`wcfg ssid <1 ~ 8> radius <radius-profile-name>`	Applies a RADIUS policy to the specified SSID profile.
`wcfg ssid <1 ~ 8> save`	Saves the specified SSID profile.
`wcfg ssid <1 ~ 8> security <security-policy-name>`	Applies a security policy to the specified SSID profile.
`wcfg ssid <1 ~ 8> show`	Displays the specified SSID profile settings.
`wcfg ssid <1 ~ 8> ssid <ssid-value>`	Sets the SSID of the specified SSID profile. *ssid-value*: Enters a descriptive name of up to 32 printable 7-bit ASCII characters.
`wcfg ssid display [1 ~ 8]`	Displays the staus of all SSID profiles or the specified SSID profile.
`wcfg ssid saveall`	Saves all SSID profiles.
`wcfg ssid spdisplay [1 ~ 8]`	Displays settings of all SSID profiles or the specified SSID profile before saving.
`wlan active <1:on|0:off>`	Activates or deactivates the wireless LAN.
`wlan association`	Displays the wireless client association list.
`wlan chid <channel-id>`	Sets the operating frequency/channel. The channels available depend on your particular region. *channel-id*: 1~11.
`wlan clear`	Resets all wireless settings to their defaults.

Table 69 General Wireless Commands (continued)

COMMAND	DESCRIPTION
`wlan dbg <level>`	Sets the WLAN debug settings. For example, enter `0` to turn debugging off. Enter `1` to turn `DEBUG INIT` on. Enter 2 to turn `DEBUG Tx` on. Enter 4 to turn `DEBUG Rx` on. *level*: RA_DEBUG_OFF[0] RA_DEBUG_INIT[1] RA_DEBUG_TX[2] RA_DEBUG_RX[4] RA_DEBUG_TX_DATA[8] RA_DEBUG_RX_DATA[10] RA_DEBUG_ERR[20] RA_DEBUG_CMD[40] RA_DEBUG_TASK[80] RA_DEBUG_INFO[100] RA_DEBUG_IOCTL[200] RA_DEBUG_WSC[400] RA_DEBUG_ALL[fff]
`wlan display`	Displays the WLAN configuration currently in the working buffer.
`wlan essid <essid>`	Sets the wireless AP's SSID.
`wlan filter <incoming|outgoing> <tcpip|generic> <profile>`	Specifies the filter action, type and profile to be used by the WLAN. `incoming`: the filter applies to traffic coming from the WAN to the LAN. `outgoing`: the filter applies to traffic coming from the LAN to the WAN. `tcpip`: the filter checks IP addresses. `generic`: the filter checks MAC addresses. *profile*: filter profile number 1~4. Use the `sys filter set` commands to configure filter profiles.
`wlan fraThreshold <256~2346>`	Sets the fragmentation threshold. If the packet size is over this value, it is fragmented.
`wlan getaplist`	Scans for and displays information of other APs within transmission range.
`wlan getchannel`	Chooses a channel with least interference.
`wlan getcounter`	Displays wirelsss statistics.
`wlan hideessid <on|off>`	Sets whether the SSID is hidden (not broadcast). on: SSID is hidden. `off`: SSID is not hidden.
`wlan ht bw <0|1>`	Sets the channel width used by the ZyXEL Device. 0: Channel Width = 20 MHz 1: Channel Width = 20/40 MHz
`wlan ht gi <0|1>`	Sets the IEEE 802.11n HT (high throughput) guard interval. 0: 800 ns long guard interval 1: 400 ns short guard interval

Table 69 General Wireless Commands (continued)

