ZyXEL

Firmware Release Note

P-334WH

Release 3.60(JZ.0)C0

Date: **August 04, 2006**
Author: **Brian Chang**

ZyXEL P-334WH Standard Version release 3.60(JZ.0)C0 Release Note

Date: August 04, 2006

Supported Platforms:

ZyXEL P-334WH

Versions:

ZyNOS Version: V3.60(JZ.0) | 08/04/2006 18:39:10
Bootbase Version:V1.05 | 04/20/2004 10:36:26

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 DUT 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 occurred if user modify gamelist file and update it to device
10. Modifying total upstream bandwidth of Bandwidth Management doesn't take effect immediately unless device is restarted. When this value is changed, please restart device manually.
11. NTP time update doesn't support domain-name type server address in AP mode if DUT IP address is static assigned
12. DUT 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 DUT to work around.

CI Command List:

Features:

Modification in 3.60(JZ.0)C0 | 08/04/2006

1. Change 3.60(JZ.0)b6 to 3.60(JZ.0)C0 FCS version.

Modification in 3.60(JZ.0)b6 | 07/30/2006

1. [BUG FIXED]
   SPR: 060724582
   Symptom: DUT select wrong parameter on PPTP mode
   Condition:
   1. Select WAN encapsulation type :PPTP mode
   2. PPTP configuration default setting is Get automatically from ISP, but DUT is select ” Use Fixed IP addres”

2. [BUG FIXED]
   SPR: 060725599
   Symptom: WAN set static PPPoE, LAN host will get DUT’s LAN IP as DNS.
   Condition:
   1. WAN set PPPoE mode, DNS from ISP. DUT’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 0.0.0.0

3. [BUG FIXED]
   SPR: 060614800
   Symptom: Device exception when use PPTP encapsulation doing overnight stress testing and it can br reproduced.
   Condition: Device exception when use PPTP encapsulation doing overnight stress testing and it can br reproduced.

Modification in 3.60(JZ.0)b5 | 07/21/2006

1. [BUG FIXED]
   SPR: 060614800
   Symptom: Device exception when use PPTP encapsulation doing overnight stress testing and it can br reproduced.
   Condition: Device exception when use PPTP encapsulation doing overnight stress

testing and it can br reproduced.

2. [BUG FIXED]
   SPR: 060710497
   Symptom: DUT crash when disable WLAN via CLI at WiFi WAN mode
   Condition:
   1. change to WiFi WAN mode
   2. DUT get the same subnet IP as 192.168.1.34
   3. CLI to disable WLAN
   4. DUT crash

3. [BUG FIXED]
   SPR: 060710499
   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 DUT
   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

4. [BUG FIXED]
   SPR: 060710503
   Symptom: ”Spoof MAC addres= 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

5. [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. (Hard to deplicate)

6. [BUG FIXED]
   SPR: 060713712
   Symptom:Wireless Fragmentation Threshold issue with WPA-PSK,WPA,WPA2,WPA2-PSK mode.

Condition: When Frag=500, Config DUT 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 DUT 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,

7. [BUG FIXED]
   SPR: 060713714
   Symptom: It without "Intra BSS blocking" function ,doesn't match the ES and PS
   Condition: It without "Intra BSS blocking" function ,doesn't match the ES and PS

8. [BUG FIXED]
   SPR: 060713715
   Symptom: Output power default is 80% not 100%
   Condition: Output power default is 80% not 100%

9. [BUG FIXED]
   SPR: 060714908
   Symptom: WAN set PPTP, enable Bandwidth, run ftp get file ftom WAN. Device will exception.
   Condition:
   Test Environment is as below:

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

   Setup:
   PC 1 : 192.168.1.33/24 GW 192.168.1.1
   PC 2 : 192.168.18.93/24 GW 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 spped 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%.

