ZyXEL

Firmware Release Note

P-335/P-335WT

Release 3.60(JO.2)C0

Date: **May 16, 2005**
Author: **Brian Chang**

ZyXEL P-335/P-335WT Standard Version release 3.60(JO.2)C0 Release Note

Date: May 16, 2005

Supported Platforms:

ZyXEL P-335/P-335WT

Versions:

ZyNOS Version: V3.60(JO.2) | 05/16/2005 14:35:03
Bootbase Version: V1.05 | 04/20/2004 10:36:26

Notes:

1. This version supports quick route and enabled by default.
2. If Wireless Port Control (SMT Menu 23.4) is "Authentication Required", P-335WT will enable 802.1x/WPA/WPA-PSK user authentication mechanism, a wireless user must login the P-335WT successfully before accessing network service. If Wireless Port Control is "No Authentication Required", P-335WT will allow all wireless users to access network service. If Wireless Port Control is "No Access Allowed", P-335WT will not allow wireless user to access network service.
3. The Local User Database does not support key generation for 802.1x dynamic web key and WPA pairwise/group key.
4. The first entry of static route is reserved for system and read-only for users.
5. Multi-lingual GUI.
6. Help pages are not complete ready yet.

Known Issues:

1. The device fails to add a firewall ACL rule for NAT server set #12 automatically.
2. Allow NetBIOS traffic between WAN & LAN doesn't work when Firewall is enabled.
3. Computers using Any IP need clear ARP table to access network after P-335/P-335WT reboot.
4. Into SMT 21.1.1.1 TCP/IP Filter rule, save source and destination IP address then back to configure again would show the error message and can not save.
5. Using FTP to upgrade F/W may cause system hang sometimes and need to reboot by manual.
6. Wireless status become down sometimes and system would re-initial wireless automatically.

7. Into SMT 1, DNS server can select Private DNS but eWC cannot select.
8. Currently, TI 4X mode is disabled by default.
9. Using FTP tool upload and download file at same time, BW MGMT monitor LAN/WAN BW limit value not correct.
10. DHCP client not RFC 2131 on rebinding request, according to RFC it should be broadcast where our device is send unicast.
11. Router's priority error in WAN.
12. BWM configure problem use wizard setup

CI Command List:

Features:

Modification in 3.60(JO.2)C0 | 05/16/2005
Convert version string from "3.60(JO.2)b3" to "3.60(JO.2)"

Modification in 3.60(JO.2)b3 | 05/13/2005
1. [BUG FIXED]
   SPR: 050511610
   Symptom:
   WLAN association list on GUI display error.
   Condition:
   WLAN association list on GUI display error.
2. [FEATURE ENHANCED]
   SMTP Authentication

Modification in 3.60(JO.2)b2 | 05/10/2005
1. [BUG FIXED]
   SPR: 050509443
   Symptom: Firmware version error on TMSS dashboard.
   Condition:
   Firmware version error on TMSS dashboard.

Modification in 3.60(JO.2)b1 | 05/04/2005
1. [FEATURE CHANGED]
   Media bandwidth management for SIP still works even though ALG_SIP is disable
2. [FEATURE ENHNACED]
   ALG enable/disable setting can be saved in rom file.
3. [FEATURE CHANGED]
   Name Modified:
   ALG_MSMN -->ALG_MSNM
   ALG_VOIP -->ALG_H323

Modification in 3.60(JO.1)C0 | 02/02/2005
1. [FEATURE CHANGED]

Convert to FCS version.

Modification in 3.60(JO.1)b3 | 01/28/2005

1. [BUG FIXED]
   Symptom: TMSS Redirected page show wrong model version
   Condition:
   Redirected page pops up when the first time client has http traffic via P335WT
   =>My router model version show 3.60(JO.0).