COMMAND	DESCRIPTION
`wlan ieee8021x authendatabase <0|1|2>`	Sets the order in which the authentication databases are consulted: 0: Local database only. 1: RADIUS only. 2: Local then RADIUS. 3: RADIUS then local.
`wlan ieee8021x display`	Displays wireless security information.
`wlan ieee8021x dynamickeyex <0|1|2>`	Sets the type of dynamic WEP key: 0: WEP disabled. 1: 64-bit WEP. 2: 128-bit WEP.
`wlan ieee8021x idletime <seconds>`	Sets the wireless security idle timeout period.
`wlan ieee8021x KMprotocol <0|1|2|3|4>`	Sets the wireless security key management protocol. 0: IEEE 802.1x. 1: WPA. 2: WPA-PSK. 3: WPA2. 4: WPA2-PSK.
`wlan ieee8021x load`	Loads wireless security information into the working buffer for configuration.
`wlan ieee8021x portcontrol <0|1|2>`	Sets the wireless port control configuration: 0: Authentication required. 1: No access. 2: No authentication.
`wlan ieee8021x PSK <psk>`	Sets the WPA(2)-PSK pre-shared key. *psk*: 8~63 English keyboard characters, no spaces.
`wlan ieee8021x reauthentime <seconds>`	Sets the re-authentication time interval.
`wlan ieee8021x save`	Saves the 802.1x wireless security information to the permanent memory.
`wlan ieee8021x wpabkuptimer <seconds>`	Sets the broadcast / multicast WPA key update timer.
`wlan ieee8021x wpamixmode <0:disable|1:enable>`	Enable or disable WPA mixed mode (WPA mixed mode allows both WPA and WPA2 clients to use the same network).
`wlan igmpsnoop active <0:Disable|1:Enable>`	Enables or disables IGMP snooping on the WLAN.
`wlan load`	Reloads the WLAN configuration from the permanent memory into the working buffer. When you do this, all unsaved changes are lost.
`wlan macfilter <enable|disable>`	Turns the MAC address filter on or off.
`wlan macfilter action <allow|deny>`	Sets the MAC filter to allow or deny devices in the list to associate with the ZyXEL Device.
`wlan macfilter set <1~12> <mac-address>`	Enters the specified MAC address into the MAC filter list in the specified slot.
`wlan mbss <1~4> active <1:on|0:off>`	Enables the specified SSID profile.

Table 69 General Wireless Commands (continued)

COMMAND	DESCRIPTION
`wlan mbss <1~4> ssid <ssid>`	Sets the SSID for the specified SSID profile. *ssid*: 1 ~ 32 characters.
`wlan mbss <1~4> hidessid <1:on|0:off>`	Enables or disables SSID hiding in the specified SSID profile.
`wlan mbss <1~4> noforward <1:on|0:off>`	Disables or enables intra-BSS traffic forwarding in the specified SSID profile.
`wlan mbss <1~4> security mode <OPEN | SHARED | WEPAUTO | WPAPSK | WPA | WPA2PSK | WPA2 | WPA1WPA2 | WPAPSKWPA2PSK>`	Sets the security mode for the specified SSID profile.
`wlan mbss <1~4> security rekeyinterv <minutes>`	Sets the rate at which the ZyXEL Device or the RADIUS server sends a new group key to all clients.
`wlan mbss <1~4> security psk <psk>`	Sets the pre-shared key for WPA-PSK or WPA2-PSK in the specified SSID profile. *psk*: 8~63 ASCII or 64 HEX characters.
`wlan mbss <1~4> security wep keytype <0: Hexadecimal|1: Ascii>`	Sets the type of the WEP keys for the specified SSID profile.
`wlan mbss <1~4> security wep key1 <key>`	Sets the first WEP key in the specified SSID profile.
`wlan mbss <1~4> security wep key2 <key>`	Sets the second WEP key in the specified SSID profile.
`wlan mbss <1~4> security wep key3 <key>`	Sets the third WEP key in the specified SSID profile.
`wlan mbss <1~4> security wep key4 <key>`	Sets the forth WEP key in the specified SSID profile.
`wlan mbss <1~4> security wep defkeyid <1~4>`	Activates one of the four WEP keys to encrypt wireless data transmission.
`wlan mbss <1~4> aclist rule <0|1|2>`	Sets the filtering action or disables MAC address filtering. 0: Disbles MAC filtering for the specified SSID profile. 1: Allows access to the ZyXEL Device. 2: Blocks access to the ZyXEL Device.
`wlan mbss <1~4> aclist add <index> <mac>`	Configures a MAC filtering rule for the specified SSID profile.
`wlan mbss <1~4> aclist remove <mac>`	Removes a MAC filtering rule from the specified SSID profile.
`wlan mbss <1~4> aclist show`	Displays all MAC filtering rules in the specified SSID profile.
`wlan mbss <1~4> clear`	Returns the specified SSID profile to the factory defaults.
`wlan mbss <1~4> save`	Saves the specified SSID profile settings.
`wlan mbss <1~4> show`	Displays the specified SSID profile settings.
`wlan mbss display`	Shows all SSID profiles settings.
`wlan mbss saveall`	Saves all SSID profiles.