10. [BUG FIXED]
    SPR: 060717002
    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
why

11. [BUG FIXED]
SPR: 060719173
Symptom: In AP mode, DUT can't get DNS IP from DHCP server.
Condition:
1. Change DUT to AP mode.
2. LAN use DHCP to get IP.
3. In CLI mode, type "ip dns st disp".
4. DNS always 0.0.0.0

Modification in 3.60(JZ.0)b4 | 07/07/2006

1. [BUG FIXED]
SPR: 060627775
Symptom:
WiFi WAN MAC Address will Clone the computer's MAC address.
Condition:
1. Router mode change to WiFi WAN mode
2. After connect to a AP router, and get the WiFi WAN IP address
3. web/ status/ WiFi WAN MAC Address will Clone the computer's MAC address.
4. accroding to V3.60(JZ.0)b2 firmware, the WiFi WAN MAC address should be same as LAN MAC address

2. [BUG FIXED]
SPR: 060627779
Symptom:
Content Filter works failed on WiFi WAN mode.
Condition:
1. Change to WiFi WAN mode
2. Enable URL Keyword Blocking or ActiveX,Java,Cookie and Web Proxy
3. Set Keyword as yam & yahoo
4. Denied Access Message as Block by testing
5. Schedule set Everyday & All Day
6. LAN host access http://www.yam.com & http://tw.yahoo.com successful
7. The result should be blocked

3. [BUG FIXED]
SPR: 060627782
Symptom:
DUT crash when run FTP to transfer files.
Condition:
1. Router mode

2. Encapsulation set to PPTP
3. Enable BM & ATC
4. FTP client transfer files to WAN
5. DUT crash & exception
6. It's easy to reproduce

4. [BUG FIXED]
   SPR: 060627783
   Symptom:
   eMule overnight testing crash on WiFi WAN mode
   Condition:
   1. Change to WiFi WAN mode
   2. get IP from AP router
   3. NAT port forwarding: eMule 4662-4672
   4. LAN host run eMule overnight
   5. DUT crash & exception
   6. It can be reproduced.

5. [BUG FIXED]
   SPR: 060627856
   Symptom:
   eMule BM testing crash on routing mode
   Condition:
   1. Routing mode
   2. Enable Bandwidth Management
   3. Enable eMule/eDonkey Service
   4. Enable LAN Minimum Bandwidth 10 kbps, WAN Minimum Bandwidth 10 kbps, WLAN Minimum Bandwidth 10 kbps, open BM monitor
   5. LAN host use eMule v0.46c tool to download & upload file, the upload speed 14.3 KB/S, download speed 39.9 KB/S
   6. Enable LAN Minimum Bandwidth 10 kbps, WAN Maxmum Bandwidth 50 kbps, WLAN Minimum Bandwidth 10 kbps, open BM monitor
   7. LAN host use eMule v0.46c tool to download & upload file, the upload speed 5.2 KB/S, download speed 38.2 KB/S
   8. run about 30 mins~ 1hour, DUT crash
   9. It can be reproduced.

6. [BUG FIXED]
   SPR: 060627857
   Symptom:
   Enable BM to do SIP MGM, after talking about 3 mins, DUT crash.
   Condition:
   1. Routing mode
   2. Enable Bandwidth Management
   3. Enable VoIP (SIP) Service
   4. Enable LAN Minimum Bandwidth 10 kbps, WAN Minimum Bandwidth 10 kbps,

WLAN Minimum Bandwidth 10 kbps
5. Phone1 register to SIP server via DUT
6. Phone2 register to SIP server via WAN
7. Phone1 call Phone2, pick up
8. wait for 3~5 mins
9. DUT crash
10. It can be reproduced.

7. [BUG FIXED]
   SPR: 060628882
   Symptom:
   Enable BM to do SIP MGM, use TFGen tool to do packet transfer
   Condition:
   1. Routing mode
   2. Enable Bandwidth Management
   3. Enable VoIP (SIP) Service
   4. Enable LAN Minimum Bandwidth 10 kbps, WAN Minimum Bandwidth 10 kbps, WLAN Minimum Bandwidth 10 kbps, open BM monitor
   5. LAN host use TFGen tool to transfer UDP port 5060, packet size 100000
   6. about 2 mins, DUT crash
   7. It can be reproduced.

8. [BUG FIXED]
   SPR: 060627850
   Symptom:
   Content filter URL keyword blocking could not block web site in routing mode amd Restrict Web Features could not work.
   Condition:
   1. Ethernet/Filter/keyword blocking/keyword list : sex , stock , google , it could not block the related web site
   2. Ethernet/Filter/Restrict Web Features/enable ActiveX, Java, Cookie and Web Proxy to block web site features , but it failed

Modification in 3.60(JZ.0)b3 | 06/22/2006

1. [FEATURE ENHANCEMENT]
   GUI supports multi-language

2. [BUG FIXED]
   SPR: 060605264
   Symptom:
   Change remote management Telnet access , device will exception
   Condition:
   Change remote management Telnet access(LAN -> L & W access), device will exception

