



Firmware Release Note

P-334WHD

Release 3.60(AMA.0)C0

Date:	Sept. 4, 2006
Author:	Watties Lin

ZyXEL P-334WHD Standard Version release 3.60(AMA.0)C0 Release Note

Date: Sept. 4, 2006

Supported Platforms:

ZyXEL P-334WHD

Versions:

ZyNOS Version: V3.60(AMA.0) | 09/04/2006 09:59:00

Bootbase Version: V1.06 | 07/06/2006 10:55:00

Notes:

1. MSN Video ALG only support with MSN 7.0 above and the default port (1863) should not be changed.
2. Bit Torrent ALG support following tools: BitComet 0.58, BitSpirit v3.1.0, BitLord 1.1, G3 Torrent v0.9999, Aeureus 2.3.0.4, BitTornado T-0.3.12

Known Issues:

1. Allow NetBIOS traffic between WAN & LAN works on limited situations.
2. Even though trigger port rule is removed, these rule still work until time out.
3. WPA-PSK with short RTS/fragment will lead to disassociation
4. STA can't associate with device anymore after failed authentication with WPA\WPA2(TTLS-CHAP)
5. STA with odyssey client using wrong password and CA can still pass the WPA2 authentication once STA passed the WPA2 authentication before.
6. Complex reconfiguration by SPT-GEN may fail in some cases.
7. VoIP(SIP) failed on enable Bandwidth MGMT.
8. Bandwidth can't access subnet mask as 255.255.255.255
9. Exception may occur if user modify gamelist file and update it to device.
10. Upstream in Bandwidth Management won't take effect immediately until system restart.
11. NTP time update doesn't support domain-name type server address in AP mode if device IP address is static assigned.
12. Device that operating in AP mode may not be accessed via LAN if it was put in a WLAN-complex environment about 30 minutes. For this you can reboot the device to work around.

CI Command List:

Features:

Modification in 3.60(AMA.0)C0 | 09/04/2006

Transfer to FCS version firmware.

Modification in 3.60(AMA.0)b4 | 08/25/2006

1. [BUG FIXED]
Symptom: Modem DNS function can't work.
Condition:
 1. Network/ WAN/ Modem Dialup/ DNS Servers/ First, Second and Third= From ISP (192.168.11.4, 168.95.1.1, 0.0.0.0)
 2. Network/ WAN/ Broadband Connection/ DNS Servers/ First, Second and Third= None
 3. Network/ DHCP server/ Advanced/ DNS Server/ First, Second and Third= None
 4. CLI: ip ping www.hinet.net --> Resolving www.hinet.net... unknown
 5. Due to Modem's DNS will bind to Broadband's DNSSPRID: 060803175
2. [BUG FIXED]
Symptom: SmartBit throughput can't work with LAN to WAN.
Condition:
 1. Firmware version V360AMA0b3
 2. Encapsulation Ethernet
 3. SmartBit setup UDP protocol
 4. Run SmartBit to test throughput
 5. SmartBit monitors display error, and stop
 6. Firmware version V360AMA0b2 is passedSPRID: 060803178
3. [BUG FIXED]
Symptom: Advanced wireless GUI issue:
Condition:
 1. Load to default setting
 2. Go to advanced wireless setup page, disable wireless and save.
 3. Select and enable "Active Wireless LAN" (Do not apply and save setting)
 4. Select the wireless=static WEP (WPA/WPA-PSK/WPA2/WPA2-PSK)
 5. The checkbox "Active Wireless LAN" is disabled.SPRID: 060803232
4. [BUG FIXED]
Symptom: Device exception when test eMule or BT over weekend.
Condition:
 1. Routing mode
 2. WAN encapsulation: Ethernet static IP address
 3. NAT port forwarding 4662~4672 to LAN host

4. Device A runs eMule over weekend, device A continuous crash
 5. Device B runs BT over weekend, device B continuous crash
- SPRID: 060807386

