ZyXEL

Firmware Release Note

P-662HW-D3

Standard version

Release 3.40(ANC.2)C0

Date:	**Jul 25 ,2006**
Author:	**Lorna Liu**

ZyXEL P-662HW-D3 Standard Version
Release 3.40(ANC.2)C0
Release Note

Date: Jul 25, 2006

Supported Platforms:

ZyXEL P-662HW-D3

Versions:

ZyNOS Version   : V3.40(ANC.2) | 7/25/2006 09:42:05
Bootbase Version   : V1.06 | 1/20/2006 9:44:11

Notes:

The P-662HW-D3, is 4th generation of ZyXEL ADSL product family. It is a high performance ADSL/ADSL2/ADSL2+ router for small/medium office to have Internet access and LAN-to-LAN application over the existing copper line. P-662HW-D3 takes advantage of much higher data rate than ADSL, speed up to 12Mbps (ADSL2) or 26Mbps (ADSL2+), greater reach, faster start-up, advanced diagnostics and better power management. This high performance ADSL router is a high integrated advanced Firewall, Bandwidth Management and IEEE 802.11g wireless features to meet the demand of high-end market.

P-662HW-D3 provides an embedded mini-PCI module for 802.11g Wireless LAN connectivity, four single auto-sensing, auto-detection 10/100BASE-T Ethernet ports for connection to the user's local network, and a single RJ-11/RJ-45 port for connection to ADSL/ADSL2/ADSL2+ line.

ADSL data pump version: TI AR7 06.00.04.00

Features:
Modifications in V 3.40(ANC.2)C0 | 7/25/2006
1. Change to FCS.

Modifications in V 3.40(ANC.2)b2 | 7/13/2006
1. [BUG FIX]   SPRID: 060718101
    Problem Symptom: Wizard setup -＞wireless setup leads to crash.
    Problem Condition: Step1. Restore default romfile.
    Step2. Enter wizard setup-＞wireless setup, and select security as "Manually assign a WEP key" then enter a wrong key like "1234", it will show an error page.
    Step3. Select "Back" and enter a correct key or you change to "Manually assign a

WPA-PSK key" or "Disable wireless security", when you apply the configuration, the device will crash.
2. [BUG FIX]   SPRID: 060718103
Problem Symptom: Bandwidth MGMT rule with bandwidth larger than 65535 can't be added correctly.
Problem Condition: Step1.Bandwidth MGMT-＞Summary LAN interface-＞Speed set to 100000.
Step2. Enter Bandwidth MGMT-＞Rule Setup and add a rule with Bandwidth smaller than 65536, it will be added correctly.
Step3. Enter Bandwidth MGMT-＞Rule Setup and add a rule with Bandwidth larger than 65536, the bandwidth which will be saved is the bandwidth you have entered subtract 65536, for example you have entered 65537, it will be saved as 1.
3. [BUG FIX]   SPRID: 060718105
Problem Symptom: An administrator log in the device for configuration, if another LAN or WAN PC also tries to enter 192.168.1.1, the administrator which have logged in will not be allowed to configure the device until it log in again and it shows "The object on the P662HW-D3 is protected" in the web page.
Problem Condition: An administrator log in the device for configuration, if another LAN or WAN PC also tries to enter 192.168.1.1, the administrator which have logged in will not be allowed to configure the device until it log in again and it shows "The object on the P662HW-D3 is protected" in the web page.
4. [ENHANCEMENT]
 Update copyrighg information to :
 Copyright (c) 1994 - 2006 ZyXEL Communications Corp.
5. [ENHANCEMENT]
 Update the sentence in GUI "Maintenance > Tools > Configuration":
 Change "Prestige" to "router"

Modifications in V 3.40(ANC.2)b1 | 7/13/2006
1. Base on P-662HW-D1 V3.40(AGZ.3)C0 change ADSL data pump to version: TI AR7 06.00.04.00(ANNEXB)

Modifications in V 3.40(ANC.1) | 5/29/2006
1. Change to FCS

Modifications in V 3.40(ANC.1)b1 | 5/29/2006
1. [FEATURE CHANGE]
   Add reset button WLAN Active--Inactive behavior, the reset button new behavior is below:
    For WLAN model: (P-660HW, P2602HW ..etc)
  - 1 sec: enable/disable WLAN function
  - 3 sec: enable OTIST
  -10 sec: reset to factory default

2. [Feature update]

Engineer note:Add CLI command to control wlan restart or not after download NVS files.

3. [Feature update]

   Add wireless card check machine in HTP

      1 when WLAN Card exist, "WLAN LED" will be always on

      2 when WLAN Card does not exist, "WLAN LED" will be always off

      3 when WLAN Card disappear, "WLAN LED" will be off ,HTP test will be Break and "SYSTEM LED" will be always on