3. [BUG FIXED]
   SPR: 060605268
   Symptom:
   Fragment threshold value error
   Condition:
   1. encapsulation : PPPoE
   2. WAN/Advance/Netbios over TCP/IP : enable ”allow between LAN & WAN” and ”allow trigger dial” --> apply , it will show ”Fragment threshold value error”

4. [BUG FIXED]
   SPR: 060606346
   Symptom: encapsulation some basic functions error
   Condition:
   1. encapsulation : PPTP
   2. PPTP configuration/static fixed IP: 192.168.11.185 ,IP Subnet Mask :255.255.255.0 , Server IP Address: 192.168.11.4 , Connection ID/Name: S:
   3. WAN IP Address Assignment /Get automatically from ISP (Default)/DNS Servers/First DNS Server: From ISP, Second DNS Server: From ISP
   4. DHCP Server/Advanced/DNS Servers/First DNS Server: From ISP, Second DNS Server: From ISP
   5. use CI command : ip ping www.hinet.net (Resolving unkonwn)
   6. LAN site pc to release & renew ip address to ping www.hinet.net , it could not find out the host www.hinet.net

5. [BUG FIXED]
   SPR: 060605242
   Symptom:
   WiFi WAN’s static 128 WEP(256 WEP) display error
   Condition:
   WiFi WAN’s static 128 WEP(256 WEP) display error:
   1. We select WiFi WAN mode, and select static 128 WEP key(ex: ”1111111111111”) and save it
   2. Then we reload this page
   3. The WEP key is modify to ”11111” by system
   4. But we still can use ”1111111111111” to associate to AP

6. [BUG FIXED]
   SPR: 060605243
   Symptom:
   Wi-Fi WAN(upto channel 11) can associate to AP that support channel upto 13
   Condition:
   Wi-Fi WAN(upto channel 11) can associate to AP that support channel upto 13:
   1. We setup DUT to Wi-Fi WAN mode and config country code=255 (channel 1~11)
   2. We setup AP’s country code=225 (channel 1~13) and operating channel=13
   3. The DUT(Wi-Fi WAN) can associate to AP

7. [BUG FIXED]
   SPR: 060605244
   Symptom:
   Wi-Fi WAN(Auto static WEP) can not associate to AP(Shared WEP):
   Condition:
   Wi-Fi WAN(Auto static WEP) can not associate to AP(Shared WEP):
   1. We config Wi-Fi WAN's DUT: Static 64 WEP key and authentication method = Auto
   2. We config AP: Static 64 WEP key and authentication method = Shared key
   3. DUT can not associate to AP

8. [BUG FIXED]
   SPR: 060605245
   Symptom:
   Wi-Fi WAN can associate to AP by using the differnet static WEP key index:
   Condition:
   Wi-Fi WAN can associate to AP by using the differnet static WEP key index:
   1. We config Wi-Fi WAN's DUT: Static 64 WEP key, authentication method = Auto and four 64 static WEP key(key index=1)
   2. We config AP: Static 64 WEP key, authentication method = auto and four 64 static WEP key(key index=2)
   3. DUT still can associate to AP

9. [BUG FIXED]
   SPR: 060605247
   Symptom:
   Wi-Fi WAN channel display error:
   Condition:
   Wi-Fi WAN channel display error:
   1. AP select channel = 3 and save
   2. After the Wi-Fi WAN DUT associate to AP, the channel disply channel=6 in status page

10. [BUG FIXED]
    SPR: 060605248
    Symptom:
    Wi-Fi WAN can not associate to AP via 256 WEP key
    Condition:
    Wi-Fi WAN can not associate to AP via 256 WEP key
    1. AP config 256 static WEP key
    2. Wi-Fi WAN DUT can not associate to AP via 256 static WEP key

11. [BUG FIXED]
    SPR: 060605250
    Symptom:

Please gray PassPhrase's button "generate" while we use 256 WEP key
Condition:
Please gray PassPhrase's button "generate" while we use 256 WEP key
1. We select 256 WEP key in DUT Router mode(While we select the 256 WEP key, the system will gray passphrase button "generate")
2. We try to reload this page
3. We find that user can click the passphrase button "generate"(Please gray it)

12. [BUG FIXED]
SPR: 060605251
Symptom:
Wi-Fi WAN passphrase 128 WEP key do not work!!
Condition:
Wi-Fi WAN passphrase 128 WEP key do not work!!
1. Wi-Fi WAN DUT can not generate passphrase 128 WEP key.