Modification in 3.60(AMA.0)b3 | 07/31/2006

1. [FEATURE ENAHNCED]
Multi-language supported included English, German, French, Spanish, Chinese and Italian.
2. [BUG FIXED]
Symptom: Device selects wrong parameter on PPTP mode
Condition:
 1. Select WAN encapsulation type: PPTP mode
 2. PPTP configuration default setting is Get automatically from ISP, but device is select "Use Fixed IP address".SPRID: 060724581
3. [BUG FIXED]
Symptom: WAN set static PPPoE, LAN host will get device's LAN IP as DNS.
Condition:
 1. WAN set PPPoE mode, DNS from ISP. Device's LAN IP is 192.168.1.1.
 2. In DHCP Server:
First DNS Server set "From ISP" as 192.168.11.4
Second DNS Server set "User Defined" as 2.2.2.2
Third DNS Server set "DNS Relay" as 192.168.1.1
 3. LAN host release/ renew IP and DNS.
 4. LAN host will get only one DNS as 192.168.1.1
 5. In CLI mode, type "ip dhcp enif0 st"
The DNS on DHCP server will show 0.0.0.0 2.2.2.2 0.0.0.0SPR: 060725600
4. [BUG FIXED]
Symptom & Condition:
Function of "Security > Firewall > Services > Disable Services Blocking"
will cause Firewall disabled.
SPRID: 060727787

Modification in 3.60(AMA.0)b2 | 07/21/2006

1. [BUG FIXED]
Symptom: Device crash when disable WLAN via CLI at WiFi WAN mode
Condition:
 1. Change to WiFi WAN mode
 2. Device gets the same subnet IP as 192.168.1.34
 3. CLI to disable WLAN
 4. Device crashSPRID: 060710496
2. [BUG FIXED]
Symptom: Wizard DNS server can't save at dial-up static IP address.

Condition:

1. Router mode
 2. Run wizard page
 3. Dial-up page, use static IP address and then configure DNS server as User-defined 168.95.1.1, 192.168.11.4 and 139.175.55.244, apply
 4. Web/ status/ the Subnet Mask display 0.0.0.0 and the DNS display "From ISP"
- SPRID: 060710505

3. [BUG FIXED]

Symptom: "Clone the computer's MAC address" display error on SMT.

Condition:

1. WiFi WAN mode
2. WAN MAC Address= Clone the computer's MAC address
3. Reboot device.
4. GUI/ status display the correct computer's MAC address 00:08:02:E0:3D:A4
5. SMT display:
 initialize ch =0, ethernet address: 00:13:49:F5:18:A1
 initialize ch =1, ethernet address: 00:00:00:00:00:00
 initialize ch =2, ethernet address: 00:13:49:F5:18:A1

SPRID: 060710498

4. [BUG FIXED]

Symptom: "Spoof MAC address= Set WAN MAC Address" display error on GUI/ Network/ WiFi WAN/ Broadband Connection.

Condition:

1. WiFi WAN mode
2. WAN MAC Address= Set WAN MAC Address 00:08:02:E0:3D:A4
3. GUI/ status display the correct computer's MAC address 00:08:02:E0:3D:A4
4. GUI/ Network/ WiFi WAN/ Broadband Connection display: 00:00:00:00:00:00

SPRID: 060710502

5. [BUG FIXED]

Symptom: Wizard page can't save non-dynamic Ethernet configuration.

Condition:

1. Wizard setup PPTP 、PPPoE and Ethernet can't writing system.
2. When we check network WAN information is error.

SPRID: 060712627

6. [BUG FIXED]

Symptom: WAN use PPTP, enable web proxy in content filter. When browse website device exception.

Condition:

1. WAN use PPTP, enable web proxy in content filter.
2. Client PC using proxy.hinet.net:80 in IE, browse a website device exception.