Modifications in V 3.40(ANC.0) | 5/22/2006

1. Change to FCS

Modifications in V 3.40(ANC.0) b1 | 5/16/2006

1. Create this project base on P-662HW-D1 V3.40(AGZ.1)b1

Annex A CI Command List

System Related Command   Home

Command				Description
sys				
	adjtime			retrive date and time from Internet
	callhist			
		add		
		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]	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]	record the access control 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
				ike [0:none/1:log/2:alert/3:both]	record the access control logs
				pki [0:none/1:log/2:alert/3:both]	record the pki logs
				cac[0:none/1:log]	record thecac logs
				anyip[0:none/1:log]	record the anyip logs
				antivirus [0:none/1:log/2:alert/3:both]	record the antivirus logs
				8021x[0:none/1:log]	record the 8021x logs
		clear			clear log
		display			display all 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
			sendmail		
		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
	smt				
		on			display smt
		off			hide smt
	stdio		[second]		change terminal timeout value
	datetime				
		period			
	time		[hour [min [sec]]]		display/set system time
	tos				
		display			display all runtime TOS
		listPerHost			display all host session count
		debug	[on|off]		turn on or off TOS debug message
		sessPerHost	<number>		configure session per host value
		dump			

		timeout		
			display	display all TOS timeout information
			icmp <idle timeout>	set idle timeout value
			igmp <idle timeout>	set idle timeout value
			tcpsyn <idle timeout>	set idle timeout value
			tcp <idle timeout>	set idle timeout value
			tcpfin <idle timeout>	set idle timeout value
			udp <idle timeout>	set idle timeout value
			gre <idle timeout>	set idle timeout value
			esp <idle timeout>	set idle timeout value
			ah <idle timeout>	set idle timeout value
			other <idle timeout>	set idle timeout value
	trcdisp			monitor packets
	trclog			
		switch	[on|off]	set system trace log
		online	[on|off]	set on/off trace log online
		level	[level]	set trace level of trace log #:1-10
		type	<bitmap>	set trace type of trace log
		disp		display trace log
		clear		clear trace
		call		display call event
		encapmask	[mask]	set/display tracelog encapsulation mask
	trcpacket			
		create	<entry> <size>	create packet trace buffer
		destroy		packet trace related commands
		channel	<name> [none|incoming|outgoing|bothway]	<channel name>=enet0,sdsl00, fr0 set packet trace direction for a given channel
		string		enable smt trace log
		switch	[on|off]	turn on/off the packet trace
		disp		display packet trace
		udp		send packet trace to other system
			switch [on|off]	set tracepacket upd switch
			addr <addr>	send trace packet to remote udp address
			port <port>	set tracepacket udp port
		parse	[[start_idx], end_idx]	parse packet content
		brief		display packet content briefly
	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
	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
	socket			display system socket information
	filter			

		clear		clear filter statistic counter
		disp		display filter statistic counters
		sw	[on|off]	set filter status switch
		set	<set>	display filter rule
		netbios		
			disp	display netbios filter status
			config <0:LAN to WAN, 1:WAN to LAN, 2:LAN to DMZ, 3:IPSec passthrough, 4:Trigger Dial> <on|off>	config netbios filter
	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
	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
		reserve	[0:no/1:yes]	Reserve UPnP NAT rules in flash after system bootup.
		save		save upnp information
	packetscan			
		display		
		active		
		type	[email|http|ftp] [yes|no]	
		autoupdate		
			display	
			set [0:none|1:1hr|2:12hr|3:24hr]	
			query	
		monitor		
			session	
			ftptable	
			create[number of session]	
		debug	[0:Off|1:Pkt Scan 2:Online update level 1|3:Online update level 2|4:Virus delect]	
		backscan		
		save		
		version		
		overflowaction	[forward | block]	
		expire		
		lk		
		register	[yes | no]	

	atsh			
	atmu			display multi boot version
	xmodemmode		[crc|checksum]	
	diag			
	routeip		<on|off>	
	bridge		<on|off>	
	save			
	display			
	password			
	default			Restore default Romfile.
	winmes			
		send	[Host IP][Messages string][Retry]	
		debug	[0|1|2]	
	snmp			
		display		
		get	<community>	
		set	<community>	
		trusthost	<IP Address>	
		trap		
			community	
			destination	
		discard		
		save		
		clear		

Exit Command

Command			Description
exit			exit smt menu

Ethernet Related Command

Command				Description
ether				
	config			display LAN configuration information
	driver			
		cnt		
			disp <name>	display ether driver counters
			clear <name>	clear ether driver counters
		iface	<ch_name> <num>	send driver iface
		mac	<ch_name> <mac_addr>	Set LAN Mac address
		reg	<ch_name>	display LAN hardware related registers
		rxmod	<ch_name> <mode>	set LAN receive mode. mode: 1: turn off receiving 2: receive only packets of this interface 3: mode 2+ broadcast 5: mode 2 + multicast 6: all packets
		status	<ch_name>	see LAN status
		init	<ch_name>	initialize LAN
		config	[0|1=auto|normal] [0|1=10|100] [0|1=HD|FD] <ch-name>	

Command				Description
				see ethernet device type

WAN Related Command
<u>Home</u>

Command				Description
wan				
	adsl			
		chandata		ADSL channel data, line rate
		close		Close ADSL line
		linedata		
			near	Show ADSL near end noise margin
			far	Show ADSL far end noise margin
		open		Open ADSL line
		opencmd		Open ADSL line with specific standard
			Glite	
			T1.413	
			Gdmt	
			multimode	
			adsl2	
			adsl2+	
			adsl2_delt	
			adsl2+_delt	
			readsl2	
			readsl2_delt	
		opmode		Show the operational mode
		rateadap	[on|off]	Turn on/off rate adaptive mechanism
		perfdata		Show performance information,CRC,FEC, error seconds..
		reset		Reset ADSL modem, and must reload the modem code again
		Status		ADSL status (ex: up, down or wait for init)
		errorsecond		
			shutdown	
		targetnoise	[value]	Adjust target noise offset
		driver		
		vchunt		
			Add <remoteNodeIndex> <vpi> <vci> <service bit(hex)>	Add a entry to hunting pool <remote node> : input the remote node index 1-8 <vpi> : vpi value <vci> : vci value <service>: it's a hex value, bit0:PPPoE/VC (1), bit1:PPPoE/LLC (2) , bit2:PPPoA/VC (4), bit3:PPPoA/LLC (8), bit4:Enet/VC (16), bit5 :Enet/LLC (32) For examples: If you need service PPPoE/LLC and Enet/LLC then the service bits will be 2+32 = 34 (decimal) = 22 (hex), you must input 22 Need to perform save after this command
			Remove <removeNodeId> <vpi> <vci>	Input remote node ID and vpi, vci value to remove the specific entry. System will save automatically.
			Active <yes|no>	Enable VC auto hunting featurer
			display	Display the hunt pool