13. [BUG FIXED]
SPR: 060606279
Symptom: Change sys op mode from Router to Wifi WAN router, Wifi WAN can't get IP from WAN AP.
Condition:
1. Change sys op mode from Router to Wifi WAN Router, Wifi WAN can't get IP from WAN AP.
2. Power off and on the device, Wifi WAN can get IP. Reboot from GUI and CI command is no work.

14. [BUG FIXED]
SPR: 060606280
Symptom: In Wifi WAN router mode, WAN MAC address clone function no used.
Condition:
1. Change to Wifi WAN mode and let Wifi WAN get an IP address.
2. Select Clone the computer's MAC address.
3. Renew Wifi WAN IP, get the same IP and un status page MAC address still show default MAC address. See associate list from WAN AP, the MAC address still default MAC address.
4. Restart device. Wifi WAN can't get IP from WAN AP.

15. [BUG FIXED]
SPR: 060606281
Symptom: In Wifi WAN mode, oprating channel always show Disbled in status page.
Condition:
1.Change to Wifi WAN mode
2. Let Wifi WAN get IP from WAN AP.
3. When connecting, the oprating channel always show Disbled in status page.

16. [BUG FIXED]
    SPR: 060606286
    Symptom: In WiFi WAN mode, BM/ Application List can't save the correct bandwidth & direction.
    Condition:
    1.Change to WiFi WAN mode
    2. Enable BM/ enable one of the application rule
    3. edit the rule, set To LAN max. 800, To WAN max. 400, press ok & apply
    3. edit the rule again, the value has been changed & has irregular rule

17. [BUG FIXED]
    SPR: 060607419
    Sympotom: "SMTP authentication" works failed with some mail servers.
    Condition:
    1. log setting : enable SMTP authentication and email now , mail server cataloged " Error 10054 reset by peer "
    2. disable SMTP authentication , email server got the digest mail
    3. Successful mail server: cis.nctu.edu.tw
    4. failed mail servers: PChome, ZyXEL and ArGoSoft.

18. [BUG FIXED]
    SPR: 060606350
    Symptom: Change schedule setting in content filter page need click other page then back.
    Condition:
    1. Enter schedule page in content filter, change any setting then apply.
    2. Change another setting then apply without click other page then back. The change will not be saved.

19. [BUG FIXED]
    SPR: 060606351
    Symptom: Channel display error in status page in Wifi WAN mode.
    Condition:
    1. In Wifi WAN Mode, when Wifi WAN is connected. The channel always show 6 even the connecting channel is 4.

20. [BUG FIXED]
    SPR: 060607422
    Sympotom: At AP mode, "SMTP authentication" works failed with all mail servers.
    Condition:
    1. log setting : enable SMTP authentication and email now , mail server cataloged " Error 10054 reset by peer "
    2. disable SMTP authentication , email server got the digest mail
    3. failed mail servers: PChome, cis.nctu.edu.tw, ZyXEL and ArGoSoft.

21. [BUG FIXED]

SPR: 060607443
Symptom: LED(MODE, WLAN) that are showed in housing panel can not light correctly!
Condition:
1. load to default, LED "MODE" is light
2. If we change from "Router mode" to "AP mode", then LED ""MODE" and "WLAN" are light

22. [BUG FIXED]
SPR: 060607407
Symptom: In Wifi WAN mode, CLI command with show message when starting.
Condition: In Wifi WAN mode, CLI command with show message when starting. It show like "Can not get dynamic clone MAC….

23. [BUG FIXED]
SPR: 060607455
Symptom: When WAN mode is not Ethernet change sys op mode, the message in message bar will out of range.
Condition:
1. In router mode, set WAN mode as PPTP.
2. Change sys op mode to Wifi WAN mode.
3. Message in the message si out of range.

24. [BUG FIXED]
SPR: 060607456
Symptom: In Wifi WAN mode, change setting in Wifi WAN advanced page. The WIFI WAN connection will disconnect.
Condition:
1. In Wifi WAN mode, change NETBIOS setting in Wifi WAN advanced page. The WIFI WAN connection will disconnect.
2. Change NETBIOS setting in LAN advanced page will not.

25. [BUG FIXED]
SPR: 060612678
Symptom: DUT display "Fragment threshold value error" when access Multicast via WAN & LAN advanced.