Modification in 3.60(JO.1)b2 | 01/26/2005

1. [BUG FIXED]
   1. Enable Wireless, and Security is "No security", go to OTIST page and click start
   2.OTIST page will show count down, at this time click to other page and back to OTIST page again
   3.Click Start button again, Status will show "Your current security mode is not supported"
2. [BUG FIXED]
   1. Reset default rom file
   2. In OTIST page, Inactive "Yes! Please enhance the Wireless Security Level to WPA-PSK automatically if no any WLAN security has been set. This will generate a random PSK key later for your convenience" and click Start button
   3. Sometimes Status will show "Write to flash fail"
3. [BUG FIXED]
   1. Upload boot base to V1.05, and in debug mode
   2. atcb-->atwm111111-->atbt1-->atsb-->atgo
   3. Check LAN MAC become 11:11:00:11:00:00 .
4. [BUG FIXED]
   1. ADVANCED\TMSS\Trend Micro Security Services
   2. Change "Enable Trend Micro Security Servivces" to "Enable Trend Micro Security Services"

Modification in 3.60(JO.1)b1 | 01/21/2005

1. [BUG FIXED]
   Symptom: Wireless Static Web can't configure
   Condition:
   1. On eWC Wireless page, select Static WEB and Passphrase is empty then click Generate button
   2. Status will show "Please Input Passphrase" and Security select No Security and click Apply, Status will show this message again and can't not save
2. [BUG FIXED]
   Symptom: WPA Group Key Update Timer can't work
   Condition:
   1. On eWC Wireless page, Security select WPA and WPA Group Key Update Timer set 60 sec, then after 60 sec check P335WT not update Group key
3. [BUG FIXED]
   Symptom: OTIST will be OFF even without change wireless configure.

Condition:
1. Process OTIST, then OTIST LED will be ON.
2. Don't change configuration SMT3.5 and save it, OTIST LED is OFF.

Modification in 3.60(JO.0)C0 | 12/23/2004

1. [FEATURE CHANGED]
   Convert to FCS version.

Modification in 3.60(JO.0)b5 | 12/22/2004

1. [BUG FIXED]
   Symptom: Use CI command type "ether edit speed <auto|10/half|10/full|100/half|100/full> Router will crash.
   Condition: Use CI command type "ether edit speed <auto|10/half|10/full|100/half|100/full> Router will crash.

Modification in 3.60(JO.0)b4 | 12/21/2004

1. [BUG FIXED]
   Symptom: WAN port uses 10/half speed will fail.
   Condition: Using 10M/half device connects to WAN port of Router, the connection will fail.

Modification in 3.60(JO.0)b3 | 12/13/2004

1. [BUG FIXED]
   Symptom: the managed traffic will be processed one-by-one instead of concurrently processing if they are configured as the same priority.
   Condition: 1. Create two pairs rule of chariot to verify bandwidth management.
   2. the managed traffic will be processed one-by-one instead of concurrently processing if they are configured as the same priority.
2. [BUG FIXED]
   Symptom: Dhcp cannot work.
   Condition: 1. Enable bandwidth management at LAN & WLAN.
   2. Using G405 or P2000W to get DHCP would fail.
3. [BUG FIXED]
   Symptom: IP alias configure problem
   Condition:
   1.In eWC configure IP alias
   2.Set IP alias 1 IP is 192.168.2.1 and active IP alias 1
   3.Set IP alias 2 IP is same as IP alias2 but not active IP alias 2 =>Fail , status show "IP Alias 1 and IP Alias 2 are in the same network"
4. [BUG FIXED]
   Symptom: Parental Control always disabled by license control.
   Condition:
   1. Enable TMSS and Parental Control.
   2. Active your account on Dashboard of TMSS.
   3. Wait a period, Parental Control still disabled by license control. It should be enabled.

5. [BUG FIXED]
   Symptom: Possible NAT issue in combination with specific SUA entry.
   Condition: While the SUA entry was there (inactive or active) all outbound sessions were PATed to port 10000!!!. And the browsing was slower, some pages didn't load at all. When removing the entry, everything came back to normal and all PATed sessions show different port. "Start port:10000 End port:30000" is the only case that could cause problems.
6. [BUG FIXED]
   Symptom: If M-1 & 1-1 are using the same public IP address, it would cause some problem.
   OLD :

#	Local StartIP	Local End IP	Global Start IP	Global End IP	Type
1	10.10.1.13	N/A	62.2.217.107	N/A	1-1
2	10.10.1.0	10.10.1.255	62. 2.217.106	N/A	M-1
3	10.10.2.0	10.10.2.255	62. 2.217.107	N/A	M-1

   NEW :

#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
1	10.0.1.13	N/A	62.2.217.107	N/A	1-1
2	10.10.1.0	10.10.1.255	62.2.217.106	N/A	M-1
3	10.10.2.0	10. 0.2.255	62.2.217.106	N/A	M-1

   The two M-1 NAT entries made the first 1-1 NAT connections fail
   Before: If there are two rules with iga conflict, previous rule will be removed and new rule still exists in runtime data structuere.
   Now: If there are two rules with iga conflict, all rules will be kept in runtime data structure.
7. [FEATURE ENHANCED]
   Support ADM5120 WAN port speed configure.
8. [BUG FIXED]
   Into italian language, the time configuration of System Menu is changed to "Config. Ora".