SPRID: 060712629

7. [BUG FIXED]

Symptom: Device crash with "CLI: aux is aux0"

Condition:

1. GUI/ fill in the correct username, password & Phone Number
2. dial-up successful

3. CLI: aux is aux0
4. Device crash & exception
SPRID: 060713704
8. [BUG FIXED]
Symptom: Modem connection will be dropped after plug and unplug WAN line several times.
Condition:
 1. Modem dial-up successful or WAN interface status up first
 2. Make sure WAN interface & modem interface connection have been built
 3. Unplug WAN line, traffic go through aux0
 4. Plug WAN line, traffic go through enet1
 5. The aux0 connection droppedSPRID: 060713711
9. [BUG FIXED]
Symptom: PPTP modem connection (PPTP modem assign) with PPTP dynamic connection (ISP assign) can't built successfully.
Condition:
 1. Network > WAN > Broadband Connection/ Encapsulation PPTP
 2. PPTP connection built failed
 3. at the same environment & configuration: P-334WH, P-334WHD --> failed; P-335U --> passedSPRID: 060714814
10. [BUG FIXED]
Symptom: Device crash when use PPTP modem to build the connection.
Condition:
 1. Network > WAN > Broadband Connection/ Encapsulation PPTP
 2. PPTP connection built failed
 3. Device continue crash 10 minutes a cycle
 4. Refer to exception logSPRID: 060714815
11. [BUG FIXED]
Symptom: In Router mode, Wireless Fragmentation Threshold issue with WPA-PSK, WPA, WPA2, WPA2-PSK mode.
Condition:

When Frag=500, Config device Wireless security with those mode, the wireless client can't transfer file, can ping only

 - step1. one FTP server at Lan1, (192.168.1.199)
 - step2. one wireless client(Intel 2915 or Other)
 - step3. Config device wireless mode= WPA-PSK, WPA, WPA2, or WPA2-PSK mode and fragmentation=500,
 - step4. from wireless Client, ping to FTP server, and run the ftp to get 10Mb file,SPRID: 060713713
12. [BUG FIXED]
Symptom: Device crash after dial-up retry count failed
Condition:
 1. Modem setup retry count= 5

ZyXEL Confidential

2. after dial-up 5 times
3. Wait for 5 minutes, device crash
4. Refer to attached file

SPRID: 060717930

13. [BUG FIXED]

Symptom: WAN set PPTP, enable Bandwidth, run ftp get file from WAN. Device wills exception.

Condition:

Test Environment is as below:

PC 1-----LAN --- DEVICE --- WAN (PPTP) ---- PQA LAB -----PC 2
(192.168.18.93)

Setup:

PC 1: 192.168.1.33/24 DEVICE LAN: 192.168.1.1

PC 2: 192.168.18.93/24 DEVICE WAN: 192.168.18.1

Enable all application and user-defined service in BM.

Step:

1. PC 1 ping 192.168.18.93 -t
2. PC 1 use cuteftp to get 85mb file from PC2
3. After download about 15%, WAN IP will be drop. Download speed is about 3.4mbps.
4. Then device will get another new WAN IP. And the cuteftp will continue get file.
5. When WAN drop 4 times, device will exception. File download is about 66%.

SPRID: 060714909

14. [BUG FIXED]

Symptom: Debug message displayed when add wrong MAC filter rule in wireless.

Condition:

1. Debug message displayed when add wrong MAC filter rule in wireless.
2. message of “why”

SPRID: 060717003

15. [BUG FIXED]

Symptom: In AP mode, device can't get DNS IP from DHCP server.

Condition:

1. Change device to AP mode.
2. LAN use DHCP to get IP.
3. In CLI, type “ip dns st disp”.
4. DNS always 0.0.0.0

SPRID: 060719174

Modification in 3.60(AMA.0)b1 | 07/06/2006

First Firmware Release.

Appendix A CI Command List

Last Updated: 2006/07/06.