				Clear	Clear the configure buffer
				Save	Save current setting into ROM file
				timer	The waiting time before checking the hunting table result
				Send	Send VC hunt pattern again
				result	Check the result of VC auto hunting
				debug	
				again	
				webredir<enable:0 | disable:1>	
	node				
			index [1-8]		Set the node pointer to specific wan profile. If you want to set WAN profile, please use this command first, system will use the index number for pointing to specific PVC (remote node), and for consequent commands reference, if index = 1 means it's ISP node
		clear			Clear the parameters of the temporary WAN profile
		ispname	[ISP name]		Enable the name of wan node
		enable			Enable the wan profile
		disable			Disable the wan profile
		encap	[1483|pppoa|pppoe|enet]		Set the wan protocol
		mux	[vc|llc]		Set the wan multiplex
		ppp			
			authen [chap|pap|both]		Set PPP authentication type
			username [name]		Set PPP username
			password [password]		Set PPP password
		service	[name]		Set PPPoE service name
		bridge	[on|off]		Set the wan bridge mode
		routeip	[on|off]		Set the wan IP routing mode
		callsch	[set1#][set2#][set3#][set4#]		Set call schedule set, set number 0 means empty
		nailedup	[on|off]		Set nailed up connection on/off
		vpi	[num]		Set the wan vpi. Range : 0~255
		vci	[num]		Set the wan vci. Range : 32~65535
		qos	[ubr|cbr]		Set the wan QOS type to be UBR or CBR
		pcr	[num]		Set the wan PCR value
		scr	[num]		Set the wan SCR value
		mbs	[num]		Set the wan MBS value
		wanip	[static|dynamic] [address]		Set the wan IP address
		remoteip	[address] [subnet mask]		Set the remote gateway IP address and subnet mask
		nat	[off | sua | full] [address mapping #]		Set type wan NAT mode to be off or SUA or Full feature
		rip	[none|in|out|both] [rip1|rip2b|rip2m]		Set the wan RIP mode and RIP version
		multicast	[none|igmpv1|igmpv2]		Set the wan IP multicast mode
		filter	[incoming|outgoing] [tcpip|generic] [set #1] [set #2] [set #3] [set #4]		Set WAN filter, incoming or outgoing can be specified, and filter set can be 1-12, value 0 means empty
		save			Save the related parameters of WAN node
		display			Display WAN profile configuration in buffer
	hwsar	disp			Display hwsar packets incoming/outgoing information
		clear			Clear hwsar packets information
		sendoam	<vpi> <vci> <f5>		

			<end-to-end> <type:0(AIS) 1(RDI) 2(LoopBack) 3(Continuity Check)>	
		driver		
			config	
			register	
			oammode<mode:0(firmware mode) 1(disable firmware mode)>	
			dischan<channel>	
			tearoam <vpi> <vci> <f5> <end-to-end> <type:0(AIS) 1(Continuity Check)>	
			test<vpi> <vci> <count> <mode:0(send packet) 1(internal loopback)>	
		debug	[on|off]	
	zeroCfg			
		status		
		on		
		off		
		flag	<disable (1:zeroCfh / 2:auto-hunt / 4:password / 7:all)>	
		debug	1:enable / 0:disable	

WLAN Related Command
<u>Home</u>

Command				Description
Wlan				
	active	[on|off]	[0|1]	Turn on/off wireless lan
	association			Show association list
	removeSTA		MAC_Addr(00a0c5123456)	
	load			Load WLAN configuration into buffer.
	Display			Display WLAN configuration data.
	chid		n(channel id)	Configure channel ID 1-13
	essid			Configure ESSID
	hideessid		[on/off]	Enable/Disable hidden SSID
	threshold			
		rts	<RTS threshold value>	Set threshold rts value
		Fragment	<Fragment threshold value>	Set threshold fragmentation value
	wep			
		type	<none|64|128|256>	Set WEP key to 64, 128 or 256 bits.
		Key		
			Set <set> <value>	Set WEP key value per set
			Default <set>	Set WEP default key set
	macfilter			
		Enable		Enable macfilter
		Disable		Disable macfilter

		Action	<allow|deny>	When action match, allow or deny this mac
		Set	<Set#> <MAC Address>	Set mac address by set
	Clear			Clear all WLAN configuration data.
	Save			Save WLAN configuration working buffer to Rom file.
	filter			
		[incoming | outgoing]	<generic>[set#1][set#2][set#3][set#4]	To set generic filter for wireless channel