Table 69 General Wireless Commands (continued)

COMMAND	DESCRIPTION
`wlan mssid guest_autoOff <1 <minutes>|0>`	This command enables or disables an automatic timeout feature of the guest wireless network. If you enable this feature the guest wireless network is turned off after the specified amount of time. Type `1` to enable the automatic timeout feature, and enter the number of *`minutes`* that the guest wireless network stays active. Enter a number from 0 to 30000. Entering 0 resets the value to the default (60 minutes). Type `0` to disable the automatic timeout feature.
`wlan mssid guestssid <ssid>`	Use this command to specify the SSID of the guest wireless network. This is the SSID guests have to configure on their wireless clients to connect to your wireless network. Type a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
`wlan mssid mode <0:guestssid off 1:guestssid on> <0:intranet blocking off 1:intranet blocking on>`	This command performs two functions and is followed by two parameters. The first parameter specifies whether you want to enable or disable your guest wireless network. Type `0` to disable the guest wireless network or type `1` to enable the guest wireless network. The second parameter specifies whether you want to block guests in the guest wireless network from accessing resources on your LAN. Type `0` to allow guests to access resources on your LAN or type `1` to block guests from accessing resources on your LAN and allow access to the Internet via the ZyXEL Device only.
`wlan mssid setprivacy defaultkeyID <1|2|3|4>`	This command specifies which WEP key guests have to configure on their wireless clients to access the guest wireless network.
`wlan mssid setprivacy type <0|1|2|3>`	This command specifies the security mode for the guest wireless network. Type one of the following: `0` to disable security on the guest wireless network, `1` to enable 64-bit WEP key encryption, `2` to enable 128-bit WEP key encryption, `3` to enable 256-bit WEP key encryption.
`wlan mssid setprivacy wepkey <1|2|3|4> <key>`	This command allows you to create up to four WEP keys. Enter `1`, `2`, `3` or `4` to specify which WEP key you are creating followed by any 5, 13 or 29 characters (ASCII string) or 10, 26 or 58 hexadecimal characters ("0-9", "A-F") for a 64-bit, 128-bit or 256-bit WEP key respectively.
`wlan mssid show`	Displays major and guest SSID settings.

Table 69 General Wireless Commands (continued)

COMMAND	DESCRIPTION
`wlan opmode <0: AP, 1: AP+Bridge, 2: Bridge Only,>`	Sets the ZyXEL Device's operation mode. This selects the operation mode for your device. 0: selects AP mode. 1: selects AP + Bridge mode. This setting enables WDS settings. 2: selects Bridge mode. This setting enables WDS settings.
`wlan qos active <0:off|1:on>`	Turns wireless LAN QoS (Quality of Service) on or off.