Modification in 3.60(JO.0)b2 | 11/22/2004

1. [BUG FIXED]
   Symptom: IP alias configure problem
   Condition:
   1.In eWC or SMT configure IP alias
   2.Set IP alias 1 IP is same as alias 2 =>Fail ,no error message and it still can save to rom
2. [BUG FIXED]
   Symptom: Using webcracker4 software to brute force password cracker a period time , DUT will crash
   Condition: 1.Using webcracker4 software to brute force password cracker a period time , DUT will crash
   2.Use session tool make many 80 port session to LAN =>DUT will be crash
3. [BUG FIXED]

Symptom: Static route for WAN subnet mask has some problem.
Condition: 1). Set WAN Encapsulation to Ethernet/ Dynamic IP.
2). Add static route on WAN, then check the route added to routing table.
3). Reboot system and make sure the WAN get IP again, then check the routing table, the route is not exist.

4. [BUG FIXED]
   Symptom: In SMT Menu 21.1 configure have some problem
   Condition:
   1.In SMT Menu 21.1 ,Edit a TCP/IP filter rule
   2.Set Destination address is 1.1.1.1 Source IP address is 2.2.2.2
   then save to rom
   3.reedit this rule and change source IP address is 5.5.5.5 then save to rom => Filter error : -16, Invalid IP source address
5. [BUG FIXED]
   Symptom: Sometime printer's USB connect to DUT's USB port ,DUT can not detect printer
   Condition: Sometime printer's USB connect to DUT's USB port ,DUT can not detect printer
6. [BUG FIXED]
   Symptom: VPN rule configure problem
   Condition: In eWC Secure Gateway Address can not use domain name
7. [BUG FIXED]
   Symptom: Apply call schedule rule to WAN ,DUT will crash
   Condition:
   1.Set WAN encapsulation is PPPoE
   2. Edit a schedule rule name is 1
   3.Goto SMT Menu 11 , Set schedules=1 then save to rom
   =>DUT will crash while PPPoE is trigger.
8. [BUG FIXED]
   Content filter keyword block problem：
   Enable content filter and add keyword block is "sina "
   Use Google to search "sina"
   Click "sina.com" web site on google's search web page，device can not block www.sina.com page.
9. [BUG FIXED]
   Symptom: VPN SA monitor problem
   Condition:
   1.Establish a VPN tunnel
   2.goto SA monitor disconnect VPN tunnel
   3.rebuilt VPN tunnel and in SA monitor click refresh button
   =>VPN tunnel rule can not display while VPN tunnel established.
10. [BUG FIXED]
    Symptom: SIP pass through by P2002 (P2P) have problem
    Condition:
    Test SIP pass through by P2002(P2P) ,sometime voice can not pass through and remote site can not hand up the call

Phone1—P2002—P335---P335—P2002---Phone2
(P2P).

11. [BUG FIXED]
    Symptom: IHV logo displays not correct on Dashboard
    Condition:
    1. Redirected page pops up when the first time client has http traffic via P335
    2. IHV logo displays not correct on Dashboard(IHV logo display like P335WT).
12. [BUG FIXED]
    Symptom: TMSS Redirected page show wrong model name
    Condition:
    Redirected page pops up when the first time client has http traffic via P335 =>My router model name show P334WT.
13. [BUG FIXED]
    Symptom: Chinese WAN page naming problem
    Condition:
    1.eWC language choice Chinese
    2.Goto 進階->廣域網路 =>inside 廣域網路 naming is 外部網路.
14. [BUG FIXED]
    Symptom: Print server naming problem
    Condition: In eWC goto print server =>it naming printer server , it should naming print server.

Modification in 3.60(JO.0)b1 | 10/27/2004

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

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