IP Related Command

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		
			address <ipaddr> [timeout]	resolve ip-addr to name
			debug <num>	enable dns debug value
			name <hostname> [timeout]	resolve name to ip-addr
			status	display dns query status
			table	display dns query table
		stats		
			clear	clear dns statistics
			disp	display dns statistics
	httpd			
		debug	[on|off]	set http debug 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
	status			display ip statistic counters
	udp			

		status		display udp status
	telnet		<host> [port]	execute telnet clinet command
	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
	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
		proxy		
	des			
		test		
		reset		
	urlfilter			
		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
			reset	clear all information
		general		
			enable	enable|disable url filter function
			display	display content filer's general setting
			exemptZone display	display exemptzone information
			exemptZone	set action flags

			actionFlags [type(1-3)][enable|disable]	
			exemptZone add [ip1] [ip2]	add exempt range
			exemptZone delete [ip1] [ip2]	delete exempt range
			exemptZone reset	clear exemptzone information
			reset	reset content filter's general setting
			webFeature	[block/nonblock] [activex/java/cookie/webproxy]
			timeOfDay	[always/hh:mm] [hh:mm]
			blockingText	[text]
		webControl		
			enable	enable cbr_filter
			display	display cbr_filter's setting
			logAndBlock [log|block|both]	set log or block on matched web site
			category	set blocked categories
			serverList display	display current cbr_filter servers
			serverList refresh	refresh cbr_filter servers
			queryURL [url][Server|localCache]	query url need to block or forward according the database on server or local cache
			cache display	display the local cache entries
			cache delete [entrynum|All]	delete the local cache entries
			cache timeout [hour]	Set timeout value of cache entries
			blockonerror [log|block][on|off]	choose log or block when server is unavailable
			unratedwebsite[block|log][on|off]	hoose log or block for unrated web site
			waitingTime [sec]	set waiting time for server
			list	

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

IPSec Related Command
Home

Command				Description
ipsec				
	debug	<1|0>		turn on|off trace for IPsec debug information
	route	dmz	<on|off>	After a packet is IPSec processed and will be sent to DMZ side, this switch is to control if this packet can be applied IPSec again.
				Remark: Only supported in ZyWALL100

		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 "only outbound traffic but no inbound 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
		chk_input	<0~255>	- Adjust input timer to check if any IPSec connection has no inbound traffic for a certain period. If yes, system will disconnect it.
				- Interval is in minutes
				- Default is 2 minuets
				- 0 means never timeout
				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 #
		switch	<on|off>	Activate or de-activate the secured remote access tunnel.
	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
		active	<Yes | No>	Set active or not
		keeyAlive	<Yes| No>	Set keep alive or not
		natTraversal	<Yes| No>	Enable NAT traversal 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
		dnsServer	<IP>	Set DNS server for IPSec VPN
		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
		authMethod <0:PreSharedKey | 1:RSASignature		Set authentication method in phase 1 in IKE
		preShareKey <string>		Set pre shared key in phase 1 in IKE
		certFile <FILE>		Set certificate file if using RSA signature as authentication method.
		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 |		set encapsulation in phase 2 in IKE

			1:Transport>	
			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
	swSkipOverl apIp		<on|off>	- When a VPN rule with remote range overlaps with local range, the switch decides if a local to local packet should apply this rule. - Default value is "off" which means "no skip".
	adjTcpMss		<off|auto|user defined value>	- After a tunnel is established, system will automatically adjust TCP MSS. - After all tunnels are drops, the MSS will adjust to the original value. - The default value is auto.
	des			-
		test		-
		reset		-
	igmp			
	pr			-

Radius Related Command
    Home

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

8021x 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

Bandwidth management Related Command   <u>Home</u>

Command						Description
bm						
	interface	lan	enable	<bandwidth xxx>		Enable bandwidth management in LAN with bandwidth xxx bps. If the user doesn't set the bandwidth, the default value is 100Mbps.
				<wrr|prr>		Select fairness-based(WRR) or priority-based(PRR) mechanism. the default value is fairness-based.
				<efficient>		Enable work-conserving feature.
			disable			Disable bandwidth management in LAN
		wan	enable	<bandwidth xxx>		Enable bandwidth management in WAN with bandwidth xxx bps. If the user doesn't set the bandwidth, the default value is 100Mbps.
				<wrr|prr>		Select fairness-based(WRR) or priority-based(PRR) mechanism. the default value is fairness-based.
				<efficient>		Enable work-conserving feature.
			disable			Disable bandwidth management in WAN
		dmz	enable	<bandwidth xxx>		Enable bandwidth management in DMZ with bandwidth xxx bps. If the user doesn't set the bandwidth, the default value is 100Mbps.
				<wrr|prr>		Select fairness-based(WRR) or priority-based(PRR) mechanism. the default value is fairness-based.
				<efficient>		Enable work-conserving feature.
			disable			Disable bandwidth management in DMZ
		wlan	enable	<bandwidth xxx>		Enable bandwidth management in WLAN with bandwidth xxx bps. If the user doesn't set the bandwidth, the default value is 100Mbps.
				<wrr|prr>		Select fairness-based(WRR) or priority-based(PRR) mechanism. the default value is fairness-based.
				<efficient>		Enable work-conserving feature.
			disable			Disable bandwidth management in WLAN
	class	lan	add #	bandwidth xxx	<name xxx>	Add a class with bandwidth xxx bps in LAN. The name is for users' information.
					<priority x>	Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The default value is 3.
					<borrow on|off>	The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The default value is off.
			mod #	<bandwidth xxx>		Modify the parameters of the class in LAN. The bandwidth is unchanged if the user doesn't set a new value.
				<name xxx>		Set the class' name.
				<priority x>		Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The priority is unchanged if the user doesn't set a new value.
				<borrow on|off>		The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The borrow is unchanged if the user doesn't set a new value.