`wlan qos debugLevel <level>`	Use this command to configure the debug settings. Debug messages are displayed via the console port.
	This command allows you to configure three parameters:
	• `debug Error`: records information about wireless LAN QoS errors.
	• `debug Tx`: records information about wireless data transmission.
	• `debug Rx`: records information about wireless data reception.
	Enter `0` to turn debugging off.
	Enter `1` to turn `debug Error` on.
	Enter `2` to turn `debug Tx` on.
	Enter `4` to turn `debug Rx` on.
	This is a binary data field with three bits, so you can also control the three parameters by entering decimal (base-10) numbers that correspond to 3-bit binary numbers. The first bit controls `debug Error`, the second bit controls `debug Tx`, and the third bit controls `debug Rx`. A binary value of 1 turns a parameter on, and a binary value of 0 turns it off.
	Thus, if you enter 6 (110 in binary), the following displays:
	`debug Error ( 1) off`
	`debug Tx ( 2) on`
	`debug Rx ( 4) on`

`wlan qos setdefwmmac <0:AP|1:STA>`	Sets the ZyXEL Device's default WMM (Wireless MultiMedia) QoS behavior depending upon its function in the wireless LAN. Chose AP if the ZyXEL Device is used as an access point. Choose STA if the ZyXEL Device is used as a wireless client (station).

Table 69 General Wireless Commands (continued)

COMMAND	DESCRIPTION
`wlan qos setwmmac <0:AP|1:STA> <0:VO|1:VI|2:BE|3:BK> <aifs> <cwmin> <cwmax> <txop-g> <txop-b> <ack-policy>`	Sets the ZyXEL Device's current WMM settings for the specified access category, as follows. VO: Voice VI: Video BE: Best effort BK: Background *aifs* is the arbitration inter-frame space number (1~1023). This controls the additional waiting period prior to sending a packet of the previously-specified type. The waiting period itself is known as the arbitration inter-frame space or AIFS (as distinct from the arbitration inter-frame space number *aifs*). In this command, the *aifs* parameter allows you to specify the AIFS as follows: AIFS = *aifs* * slot-time. Standard slot times are as follows: IEEE 802.11a: 9 µs IEEE 802.11b: 20 µs IEEE 802.11g: 9 µs IEEE 802.11b/g: 20 µs so an *aifs* of 100 in an IEEE802.11g network results in an AIFS of 900µs. When the AIFS time has elapsed, the ZyXEL Device waits for a further time period, known as the contention window (CW), for collision avoidance purposes. *cwmin* is the minimum contention window value, and *cwmax* is the maximum contention window value. The cwmin and cwmax values are 2^n-1 in the range 1~1024, so allowed values are 1, 3, 7, 15, 31, 63, 511 and 1023. The *cwmin* value must be smaller than or equal to the *cwmax* value. The *cwmin* and *cwmax* values are multiples of the slot time, so a *cwmin* value of 15 in an IEEE 802.11g network would result in a minimum contention window of 135µs. The CW length is defined by a random number between the *cwmin* and *cwmax* values. The CW length increases with every retry, until it reaches *cwmax*. *txop-g* is the transmission opportunity limit for packets sent over an IEEE802.11g network, and *txop-b* is the transmission opportunity limit for packets sent over an IEEE802.11b network. The transmission opportunity limit is the largest permitted single wireless transmission; when data is too big, it is split up into separate wireless transmissions. Use *ack-policy* to set whether received transmissions are acknowledged. Enter 0 to send acknowledgements, or enter 1 to send no acknowledgements. Acknowledgements increase reliability, but also increase the quantity of traffic.
`wlan qos showwmmac`	Displays the ZyXEL Device's current WMM access category settings.

Table 69 General Wireless Commands (continued)