Command Class List Table		
System Related Command	Exit Command	Device Related Command
Ethernet Related Command	POE Related Command	PPTP Related Command
Configuration Related Command	IP Related Command	Modem Dialup Command
Firewall Related Command	Wireless LAN Related Command	Bridge Related Command
Radius Related Command	802.1x Related Command	

System Related Command

[Home](#)

Command				Description
sys				
	atsh			Display system MRD and checksum
	callhist			
		display		display call history
		remove	<index>	remove entry from call history
	countrycode		[countrycode]	set country code
	datetime			
		date		Display system date year/month/day
		time		Display system time hour/minute/second
		period		The period to synchronize with time server
	domainname			display domain name
	edit		<filename>	edit a text file
	extraphnum			maintain extra phone numbers for outcalls
		add	<set 1-3> <1 st phone num> [2 nd phone num]	add extra phone numbers
		display		display extra phone numbers
		node	<num>	set all extend phone number to remote node <num>
		remove	<set 1-3>	remove extra phone numbers
		reset		reset flag and mask
	feature			display feature bit
	hostname		[hostname]	display system hostname
	logs			
		category		
			access [0:none/1:log/2:alert/3:both]	record the access control logs
			attack [0:none/1:log/2:alert/3:both]	record and alert the firewall attack logs
			display	display the category setting
			error [0:none/1:log/2:alert/3:both]	record and alert the system error logs
			ipsec [0:none/1:log/2:alert/3:both]	record the access control logs
			ike [0:none/1:log/2:alert/3:both]	record the access control logs
			javablocked [0:none/1:log]	record the java etc. blocked logs
			mten [0:none/1:log]	record the system maintenance logs
			upnp [0:none/1:log]	record upnp logs
			urlblocked [0:none/1:log/2:alert/3:both]	record and alert the web blocked logs
			urlforward [0:none/1:log]	record web forward logs
		clear		clear log
		display	[access attack error ipsec ike javablocked mten urlblocked urlforward]	display all logs or specify category logs
		errlog		
			clear	display log error
			disp	clear log error

ZyXEL Confidential

		online	turn on/off error log online display
	load		load the log setting buffer
	mail		
		alertAddr [mail address]	send alerts to this mail address
		display	display mail setting
		logAddr [mail address]	send logs to this mail address
		schedule display	display mail schedule
		schedule hour [0-23]	hour time to send the logs
		schedule minute [0-59]	minute time to send the logs
		schedule policy [0:full/1:hourly/2:daily/3:weekly/4:none]	mail schedule policy
		schedule week [0:sun/1:mon/2:tue/3:wed/4:thu/5:fri/6:sat]	weekly time to send the logs
		server [domainName/IP]	mail server to send the logs
		subject [mail subject]	mail subject
	save		save the log setting buffer
	syslog		
		active [0:no/1:yes]	active to enable unix syslog
		display	display syslog setting
		facility [Local ID(1-7)]	log the messages to different files
		server [domainName/IP]	syslog server to send the logs
rn			
	load	<entry no.>	load remote node information
	disp	<entry no.>(0:working buffer)	display remote node information
	nat	<none sua full_feature>	config remote node nat
	nailup	<no yes>	config remote node nailup
	mtu	<value>	set remote node mtu
	save	[entry no.]	save remote node information
	stdio	[minute]	change terminal timeout value
	trcdisp		monitor packets
	trclog		
	trcpacket		
	version		display RAS code and driver version
	view	<filename>	view a text file
	wdog		
	switch	[on/off]	set on/off wdog
	cnt	[value]	display watchdog counts value: 0-34463
	romreset		restore default romfile
	pwderrtm	[minute]	Set or display the password error blocking timeout value.
	upnp		
	active	[0:no/1:yes]	Activate or deactivate the saved upnp settings
	config	[0:deny/1:permit]	Allow users to make configuration changes. through UPnP
	display		display upnp information
	firewall	[0:deny/1:pass]	Allow UPnP to pass through Firewall.
	load		save upnp information
	save		save upnp information
	opmode	[0:Router/1:AP/2:WiFi-WAN Router]	Set and display system operation mode
	socket		display system socket information
	filter		