			del #			Delete the class # and its filter and all its children class and their filters in LAN.
		wan	add #	bandwidth xxx	<name xxx>	Add a class with bandwidth xxx bps in WAN. The name is for users' information.
					<priority x>	Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The default value is 3.
					<borrow on|off>	The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The default value is off.
			mod #	<bandwidth xxx>		Modify the parameters of the class in WAN. The bandwidth is unchanged if the user doesn't set a new value.
				<name xxx>		Set the class' name.
				<priority x>		Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The priority is unchanged if the user doesn't set a new value.
				<borrow on|off>		The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The borrow is unchanged if the user doesn't set a new value.
			del #			Delete the class # and its filter and all its children class and their filters in WAN.
		dmz	add #	bandwidth xxx	<name xxx>	Add a class with bandwidth xxx bps in DMZ. The name is for users' information.
					<priority x>	Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The default value is 3.
					<borrow on|off>	The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The default value is off.
			mod #	<bandwidth xxx>		Modify the parameters of the class in DMZ. The bandwidth is unchanged if the user doesn't set a new value.
				<name xxx>		Set the class' name.
				<priority x>		Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The priority is unchanged if the user doesn't set a new value.
				<borrow on|off>		The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The borrow is unchanged if the user doesn't set a new value.
			del #			Delete the class # and its filter and all its children class and their filters in DMZ.
		wlan	add #	bandwidth xxx	<name xxx>	Add a class with bandwidth xxx bps in WLAN. The name is for users' information.
					<priority x>	Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The default value is 3.
					<borrow on|off>	The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The default value is off.
			mod #	<bandwidth xxx>		Modify the parameters of the class in WLAN. The bandwidth is unchanged if the user doesn't set a new value.

				<name xxx>		Set the class' name.
				<priority x>		Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The priority is unchanged if the user doesn't set a new value.
				<borrow on|off>		The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The borrow is unchanged if the user doesn't set a new value.
			del #			Delete the class # and its filter and all its children class and their filters in WLAN.
	filter	lan	add #	Daddr <mask Dmask> Dport Saddr <mask Smask> Sport protocol		Add a filter for class # in LAN. The filter contains destination address (netmask), destination port, source address (netmask), source port and protocol. You may set the value as 0 if you do not care the item.
			del #			Delete a filter which belongs to class # in LAN.
		wan	add #	Daddr <mask Dmask> Dport Saddr <mask Smask> Sport protocol		Add a filter for class # in WAN. The filter contains destination address (netmask), destination port, source address (netmask), source port and protocol. You may set the value as 0 if you do not care the item.
			del #			Delete a filter which belongs to class # in WAN.
		dmz	add #	Daddr <mask Dmask> Dport Saddr <mask Smask> Sport protocol		Add a filter for class # in DMZ. The filter contains destination address (netmask), destination port, source address (netmask), source port and protocol. You may set the value as 0 if you do not care the item.
			del #			Delete a filter which belongs to class # in DMZ.
		wlan	add #	Daddr <mask Dmask> Dport Saddr <mask Smask> Sport protocol		Add a filter for class # in WLAN. The filter contains destination address (netmask), destination port, source address (netmask), source port and protocol. You may set the value as 0 if you do not care the item.
			del #			Delete a filter which belongs to class # in WLAN.
	show	interface	lan			Show the interface settings of LAN
			wan			Show the interface settings of WAN
			dmz			Show the interface settings of DMZ
			wlan			Show the interface settings of WLAN
		class	lan			Show the classes settings of LAN
			wan			Show the classes settings of WAN
			dmz			Show the classes settings of DMZ
			wlan			Show the classes settings of WLAN
		filter	lan			Show the filters settings of LAN
			wan			Show the filters settings of WAN
			dmz			Show the filters settings of DMZ
			wlan			Show the filters settings of WLAN
		statistics	lan			Show the statistics of the classes in LAN
			wan			Show the statistics of the classes in WAN
			dmz			Show the statistics of the classes in DMZ
			wlan			Show the statistics of the classes in WLAN
	monitor	lan	<#>			Monitor the bandwidth of class # in LAN. If the class is not specific, all the classes in LAN will be monitored.

							Description
							The first time you key the command will set it on; the second time you will set it off, and so on.
		wan	<#>				Monitor the bandwidth of class # in WAN. If the class is not specific, all the classes in WAN will be monitored. The first time you key the command will set it on; the second time you will set it off, and so on.
		dmz	<#>				Monitor the bandwidth of class # in DMZ. If the class is not specific, all the classes in DMZ will be monitored. The first time you key the command will set it on; the second time you will set it off, and so on.
		wlan	<#>				Monitor the bandwidth of class # in WLAN. If the class is not specific, all the classes in WLAN will be monitored. The first time you key the command will set it on; the second time you will set it off, and so on.
	config	save					Save the configuration.
		load					Load the configuration.
		clear					Clear the configuration.
	debug						
	defaultClassBw						

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
		cnt		
			disp	Display firewall log type and count.
			clear	Clear firewall log count.
		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		
			triangle	Set if firewall ignore triangle route in lan/wan/dmz/wlan
		schedule		
			load [set # rule #]	
			display	

				save	
				week	
				timeOfDay [always/hh:mm]	