COMMAND	DESCRIPTION
`wlan qos wmmdelAppRule <index>`	Deletes an application priority rule, where <*index*> is the rule number.
`wlan qos wmmqosPolicy <0:default|1:AP>`	Use this command to set the current WMM QoS policy. Choose `AP` to use Application Priority or chose `default` to use the ToS value in a packet's headers to control its priority.
`wlan qos wmmsetAppRule <index> <app_name> <app_type> <port> <priority>`	Configures an application priority rule. *index* is the rule number. *app_name* is the name of the rule. *app_type* is the type of application, where: 0 is user-defined 1 is e-mail 2 is FTP 3 is WWW. *port* is the port number. If the <*app_type*> is e-mail, FTP or WWW, a port number is automatically assigned; leave this value at 0. *priority* is the application's priority, where: 0: highest 1: high 2: medium 3: low
`wlan qos wmmshowAppRule`	Displays all application priority rules.
`wlan radio <1: B only, 2: G Only, 3: B+G>`	Sets the type of radio signal used to transmit data.
`wlan radius account active <1:yes|0:no>`	Enables or disables external accounting via a RADIUS accounting server.
`wlan radius account port <port>`	Sets the listening port of the RADIUS accounting server. The default port number is 1812.
`wlan radius account serverIP <ip-address>`	Sets the ip address of the RADIUS accounting server.
`wlan radius account sharedsecret <password>`	Specifies a password to be shared between the ZyXEL Device and the RADIUS server. *password*: Up to 31 alphanumeric characters.
`wlan radius authen active <1:yes|0:no>`	Enables or disables external authentication via a RADIUS server.
`wlan radius authen port <port>`	Sets the listening port of the RADIUS server. The default port number is 1812.
`wlan radius authen serverIP <ip-address>`	Sets the IP address of the RADIUS server.
`wlan radius authen sharedsecret <password>`	Specifies a password to be shared between the ZyXEL Device and the RADIUS server. *password*: Up to 31 alphanumeric characters.
`wlan radius display`	Displays the RADIUS settings.
`wlan radius load`	Loads the RADIUS setting for configuration.
`wlan radius save`	Saves the RADIUS settings.
`wlan removeSTA <mac-address>`	Disconnects the connected wireless station with the specified MAC address.

Table 69 General Wireless Commands (continued)

COMMAND	DESCRIPTION
`wlan resetcount <1>`	Removes wirelsss statistics.
`wlan restart`	Resets the wireless driver on the ZyXEL Device.
`wlan rtsThreshold <256~2346>`	Sets the RTS threshold value. When IEEE802.11g is enabled, the threshold is always 4096. When IEEE802.11g is not enabled, the threshold can be 0~2432.
`wlan save`	Saves all wireless settings to the permanent memory.
`wlan scan`	Scans for a channel which is not used by another device.
`wlan setautochan <0|1>`	Disables or enables auto channel selection. 0: Disable 1: Enable
`wlan setbeaconperiod <20~1024>`	Sets a time interval in milisecond to specify how often the ZyXEL Device broadcasts the SSID.
`wlan setchannel <1~14>`	Sets the wireless channel depending on your region.
`wlan setdisasssta <mac>`	Disconnects a specified wireless client.
`wlan setfragthr <256~2346>`	Sets the maximum data fragment size that can be sent.
`wlan setled <0|1>`	Turns on or off the WLAN LED. 0: OFF 1: ON
`wlan setnoforbssid <0|1>`	Allows or disallows traffic forwarding between different BSSs. 0: Disable 1: Enable
`wlan setradio <0|1>`	Disables or enables the radio. 0: Off 1: On
`wlan setrtsthr <1~2347>`	Sets the RTS threshold.
`wlan setsitesurvey <1>`	Issues a site survey command to the WLAN driver.
`wlan settxburst <0|1>`	Disables or enables transmission burst. 0: Disable 1: Enable
`wlan settxpower <1 ~ 100>`	Sets the output power of the ZyXEL Device.
`wlan settxpream <0|1|2>`	Sets the preamble type. 0: Long Preamble 1: Short Preamble 2: Auto

Table 69 General Wireless Commands (continued)