ZyXEL Confidential

		netbios		
			disp	Display NetBIOS Filter Status
			Config <0:Between LAN and WAN, 3:IPSec pass through, 4:Trigger Dial> <on/off>	Set NetBIOS Filter Status
	roadrunner			
		debug	<level>	enable/disable roadrunner service 0: diable <default> 1: enable
		display	<iface name>	display roadrunner information iface-name: enif0, wanif0
		restart	<iface name>	restart roadrunner
	ddns			
		debug	<level>	enable/disable ddns service
		display	<iface name>	display ddns information
		restart	<iface name>	restart ddns
		logout	<iface name>	logout ddns
	cpu			
		display		display CPU utilization

Exit Command

[Home](#)

Command				Description
exit				exit smt menu

Device Related Command

[Home](#)

Command				Description
dev				
	dial		<node#>	dial to remote node

Ethernet Related Command

[Home](#)

Command				Description
ether				
	config			display LAN configuration information
	driver			
		cnt		
		disp <name>		display ether driver counters
		ioctl	<ch_name>	Useless in this stage.
		status	<ch_name>	see LAN status
	version			see ethernet device type
	spoofmac			
		Macdir	<xx:xx:xx:xx:xx:xx>	Assign MAC for system
		Macbylan	ip<xxx.xxx.xxx.xxx>	Assign LAN PC MAC for system
		display		Display MAC spoof information
	edit			
		load	<ether no.>	load ether data from spt
		mtu	<value>	set ether data mtu
		accessblock	<0:disable 1:enable>	block internet access
		save		save ether data to spt

POE Related Command

[Home](#)

Command				Description
poe				
	status		[ch_name]	see poe status
	dial		<node>	dial a remote node

ZyXEL Confidential

	drop		<node>	drop a pppoe call
	ether		[rfc3com]	set /display pppoe ether type

PPTP Related Command

[Home](#)

Command				Description
pptp				
	dial		<rn-name>	dial a remote node
	drop		<rn-name>	drop a remote node call
	tunnel		<tunnel id>	display pptp tunnel information

Configuration Related Command

[Home](#)

Command					Description
config					The parameters of config are listed below.
edit	firewall	active <yes no>			Activate or deactivate the saved firewall settings
retrieve	firewall				Retrieve current saved firewall settings
save	firewall				Save the current firewall settings
display	firewall				Displays all the firewall settings
		set <set#>			Display current entries of a set configuration; including timeout values, name, default-permit, and number of rules in the set.
		set <set#>	rule <rule#>		Display current entries of a rule in a set.
		attack			Display all the attack alert settings in PNC
		e-mail			Display all the e-mail settings in PNC
		?			Display all the available sub commands
		e-mail	mail-server <mail server IP>		Edit the mail server IP to send the alert
			return-addr <e-mail address>		Edit the mail address for returning an email alert
			e-mail-to <e-mail address>		Edit the mail address to send the alert
			policy <full hourly daily weekly>		Edit email schedule when log is full or per hour, day, week.
			day <sunday monday tuesday wednesday thursday friday saturday>		Edit the day to send the log when the email policy is set to Weekly
			hour <0~23>		Edit the hour to send the log when the email policy is set to daily or weekly
			minute <0~59>		Edit the minute to send to log when the email policy is set to daily or weekly
			Subject <mail subject>		Edit the email subject
		attack	send-alert <yes no>		Activate or deactivate the firewall DoS attacks notification emails
			block <yes no>		Yes: Block the traffic when exceeds the tcp-max-incomplete threshold
					No: Delete the oldest half-open session when exceeds the tcp-max-incomplete threshold
			block-minute <0~255>		Only valid when sets 'Block' to yes. The unit is minute