Certificate Management (PKI) Command   Home

Command				Description
certificates				
	my_cert			
		create		
			selfsigned <name> <subject> [key size]	Create a self-signed local host certificate. <name> specifies a descriptive name for the generated certificate. <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
			request <name> <subject> [key size]	Create a certificate request and save it to the router for later manual enrollment. <name> specifies a descriptive name for the generated certification request. <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
			scep_enroll <name> <CA addr> <CA cert> <auth key> <subject> [key size]	Create a certificate request and enroll for a certificate immediately online using SCEP protocol. <name> specifies a descriptive name for the enrolled certificate. <CA addr> specifies the CA server address. <CA cert> specifies the name of the CA certificate. <auth key> specifies the key used for user authentication. If the key contains spaces, please put it in quotes. To leave it blank, type "". <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
			cmp_enroll <name> <CA addr> <CA cert> <auth key> <subject> [key size]	Create a certificate request and enroll for a certificate immediately online using CMP protocol. <name> specifies a descriptive name for the enrolled certificate. <CA addr> specifies the CA server address. <CA cert> specifies the name of the CA certificate. <auth key> specifies the id and key used for user authentication. The format is "id:key". To leave the id and key blank, type ":". <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
		import [name]		Import the PEM-encoded certificate from stdin. [name] specifies the descriptive name (optional) as which the imported certificate is to be saved. For my certificate importation to be successful, a certification request corresponding to the

				imported certificate must already exist on ZyWALL. After the importation, the certification request will automatically be deleted. If a descriptive name is not specified for the imported certificate, the certificate will adopt the descriptive name of the certification request.
		export <name>		Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
		view <name>		View the information of the specified local host certificate. <name> specifies the name of the certificate to be viewed.
		verify <name> [timeout]		Verify the certification path of the specified local host certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
		delete <name>		Delete the specified local host certificate. <name> specifies the name of the certificate to be deleted.
		list		List all my certificate names and basic information.
		rename <old name> <new name>		Rename the specified my certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
		def_selfsigned [name]		Set the specified self-signed certificate as the default self-signed certificate. [name] specifies the name of the certificate to be set as the default self-signed certificate. If [name] is not specified, the name of the current self-signed certificate is displayed.
	ca_trusted			
		import <name>		Import the PEM-encoded certificate from stdin. <name> specifies the name as which the imported CA certificate is to be saved.
		export <name>		Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
		view <name>		View the information of the specified trusted CA certificate. <name> specifies the name of the certificate to be viewed.
		verify <name> [timeout]		Verify the certification path of the specified trusted CA certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
		delete <name>		Delete the specified trusted CA certificate. <name> specifies the name of the certificate to be deleted.
		list		List all trusted CA certificate names and basic information.
		rename <old name> <new name>		Rename the specified trusted CA certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
		crl_issuer <name> [on|off]		Specify whether or not the specified CA issues CRL. <name> specifies the name of the CA certificate. [on|off] specifies whether or not the CA issues CRL. If [on|off] is not specified, the current crl_issuer status of the CA.
	remote _trusted			
		import <name>		Import the PEM-encoded certificate from stdin. <name> specifies the name as which the imported remote host

				certificate is to be saved.
		export <name>		Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
		view <name>		View the information of the specified trusted remote host certificate. <name> specifies the name of the certificate to be viewed.
		verify <name> [timeout]		Verify the certification path of the specified trusted remote host certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
		delete <name>		Delete the specified trusted remote host certificate. <name> specifies the name of the certificate to be deleted.
		list		List all trusted remote host certificate names and basic information.
		rename <old name> <new name>		Rename the specified trusted remote host certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
	dir_ser ver			
		add <name> <addr[:port]> [login:pswd]		Add a new directory service. <name> specifies a descriptive name as which the added directory server is to be saved. <addr[:port]> specifies the server address (required) and port (optional). The format is "server-address[:port]". The default port is 389. [login:pswd] specifies the login name and password, if required. The format is "[login:password]".
		delete <name>		Delete the specified directory service. <name> specifies the name of the directory server to be deleted.
		view <name>		View the specified directory service. <name> specifies the name of the directory server to be viewed.
		edit <name> <addr[:port]> [login:pswd]		Edit the specified directory service. <name> specifies the name of the directory server to be edited. <addr[:port]> specifies the server address (required) and port (optional). The format is "server-address[:port]". The default port is 389. [login:pswd] specifies the login name and password, if required. The format is "[login:password]".
		list		List all directory service names and basic information.
		rename <old name> <new name>		Rename the specified directory service. <old name> specifies the name of the directory server to be renamed. <new name> specifies the new name as which the directory server is to be saved.

AutoSec Related Command
Home

Command				Description
autoS ec				
	start			
	duration		<value(sec)>	
	port		<port_num>	
	key		<USER_KEY>	
	gui_start			