COMMAND	DESCRIPTION
`wlan setwmode <0~9>`	Sets wireless mode. 0: 802.11 B/G mixed 1: 802.11 B only 2: 802.11 A only 4: 802.11 G only 6: 802.11 N only 7: 802.11 G/N mixed 8: 802.11 A/N mixed 9: 802.11 B/G/N mixed
`wlan threshold fragment <threshold>`	Sets the fragmentation threshold value.
`wlan threshold rts <threshold>`	Sets the RTS/CTS threshold value. When G+ is enabled, the threshold is always 4096. When G+ is not enabled, the threshold can be 0~2432.
`wlan version`	Displays the PCI (Peripheral Component Interconnect), HAL (Hardware Abstraction Layer) and IEEE 802.11 version used by the device. PCI (Peripheral Component Interconnect) refers to the PCI bus connecting the wireless card. HAL (Hardware Abstraction Layer) refers to the software that allows higher level languages to interact with hardware such as a computer motherboard. IEEE 802.11 (or Wi-Fi) refers to a set of wireless LAN technology standards.
`wlan wds`	Displays WDS (Wireless Distribution System) settings and connection status if WDS is enabled.
`wlan wds mode <0|1|2|3|4>`	Sets the WDS operating mode. 0: Disable to turn off WDS on the ZyXEL Device. 1: Restrict mode to enable WDS on the ZyXEL Device. 2: Bridge mode to enable WDS but the ZyXEL Device acts as a bridge. 3: Repeater mode to enable WDS but the ZyXEL Device acts as a repeater. 4: Lazy mode to enable auto learning from the WDS packets that contain the Addr4 field.
`wlan wds secmode <1|2|4|8>`	Sets the WDS security mode. 1: OPEN 2: WEP 4: TKIP 8: AES
`wlan wds add <1~4> <0:off|1:on> <mac> [key1] [key2] [key3] [key4] [defaultkeyid] [psk]`	Adds a WDS link and sets whether the link is active or not. If the WDS security mode is `OPEN`, you do not need to set the key(s). If the WDS security mode is `WEP`, you need to specify four WEP keys and the default key. If the WDS security mode is `TKIP` or `AES`, you need to configure a pre-shared key.

Table 69 General Wireless Commands (continued)

COMMAND	DESCRIPTION
`wlan wds defaultkeyid <1~4>`	Sets a default WEP key to use for data encryption in WDS.
`wlan wds show`	Displays the current WDS settings.
`wlan wds remove <mac>`	Deletes a specified WDS link.
`wlan wep key default <1|2|3|4>`	Activates one of the four WEP keys to encrypt wireless data transmission.
`wlan wep key set <1|2|3|4> <key>`	Sets the specified WEP key. The number of characters you enter as the <key> depends on the WEP keysize you selected. If you use a 64-bit key, enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you use a 128-bit WEP key, enter 13 ASCII characters or 26 hexadecimal characters. If you use a 152-bit WEP key, enter 16 ASCII characters or 32 hexadecimal characters.
`wlan wep type <none|64|128|256>`	Sets the length of the WEP security key.
`wlan wps setopmode <0~4>`	Sets the WPS operating mode. 0: Disable to activate WPS. 1: Enrollee to have the ZyXEL Device work as a WPS enrollee. 2: Proxy to have the ZyXEL Device work as a WPS proxy. 4: Registrar to have the ZyXEL Device work as a WPS registrar.
`wlan wps setstatus <1|2>`	Sets the ZyXEL Device to be configured or unconfigured. 1: AP is un-configured 2: AP is configured
`wlan wps setconfmethod <1|2>`	Sets the method used to configure WPS. 1: use PIN code (Personal Identification Number) 2: use PBC (Push Button Communication)
`wlan wps setenrolleepin <pin>`	Sets the PIN of the device that you are setting up a WPS connection with.
`wlan wps start <0|1>`	Starts or stops adding a wireless device to your wireless network using WPS. 0: Disable 1: Enable
`wlan wps setdevname <name>`	Sets your device name in WPS.
`wlan wps setmanuname <name>`	Sets the WPS manufacturer name.
`wlan wps setmodelname <name>`	Sets the WPS model name.
`wlan wps setserial <number>`	Sets the WPS serial number.
`wlan wps setvendorpin <pin>`	Enters up to eight digits to set a user-defined WPS PIN code in the enrollee device.
`wlan wps showStatus`	Displays WPS configurations.
`wlan wps genPIN <Yes:1|No:0>`	Sets the ZyXEL Device to create a new PIN.