			minute-high <0~255>		The threshold to start to delete the old half-opened sessions to minute-low
			minute-low <0~255>		The threshold to stop deleting the old half-opened session
			max-incomplete-high <0~255>		The threshold to start to delete the old half-opened sessions to max-incomplete-low
			max-incomplete-low <0~255>		The threshold to stop deleting the half-opened session
			tcp-max-incomplete <0~255>		The threshold to start executing the block field
		set <set#>	name <desired name>		Edit the name for a set
			default-permit <forward block>		Edit whether a packet is dropped or allowed when it does not match the default set
			icmp-timeout <seconds>		Edit the timeout for an idle ICMP session before it is terminated
			udp-idle-timeout <seconds>		Edit the timeout for an idle UDP session before it is terminated
			connection-timeout <seconds>		Edit the wait time for the SYN TCP sessions before it is terminated
			fin-wait-timeout <seconds>		Edit the wait time for FIN in concluding a TCP session before it is terminated
			tcp-idle-timeout <seconds>		Edit the timeout for an idle TCP session before it is terminated
			pnc <yes no>		PNC is allowed when 'yes' is set even there is a rule to block PNC
			log <yes no>		Switch on/off sending the log for matching the default permit
			rule <rule#>	permit <forward block>	Edit whether a packet is dropped or allowed when it matches this rule
				active <yes no>	Edit whether a rule is enabled or not
				protocol <0~255>	Edit the protocol number for a rule. 1=ICMP, 6=TCP, 17=UDP...
				Log <none match not-match both>	Sending a log for a rule when the packet none matches not match both the rule
				alert <yes no>	Activate or deactivate the notification when a DoS attack occurs or there is a violation of any alert settings. In case of such instances, the function will send an email to the SMTP destination address and log an alert.
				srcaddr-single <ip address>	Select and edit a source address of a packet which complies to this rule
				srcaddr-subnet <ip address> <subnet mask>	Select and edit a source address and subnet mask if a packet which complies to this rule.
				srcaddr-range <start ip address> <end ip address>	Select and edit a source address range of a packet which complies to this rule.
				destaddr-single <ip address>	Select and edit a destination address of a packet which complies to this rule
				destaddr-subnet <ip address> <subnet mask>	Select and edit a destination address and subnet mask if a packet which complies to this rule.
				destaddr-range <start ip address> <end ip address>	Select and edit a destination address range of a packet which complies to this rule.
				tcp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive

ZyXEL Confidential

					port numbers, the user may repeat this command line to enter the multiple port numbers.
				tcp destport-range <start port#> <end port#>	Select and edit a destination port range of a packet which comply to this rule.
				udp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, users may repeat this command line to enter the multiple port numbers.
				udp destport-range <start port#> <end port#>	Select and edit a destination port range of a packet which comply to this rule.
				desport-custom <desired custom port name>	Type in the desired custom port name
delete	firewall	e-mail			Remove all email alert settings
		attack			Reset all alert settings to defaults
		set <set#>			Remove a specified set from the firewall configuration
		set <set#>	rule <rule#>		Remove a specified rule in a set from the firewall configuration
insert	firewall	e-mail			Insert email alert settings
		attack			Insert attack alert settings
		set <set#>			Insert a specified rule set to the firewall configuration
		set <set#>	rule <rule#>		Insert a specified rule in a set to the firewall configuration
cli					Display the choices of command list.
debug	<1 0>				Turn on/off trace for firewall debug information.