26. [BUG FIXED]
SPR: 060612731
Symptom: LAN host DNS address error.
Condition:
1. Web/ Network/ WAN/ Ethernet dynamic IP address, DNS Server = From ISP
2. LAN host do "IP release & renew", PC get the correct DNS address as 192.168.11.4 & 168.95.1.1
3. Web/ Network/ WAN/ Ethernet fixed IP address, DNS Server = From ISP
4. Web/ Network/ DHCP Server/ Advanced/ First DNS Server= 1.1.1.1

5. Reboot DUT
5. LAN host do "IP release & renew", PC get the DNS address as 1.1.1.1, 192.168.11.4 & 168.95.1.1
6. The correct DNS address should be only 1.1.1.1 on LAN host

27. [BUG FIXED]
SPR: 060612718
Symptom: WiFi WAN static 64 WEP key index can not be changed.
Condition:
1. WiFi WAN mode and use static 64 WEP key
2. If we select key index=2, then press button "apply"
3. After we fresh the GUI, then we find that the key index is still in index 1

28. [BUG FIXED]
SPR: 060613775
Symptom: DUT crash when run PPTP wizard.
Condition:
1. Default rom file
2. run wizard and select PPTP dynamic, successful to access Internet
3. Default rom file
4. run wizard and select PPTP static, DUT crash and exception continuous
5. Run on Automation site, occur rate= 100%
6. Run on the other site or PC, occur rate= 50%

29. [BUG FIXED]
SPR: 060612728
Sympton: Change the setting in Content Filter Schedule page will not be saved.
Condition: In Security/ Content Filter/ Schedule, when you change the setting without clicking another page then back, the change will not be saved.
Step 1: Setting schedule as "everyday" then apply.
Step 2: Unchecked the "Fri" item then apply.
Step 3: Click another page then back, the setting still is "everyday".

Modification in 3.60(JZ.0)b2 | 06/01/2006

1. [FEATURE ENHANCEMENT]
WLAN output power control support

Modification in 3.60(JZ.0)b1 | 05/26/2006

First Firmware Release

Annex A CI Command List

Last Updated: 2002/11/26

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	IPSec Related Command
Firewall Related Command	Wireless LAN Related Command	Bridge Related Command
Radius Related Command	802.1x Related Command	Auto WLAN Security Delivery Command

System Related Command Home

Command				Description
sys				
	adjtime			retrive date and time from Internet
	callhist			
		display		display call history
		remove	<index>	remove entry from call history
	countrycode		[countrycode]	set country code
	date		[year month date]	set/display date
	domainname			display domain name
	edit		<filename>	edit a text file
	extraphnum			maintain extra phone numbers for outcalls
		add	<set 1-3> <1st phone num> [2nd 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
			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
	log			
		clear		clear log error
		disp		display log error
		online	[on|off]	turn on/off error log online display
		resolve		Resolve mail server and syslog server address
	mbuf			
		link	link	list system mbuf link
		pool	<id> [type]	list system mbuf pool
		status		display system mbuf status
		disp	<address>	display mbuf status
		cnt		
			disp	display system mbuf count
			clear	clear system mbuf count
		debug	[on|off]	
	pwderrtm		[minute]	Set or display the password error blocking timeout value.
	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
	smt			not support in this product
	stdio		[minute]	change terminal timeout value
	time		[hour [min [sec]]]	display/set system time
	trcdisp			monitor packets
	trclog			
	trcpacket			
	syslog			
		server	[destIP]	set syslog server IP address
		facility	<FacilityNo>	set syslog facility
		type	[type]	set/display syslog type flag

		mode	[on|off]	set syslog mode
	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
	server			
		access	<telnet|ftp|web|icmp|snmp|dns> <value>	set server access type
		load		load server information
		disp		display server information
		port	<telnet|ftp|web|snmp> <port>	set server port
		save		save server information
		secureip	<telnet|ftp|web|icmp|snmp|dns> <ip>	set server secure ip addr
	fwnotify			
		load		load fwnotify entry from spt
		save		save fwnotify entry to spt
		url	<url>	set fwnotify url
		days	<days>	set fwnotify days
		active	<flag>	turn on/off fwnotify flag
		disp		display firmware notify information
		check		check firmware notify event
		debug	<flag>	turn on/off firmware notify debug flag
	cmgr			
		trace		
			disp <ch-name>	show the connection trace of this channel
			clear <ch-name>	clear the connection trace of this channel
		cnt	<ch-name>	show channel connection related counter
	socket			display system socket information
	filter			
		netbios		
	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
	filter			
		netbios		
	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