Table 69 General Wireless Commands (continued)

COMMAND	DESCRIPTION
`wlan wps release <Yes:1|No:0>`	Enables or disables removing of all configured wireless and wireless security settings for WPS connections.
`wlan wmm active <Yes:1|No:0>`	Enables or disables the WMM feature on the ZyXEL Device.

22.2 Command Examples

This section shows how to use the wireless LAN commands in some example scenarios.

22.2.1 WLAN Setup Example

The example varies depending on the commands you can use on your ZyXEL Device.

The following example:

- Activates the WLAN.
- Sets the wireless channel to 6.
- Sets the SSID to “ZyWiFi”.
- Sets the MAC address filter to deny association to devices on its list.
- Adds the MAC address “fa:fa:fa:fa:fa:fa” to the MAC address filter list slot 1.
- Activates the MAC filter.
- Sets the WEP type to 128-bit.
- Configures the WEP key 1 to be “1234567890123”.
- Sets the ZyXEL Device to use WEP key 1.
- Turns on QoS.
- Sets the QoS to AP mode.
- Configures the Voice QoS settings with an *`aifs`* of 9µs, a *`cwmin`* of 7 and a *`cwmax`* of 15, a *`txop-b`* of 250 and a *`txop-g`* of 250.
- Saves the configuration.
- Displays the configuration.

```
ras> wlan active 1
wlan active 1
TFTP Client Start
ras> wlan chid 6
ras> wlan essid ZyWiFi
ras> wlan macfilter action deny
ras> wlan macfilter set 1 fa:fa:fa:fa:fa:fa
ras> wlan macfilter enable
ras> wlan wep type 128
ras> wlan wep key set 1 1234567890123
ras> wlan wep key default 1
ras> wlan qos active 1
ras> wlan qos setdefwmmac 0
ras> wlan qos setwmmac 0 0 9 7 15 250 250 1
TFTP Client Start
Running time AP WMMAC value:
AC_VO: aifs= 9, cwmin=  7, cwmax=  15, txop G=250, txop B=250, ack policy= 1
AC_VI: aifs= 0, cwmin=  0, cwmax=   0, txop G=  0, txop B=  0, ack policy= 0
AC_BE: aifs= 0, cwmin=  0, cwmax=   0, txop G=  0, txop B=  0, ack policy= 0
AC_BK: aifs= 0, cwmin=  0, cwmax=   0, txop G=  0, txop B=  0, ack policy= 0
Running time STA WMMAC value:
AC_VO: aifs= 0, cwmin=  0, cwmax=   0, txop G=  0, txop B=  0, ack policy= 0
AC_VI: aifs= 0, cwmin=  0, cwmax=   0, txop G=  0, txop B=  0, ack policy= 0
AC_BE: aifs= 0, cwmin=  0, cwmax=   0, txop G=  0, txop B=  0, ack policy= 0
AC_BK: aifs= 0, cwmin=  0, cwmax=   0, txop G=  0, txop B=  0, ack policy= 0
ras> wlan save
TFTP Client Start
wlan: save ok
ras> wlan display
essid                   = ZyWiFi
chid                    = 6
hide essid              = No
RTS  threshold          = 4096
Frag threshold          = 4096
WEP key type            = 128 bit
WEP default key                 = 1
MAC filter active               = 1
MAC filter action               = Deny
index    MAC address     index    MAC address
-------------------------------------------------
1    FA:FA:FA:FA:FA:FA   17   00:00:00:00:00:00
2    00:00:00:00:00:00   18   00:00:00:00:00:00
3    00:00:00:00:00:00   19   00:00:00:00:00:00
4    00:00:00:00:00:00   20   00:00:00:00:00:00
5    00:00:00:00:00:00   21   00:00:00:00:00:00
6    00:00:00:00:00:00   22   00:00:00:00:00:00
7    00:00:00:00:00:00   23   00:00:00:00:00:00
8    00:00:00:00:00:00   24   00:00:00:00:00:00
9    00:00:00:00:00:00   25   00:00:00:00:00:00
10   00:00:00:00:00:00   26   00:00:00:00:00:00
11   00:00:00:00:00:00   27   00:00:00:00:00:00
12   00:00:00:00:00:00   28   00:00:00:00:00:00
13   00:00:00:00:00:00   29   00:00:00:00:00:00
14   00:00:00:00:00:00   30   00:00:00:00:00:00
15   00:00:00:00:00:00   31   00:00:00:00:00:00
16   00:00:00:00:00:00   32   00:00:00:00:00:00
```