Wireless LAN Related Command[Home](#)

Command				Description
wlan				
	active		[on/off]	set on/off wlan
	association			display association list
	autoChid		<1: on, 0: off>	Enable/disable auto channel select
	chid		[channel id]	set channel
	chgmode		<1: B only, 2: G Only, 3: B+G>	Set 802.11b/g/mixed mode
	chgoperation		<0:AP, 1:STA>	Set wlan mode
	connection			Any ssid
	cloneMAC		<0:none 1:static 2:dynamic> <MAC addr/IP addr>	Set WiFi-WAN Router mode MAC clone
	disconnect			
	essid		[ess id]	set ESSID
	Hideessid		<on, off>	Set hide/show ESSID
	limituser		<number>	Limit user number in AP mode
	Outputpower		<0: 17 dBm, 1: 14 dBm, 2: 11 dBm>	Set wlan output power
	Preamble		<0: Dynamic, 1: Long>	Set wlan preamble
	removeSTA		<MAC ADDRESS>	Remove wireless Client
	Reset			Reset wireless
	Scan			Auto channel select
	version			display WLAN version information

Bridge Related Command[Home](#)

Command				Description
Bridge				
	cnt			related to bridge routing statistic table

ZyXEL Confidential

		Disp		display bridge route counter
		Clear		clear bridge route counter
	stat			related to bridge packet statistic table
		Disp		display bridge route packet counter
		Clear		clear bridge route packet counter

Radius Related Command

[Home](#)

Command				Description
Radius				
	auth			show current radius authentication server configuration
	acct			show current radius accounting server configuration

802.1x Related Command

[Home](#)

Command				Description
8021x				
	debug	Level	[debug level]	set ieee802.1x debug message level
		Trace		show all supplications in the supplication table
		User	[username]	show the specified user status in the supplicant table

IP Related Command

[Home](#)

Command				Description
ip				
	address		[addr]	display host ip address
	alias		<iface>	alias iface
	aliasdis		<0 1>	disable alias
	arp			
		status	<iface>	display ip arp status
	dhcp		<iface>	
		client		
			Release	release DHCP client IP
			Renew	renew DHCP client IP
		status	[option]	show dhcp status
	dns			
		query		
		server	<primary> [secondary] [third]	set dns server
		stats		
			Clear	clear dns statistics
			Disp	display dns statistics
	httpd			
	icmp			
		status		display icmp statistic counter
		discovery	<iface> [on off]	set icmp router discovery flag
	ifconfig		[iface] [ipaddr] [broadcast <addr> [mtu <value> dynamic]	configure network interface
	ping		<hostid>	ping remote host
	route			
		status	[if]	display routing table
		add	<dest_addr default>[/<bits>] <gateway> [<metric>]	add route
		addiface	<dest_addr default>[/<bits>]	add an entry to the routing table to iface

ZyXEL Confidential

			<gateway> [<metric>]	
		addprivate	<dest_addr default>[/<bits>] <gateway> [<metric>]	add private route
		drop	<host addr> [/<bits>]	drop a route
	status			display ip statistic counters
	udp	status		Display udp status
	tcp	status		Disp tcp status
		telnet	<host>	telnet to <host>
	traceroute		<host> [ttl] [wait] [queries]	send probes to trace route of a remote host
	xparent			
		join	<iface1> [<iface2>]	join iface2 to iface1 group
		break	<iface>	break iface to leave ipxparent group
	urlfilter			
		reginfo		
			Display	display urlfilter registration information
			Name	set urlfilter registration name
			eMail <size>	set urlfilter registration email addr
			country <size>	set urlfilter registration country
			clearAll	clear urlfilter register information
		category		
			Display	display urlfilter category
			webFeature [block/nonblock] [activex/java/cookei/webproxy]	block or unblock webfeature
			logAndBlock [log/logAndBlock]	set log only or log and block
			blockCategory [block/nonblock] [all/type(1-14)]	block or unblock type
			timeOfDay [always/hh:mm] [hh:mm]	set block time
			clearAll	clear all category information
		listUpdate		
			Display	display listupdate status
			actionFlags [yes/no]	set listupdate or not
			scheduleFlag [pending]	set schedule flag
			dayFlag [pending]	set day flag
			time [pending]	set time
			clearAll	clear all listupdate information
		exemptZone		
			Display	display exemptzone information
			actionFlags [type(1-3)][enable/disable]	set action flags
			add [ip1] [ip2]	add exempt range
			delete [ip1] [ip2]	delete exempt range
			clearAll	clear exemptzone information
		customize		
			Display	display customize action flags
			actionFlags[filterList/disableAllExce ptTrusted/unblockRWFTToTrusted/k eywordBlock/fullPath/caseInsensiti ve/fileName][enable/disable]	set action flags
			logFlags [type(1-3)][enable/disable]	set log flags
			add [string] [trust/untrust/keyword]	add url string
			delete [string] [trust/untrust/keyword]	delete url string
			clearAll	clear all information
		logDisplay		display cyber log
		ftplist		update cyber list data