Exit Command Home

Command				Description
exit				exit smt menu

Device Related Command Home

Command				Description
dev				
	channel			
		drop	<channel_name>	drop channel
	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
	pkttest			
		disp		
			packet <level>	set ether test packet display level
			event <ch> [on|off]	turn on/off ether test event display
		sap	[ch_name]	send sap packet
		arp	<ch_name> <ip-addr>	send arp packet to ip-addr
	debug			
		disp	<ch_name>	display ethernet debug infomation
		level	<ch_name> <level>	set the ethernet debug level level 0: disable debug log level 1:enable debug log (default)
	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
	drop		<node>	drop a pppoe call
	ether		[rfc|3com]	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 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
	chid		[channel id]	set channel
	diagnose			self-diagnostics
	essid		[ess id]	set ESS ID
	version			display WLAN version information

Bridge Related Command Home

Command				Description
Bridge				
	cnt			related to bridge routing statistic table
		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>] <gateway> [<metric>]	add an entry to the routing table to iface
		addprivate	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add private route
		drop	<host addr> [/<bits>]	drop a route
	smtp			
	status			display ip statistic counters
	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.
	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
	ave			anti-virus enforce

	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/disableAllExceptTrusted/unblockRWFToTrusted/keywordBlock/fullPath/caseInsensitive/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
		listServerIP	<ipaddr>	set list server ip
		listServerName	<name>	set list server name
	tredir			
		failcount	<count>	set tredir failcount
		partner	<ipaddr>	set tredir partner
		target	<ipaddr>	set tredir target
		timeout	<timeout>	set tredir timeout
		checktime	<period>	set tredir checktime
		active	<on|off>	set tredir active
		save		save tredir information
		disp		display tredir information

		debug	<value>	set tredir debug value
	nat			
		server		
			disp	display nat server table
			load <set id>	load nat server information from ROM
			save	save nat server information to ROM
			clear <set id>	clear nat server information
			edit active <yes|no>	set nat server edit active flag
			edit svrport <start port> [end port]	set nat server server port
			edit intport <start port> [end port]	set nat server forward port
			edit remotehost <start ip> [end ip]	set nat server remote host ip
			edit leasetime [time]	set nat server lease time
			edit rulename [name]	set nat server rule name
			edit forwardip [ip]	set nat server server ip
			edit protocol [protocol id]	set nat server protocol
			edit clear	clear one rule in the set
		service		
			irc [on|off]	turn on/off irc flag
		resetport		reset all nat server table entries
		incikeport	[on|off]	turn on/off increase ike port flag
	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
	pr			

IPSec Related Command Home

Command				Description
ipsec				
	debug	<1|0>		turn on|off trace for IPsec debug information
	ipsec_log_disp			show IPSec log, same as menu 27.3
	route	lan	<on|off>	After a packet is IPSec processed and will be sent to LAN side, this switch is to control if this packet can be applied IPSec again.
				Remark: Command available since 3.50(WA.3)
		wan	<on|off>	After a packet is IPSec processed and will be sent to WAN side, this switch is to control if this packet can be applied IPSec again.
				Remark: Command available since 3.50(WA.3)
	show_runtime	sa		display runtime phase 1 and phase 2 SA information