The following example:

- Activates the WLAN.
- Sets the wireless channel to 6.
- Sets the SSID to “ZyWiFi”.
- Sets the MAC address filter to deny association to devices on its list.
- Adds the MAC address “fa:fa:fa:fa:fa:fa” to the MAC address filter list slot 1.
- Sets the WEP key type to ASCII.
- Configures the WEP key 1 to be “1234567890123”.
- Sets the ZyXEL Device to use WEP key 1.
- Turns on QoS.

```
ras> wlan active 1
ras> wlan setchannel 6
ras> wlan mbss 1 ssid ZyWiFi
ras> wlan mbss 1 aclist rule 2
ras> wlan mbss 1 aclist add 1 fa:fa:fa:fa:fa:fa
ras> wlan mbss 1 security wep keytype 1
ras> wlan mbss 1 security wep key1 1234567890123
ras> wlan mbss 1 security wep defkeyid 1
ras> wlan mbss 1 save
ras> wlan wmm active 1
```

22.2.2 RADIUS Example

This example enables RADIUS for configuration and specifies the IP address (**172.16.1.201**), port number (**1844**) and the shared secret (**asdfkjas123**) for communication between the ZyXEL Device and the RADIUS server.

```
ras> wlan radius load
ras> wlan radius authen active 1
ras> wlan radius authen serverIP 172.16.1.201
ras> wlan radius authen port 1844
ras> wlan radius authen sharedsecret asdfkjas123
```

This example displays the RADIUS authentication server settings configured on the ZyXEL Device.

```
ras> radius auth
authentication server:   non-active
                IP   :   172.16.1.201
                Port :   1844
                Key  :   asdfkjas123
```

PART III
Appendices and Index of Commands

A

Legal Information

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CLASS 1 LASER PRODUCT

APPAREIL A LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating

condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

B

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional offices are listed below (see also http://www.zyxel.com/web/contact_us.php). Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

"+" is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

China - ZyXEL Communications (Beijing) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales Email: sales@zyxel.cn
- Telephone: +86-010-82800646
- Fax: +86-010-82800587
- Address: 902, Unit B, Horizon Building, No.6, Zhichun Str, Haidian District, Beijing
- Web: http://www.zyxel.cn

China - ZyXEL Communications (Shanghai) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales Email: sales@zyxel.cn
- Telephone: +86-021-61199055
- Fax: +86-021-52069033

- Address: 1005F, ShengGao International Tower, No.137 XianXia Rd, Shanghai
- Web: http://www.zyxel.cn

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Taiwan

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-2-27399889
- Fax: +886-2-27353220
- Web: http://www.zyxel.com.tw
- Address: Room B, 21F., No.333, Sec. 2, Dunhua S. Rd., Da-an District, Taipei

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Turkey

- Support E-mail: cso@zyxel.com.tr
- Telephone: +90 212 222 55 22
- Fax: +90-212-220-2526
- Web: http:www.zyxel.com.tr
- Address: Kaptanpasa Mahallesi Piyalepasa Bulvari Ortadogu Plaza N:14/13 K:6 Okmeydani/Sisli Istanbul/Turkey

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 0845 122 0301 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

Index of Commands

Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.