ZyXEL Confidential

		listServerIP	<ipaddr>	set list server ip
		listServerName	<name>	set list server name
	stroute			
		display	[rule # buf]	display rule index or detail message in rule.
		load	<rule #>	load static route rule in buffer
		save		save rule from buffer to spt.
		config		
			name <site name>	set name for static route.
			destination <dest addr>[/<bits>] <gateway> [<metric>]	set static route destination address and gateway.
			mask <IP subnet mask>	set static route subnet mask.
			gateway <IP address>	set static route gateway address.
			metric <metric #>	set static route metric number.
			private <yes/no>	set private mode.
			active <yes/no>	set static route rule enable or disable.
	Ident		<on/off>	Reject IDENT packet switch on/off
	dropIcmp		<0/1>	Device allows/drops ICMP fragment packets
	lite		[0:disable 1:enable lite firewall 2:enable lite and quickpath]	Lite firewall setting
	igmp			
		debug	[level]	set igmp debug level
		forwardall	[on/off]	turn on/off igmp forward to all interfaces flag
		querier	[on/off]	turn on/off igmp stop query flag
		iface		
			<iface> grouptm <timeout>	set igmp group timeout
			<iface> interval <interval>	set igmp query interval
			<iface> join <group>	join a group on iface
			<iface> leave <group>	leave a group on iface
			<iface> query	send query on iface
			<iface> rsptime [time]	set igmp response time
			<iface> start	turn on of igmp on iface
			<iface> stop	turn off of igmp on iface
			<iface> ttl <threshold>	set ttl threshold
			<iface> v1compat [on/off]	turn on/off v1compat on iface
		robustness	<num>	set igmp robustness variable
		status		dump igmp status

Firewall Related Command[Home](#)

Command				Description
sys	Firewall			
		acl		
			Disp	Display specific ACL set # rule #, or all ACLs.
		active	<yes/no>	Active firewall or deactivate firewall
		clear		Clear firewall log
		cnt		
			Disp	Display firewall log type and count.
			Clear	Clear firewall log count.
		disp		Display firewall log
		online		Set firewall log online.
		pktdump		Dump the 64 bytes of dropped packet by firewall
		update		Update firewall
		dynamicrule		
		tcprst		

ZyXEL Confidential

			Rst	Set TCP reset sending on/off.
			rst113	Set TCP reset sending for port 113 on/off.
			Display	Display TCP reset sending setting.
		icmp		
		dos		
			Smtpt	Set SMTP DoS defender on/off
			Display	Display SMTP DoS defender setting.
			Ignore	Set if firewall ignore DoS in lan/wan/dmz/wlan
		ignore		
			Dos	Set if firewall ignore DoS in lan/wan/dmz/wlan
			Triangle	Set if firewall ignore triangle route in lan/wan/dmz/wlan

Modem Dialup Related Command

[Home](#)

Command				Description
aux				
	atring		<device name>	Display modem buffer
	cnt			
		Disp	<device name>	Display counter information
		clear	<device name>	Clear counter information
	drop		<device name>	Drop connect
	init		<device name>	Init modem
	node			
		Index		Set remote node index
		Display		Display remote node information
		Save		Save remote node information
		Active		Active remote node
		Rnname		Set remote node name
		Username		Set user name
		Password		Set password
		phone		Set phone number
	rate		<device name>	Display modem tx/rx rate