		spd		When a dynamic rule accepts a request and a tunnel is established, a runtime SPD is created according to peer local IP address. This command is to show these runtime SPD.
	switch	<on|off>		As long as there exists one active IPSec rule, all packets will run into IPSec process to check SPD. This switch is to control if a packet should do this. If it is turned on, even there exists active IPSec rules, packets will not run IPSec process.
	timer	chk_my_ip	<1~3600>	- Adjust timer to check if WAN IP in menu is changed
				- Interval is in seconds
				- Default is 10 seconds
				- 0 is not a valid value
		chk_conn.	<0~255>	- Adjust auto-timer to check if any IPsec connection has no traffic for certain period. If yes, system will disconnect it.
				- Interval is in minutes
				- Default is 2 minuets
				- 0 means never timeout
		update_peer	<0~255>	- Adjust auto-timer to update IPSec rules which use domain name as the secure gateway IP.
				- Interval is in minutes
				- Default is 30 minutes
				- 0 means never update
				Remark: Command available since 3.50(WA.3)
	updatePeerIp			Force system to update IPSec rules which use domain name as the secure gateway IP right away.
				Remark: Command available since 3.50(WA.3)
	dial	<rule #>		Initiate IPSec rule <#> from ZyWALL box
				Remark: Command available since 3.50(WA.3)
	display	<rule #>		Display IPSec rule #
	remote	key	<string>	I add a secured remote access tunnel with pre-shared key. It is a dynamic rule with local: the route's WAN IP. The algorithms with it are fixed to phase1: DES+MD5, DH1 and SA lifetime 28800 seconds; phase2: DES+MD5, PFS off, no anti-replay and SA lifetime 28800 seconds. The length of pre-shared key is between 8 to 31 ASCII characters.
		switch	<on|off>	Activate or de-activate the secured remote access tunnel.
	keep_alive	<rule #>	<on|off>	Set ipsec keep_alive flag
	load	<rule #>		Load ipsec rule
	save			Save ipsec rules
	config	netbios	active <on|off>	Set netbios active flag
			group <group index1, group index2…>	Set netbios group
		name	<string>	Set rule name
		name	<string>	Set rule name
		keeyAlive	<Yes| No>	Set keep alive or not
		lcIdType	<0:IP | 1:DNS | 2:Email>	Set local ID type
		lcIdContent	<string>	Set local ID content
		myIpAddr	<IP address>	Set my IP address

		peerIdType	<0:IP | 1:DNS | 2:Email>	Set peer ID type
		peerIdContent	<string>	Set peer ID content
		secureGwAddr	<IP address | Domain name>	Set secure gateway address or domain name
		protocol	<1:ICMP | 6:TCP | 17:UDP>	Set protocol
		lcAddrType	<0:single | 1:range | 2:subnet>	Set local address type
		lcAddrStart	<IP>	Set local start address
		lcAddrEndMask	<IP>	Set local end address or mask
		lcPortStart	<port>	Set local start port
		lcPortEnd	<port>	Set local end port
		rmAddrType	<0:single | 1:range | 2:subnet>	Set remote address type
		rmAddrStart	<IP>	Set remote start address
		rmAddrEndMask	<IP>	Set remote end address or mask
		rmPortStart	<port>	Set remote start port
		rmPortEnd	<port>	Set remote end port
		antiReplay	<Yes | No>	Set anitreplay or not
		keyManage	<0:IKE | 1:Manual>	Set key manage
		ike	negotiationMode <0:Main | 1:Aggressive>	Set negotiation mode in phase 1 in IKE
			preShareKey <string>	Set pre shared key in phase 1 in IKE
			p1EncryAlgo <0:DES | 1:3DES>	Set encryption algorithm in phase 1 in IKE
			p1AuthAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in phase 1 in IKE
			p1SaLifeTime <seconds>	Set sa life time in phase 1 in IKE
			p1KeyGroup <0:DH1 | 1:DH2>	Set key group in phase 1 in IKE
			activeProtocol <0:AH | 1:ESP>	Set active protocol in phase 2 in IKE
			p2EncryAlgo <0:Null | 1:DES | 2:3DES>	Set encryption algorithm in phase 2 in IKE
			p2AuthAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in phase 2 in IKE
			p2SaLifeTime <seconds>	Set sa life time in phase 2 in IKE
			encap <0:Tunnel | 1:Transport>	set encapsulation in phase 2 in IKE
			pfs <0:None | 1:DH1 | 2:DH2>	set pfs in phase 2 in IKE
		manual	activeProtocol <0:AH | 1:ESP>	Set active protocol in manual
		manual ah	encap <0:Tunnel | 1:Transport>	Set encapsulation in ah in manual
			spi <decimal>	Set spi in ah in manual
			authAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in ah in manual
			authKey <string>	Set authentication key in ah in manual
		manual esp	encap <0:Tunnel | 1:Transport>	Set encapsulation in esp in manual
			spi <decimal>	Set spi in esp in manual
			encryAlgo <0:Null | 1:DES | 2:3DES>	Set encryption algorithm in esp in manual
			encryKey <string>	Set encryption key in esp in manual
			authAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in esp in manual
			authKey < string>	Set authentication key in esp in manual

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		
			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		
			smtp	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

Annex A CI Command List

Auto WLAN Security Delivery Related Command

Home

Command				Description
autoSec	Start			Start the process of WLAN configuration delivery
	Duration			Set the delivery process duration time in seconds
	Port			Set the communication port
	key			Set the communication encryption key