SMT Related command

Home

No	Command	Description	Comment
	sys general load	Load system general info to buffer	Menu 1
	sys general bridge [on|off]	Set system bridge on/off	Menu 1
	sys general routeip [on|off]	Set system IP routing on/off	Menu 1
	sys general location [geographic location]	Set the geographic location of your prestige.	Menu 1
	sys general hostname [hostname]	Set system name	Menu 1
	sys general contactname [contactname]	Set contact person's name	Menu 1
	sys general domainname [domainname]	Set domainname	Menu 1
	sys general save	Save general info to flash.	Save Menu 1
	sys general display	Display information in menu 1	Display Menu 1
	sys ddns debug	Open dynamic DNS debug mode	Menu 1.1
	sys ddns display	Display dynamic DNS information	Menu 1.1
	sys ddns restart	Restart dynamic DNS	Menu 1.1
	sys ddns logout	Logout dynamic DNS	Menu 1.1
	sys ddns config load	Load dynamic DNS to buffer	Menu 1.1
	sys ddns config active [0|1]	Active dynamic DNS	Menu 1.1
	sys ddns config hostname	Set the domain name assigned by dynamic DNS provider	Menu 1.1
	sys ddns config emailaddress	Set your E-mail address	Menu 1.1
	sys ddns config username	Set your user name	Menu 1.1
	sys ddns config password	Set the password assigned to you	Menu 1.1
	sys ddns config save	Save dynamic DNS setting to flash	Menu 1.1
	sys default	Load All Default Settings Except LAN and DHCP.	
	sys save	Save all the parameters which will include menu1, menu 3.2 LAN, menu 4 or menu 11 WAN, menu 12 static route, menu 15 NAT server set, menu 21 filter sets, menu 22 SNMP, menu 24.11 remote management and 3.5 Wireless LAN	
	lan index [1|2|3] 1: Select main LAN Interface 2: Select IP Alias 1 3: Select IP Alias 2	Select a LAN interface to edit	Menu 3.2
	lan active [on|off]	Turn on or off on IP Alias Interface	Menu 3.2.1
	lan ipaddr [address] [subnet mask]	Set LAN IP address and subnet mask Example: > lan ipaddr 192.168.1.1 255.255.255.0	Menu 3.2
	lan rip [none|in|out|both] [rip1|rip2b|rip2m]	Set LAN IP RIP mode and RIP version, if you choose none in the first parameter, the second parameter is also necessary	Menu 3.2
	lan multicast [none|igmpv1|igmpv2]	Set LAN IP multicast mode	Menu 3.2
	lan filter [incoming|outgoing] [tcpip|generic] [set#1] [set#2] [set#3] [set#4]	Set LAN filter to be incoming/outgoing or protocol /device and the filter set could be 1-12, 0 means empty Example: Lan filter incoming tcpip 1 0 0 0	Menu 3.1
	lan dhcp mode [server|relay|none]	Set DHCP mode to be"server", "relay", "none"	Menu 3.2
	lan dhcp server dnsserver [pri dns] [sec dns]	Set primary and secondary LAN DNS server	Menu 3.2
	lan dhcp server pool [start-address] [num]	Set DHCP start address and pool size	Menu 3.2
	lan dhcp server gateway [IP address]	Set DHCP gateway	Menu 3.2

	lan dhcp server netmask [subnet mask]	Set DHCP subnet mask	Menu 3.2
	lan dhcp server leasetime [second]	Set DHCP lease time	Menu 3.2
	lan dhcp server renewaltime [second]	Set DHCP renew time	Menu 3.2
	lan dhcp server rebindtime [second]	Set DHCP rebind time	Menu 3.2
	lan dhcp relay server [IP address]	Set IP address of DHCP relay server	Menu 3.2
	lan display	Display LAN or IP alias parameters	Display Menu 3
	lan clear	Clear the Working Buffer	
	lan save	Save LAN related parameters	
	wan node index [1-8]	Set the node pointer to specific wan profile. If you want to set WAN profile, please use this command first, system will use the index number for pointing to specific PVC (remote node), and for consequent commands reference, if index = 1 means it's ISP node	Menu 11.1
	wan node clear	Clear the parameters of the temporary WAN profile	Menu 11.1
	wan node ispname [ISP name]	Enable the name of wan node	Menu 11.1
	wan node enable	Enable the wan profile	Menu 11.1
	wan node disable	Disable the wan profile	Menu 11.1
	wan node encap [1483|pppoa|pppoe|enet]	Set the wan protocol	Menu 11.1
	wan node mux [vc|llc]	Set the wan multiplex	Menu 11.1
	wan node ppp authen [chap|pap|both]	Set PPP authentication type	Menu 11.1
	wan node ppp username [name]	Set PPP username	Menu 11.1
	wan node ppp password [password]	Set PPP password	Menu 11.1
	wan node service [name]	Set PPPoE service name	Menu 11.1
	wan node bridge [on|off]	Set the wan bridge mode	Menu 11.1
	wan node routeip [on|off]	Set the wan IP routing mode	Menu 11.1
	wan node callsch [set1#][set2#][set3#][set4#]	Set call schedule set, set number 0 means empty	Menu 11.1
	wan node nailedup [on|off]	Set nailed up connection on/off	Menu 11.1
	wan node vpi [num]	Set the wan vpi. Range : 0~255	Menu 11.6
	wan node vci [num]	Set the wan vci. Range : 32~65535	Menu 11.6
	wan node qos[ubr|cbr]	Set the wan QOS type to be UBR or CBR	Menu 11.6
	wan node pcr [num]	Set the wan PCR value	Menu 11.6
	wan node scr [num]	Set the wan SCR value	Menu 11.6
	wan node mbs [num]	Set the wan MBS value	Menu 11.6
	wan node wanip [static|dynamic] [address]	Set the wan IP address	Menu 11.3
	wan node remoteip [address] [subnet mask]	Set the remote gateway IP address and subnet mask	Menu 11.3
	wan node nat [off	sua	full] [address mapping #]	Set type wan NAT mode to be off or SUA or Full feature	Menu 11.3
	wan node metric [num]	Set the wan metric number	Menu 11.3
	wan node private [yes|no]	Set the wan private or not.	Menu 11.3
	wan node rip [none|in|out|both] [rip1|rip2b|rip2m]	Set the wan RIP mode and RIP version	Menu 11.3
	wan node multicast [none|igmpv1|igmpv2]	Set the wan IP multicast mode	Menu 11.3
	wan node ippolicy [set #1] [set #2] [set #3] [set #4]	Set WAN IP policy can be specified, and policy set can be 1-12, value 0 means empty	Menu 11.3
	wan node bridgetimeout [min#]	Set wan bridge mode, Ethernet address timeout minutes.	Menu 11.3

	wan node filter [incoming|outgoing] [tcpip|generic] [set #1] [set #2] [set #3] [set #4]	Set WAN filter, incoming or outgoing can be specified, and filter set can be 1-12, value 0 means empty	Menu 11.5
	wan node idletimeout [second]	Set idle timeout.	Menu 11.1
	wan node save	Save the related parameters of WAN node	
	wan node display	Display WAN profile configuration in buffer	Display Menu 11
	ip route addrom index [Rule #]	Select a Static Route index 1-16 to edit	Menu 12.1
	ip route addrom name [Name]	Set Rule Name	Menu 12.1
	ip route addrom active [on|off]	Set Active or Inactive Flag	Menu 12.1
	ip route addrom set [dest address/ mask bits] [gateway] [metric]	Set IP static route Example: > ip ro addrom set 192.168.1.33/24 192.168.1.1 2	Menu 12.1
	ip route addrom private [yes|no]	Set Private Flag	Menu 12.1
	ip route addrom disp	Display both working buffer and Editing Entry	Menu 12.1
	ip route addrom freememory	Discard all changes	Menu 12.1
	ip route addrom save	Save edited settings	Menu 12.1
	ip route addrom clear [Index #]	Clear Static Route Index	Menu 12.1
	bridge staticRoute index [Rule #]	Select a bridge Static Route index 1-16 to edit	Menu 12.3
	bridge staticRoute name [Name]	Set Rule Name	Menu 12.3
	bridge staticRoute active [on|off]	Set Active or Inactive Flag	Menu 12.3
	bridge staticRoute set [ether address] [ipaddress] [gatewayNode]	Set bridge static route Example: >bridge staticRoute set 001349012345 192.168.1.1 1	Menu 12.3
	bridge staticRoute display	Display both working buffer and Editing Entry	Menu 12.3
	bridge staticRoute freememory	Discard all changes	Menu 12.3
	bridge staticRoute save	Save edited settings	Menu 12.3
	bridge staticRoute clear [Index #]	Clear Static Route Index	Menu 12.3
	sys dialinUser index [index #]	Set the index of dial-in user, you may apply this command first before you begin to configure the dial-in user.	Menu 14
	sys dialinUser username [username]	Set the name of dial-in user	Menu 14
	sys dialinUser active [yes | no]	Active the dial-in user	Menu 14
	sys dialinUser password [password]	Set password	Menu 14
	sys dialinUser display	Display configuration	Menu 14
	sys dialinUser save	Save configuration	Menu 14
	sys dialinUser free	Free buffer info of the dial-in user	Menu 14
	sys dialinUser clear	Delete the dial-in user	Menu 14
	ip nat addrmap map [map#] [set name]	Select NAT address mapping set and set mapping set name, but set name is optional Example: > ip nat addrmap map 1 myset	Menu 15.1
	ip nat addrmap rule [rule#] [insert | edit] [type] [local start IP] [local end IP] [global start IP] [global end IP] [server set #]	Set NAT address mapping rule. If the "type" is not "inside-server" then the "type" field will still need a dummy value like "0". Type is 0 - 4 = one-to-one, many-to-one, many-to-many-overload, many-to-many-non overload, inside-server Example: > ip nat addrmap rule 1 edit 3 192.168.1.10 192.168.1.20 192.168.10.56 192.168.1.56 0	Menu 15.1

ip nat addrmap clear [map#] [rule#]	Clear the selected rule of the set	Menu 15.1
ip nat addrmap freememory	Discard Changes	Menu 15.1
ip nat addrmap disp	Display nat set information	Menu 15.1
ip nat addrmap save	Save settings	Menu 15.1
ip nat server load [set#]	Load the server sets of NAT into buffer	Menu 15.2
ip nat server disp [1]	"disp 1" means to display the NAT server set in buffer, if parameter "1" is omitted, then it will display all the server sets	Menu 15.2
ip nat server save	Save the NAT server set buffer into flash	Menu 15.2
ip nat server clear [set#]	Clear the server set [set#], must use "save" command to let it save into flash	Menu 15.2
ip nat server edit [rule#] active	Activate the rule [rule#], rule number is 1 to 24, the number 25-36 is for UPNP application	Menu 15.2
ip nat server edit [rule#] svrport <start port> <end port>	Configure the port range from <start port > to <end port>	Menu 15.2
ip nat server edit [rule#] remotehost <start IP> <end IP>	Configure the IP address range of remote host (Leave it to be default value if you don't need this command)	Menu 15.2
ip nat server edit [rule#] leasetime <seconds>	Configure the lease time (Leave it to be default value if you don't want this command)	Menu 15.2
ip nat server edit [rule#] rulename <string>	Configure the name of the rule (Leave it to be default value if you don't want this command)	Menu 15.2
ip nat server edit [rule#] forwardip <IP address>	Configure the LAN IP address to be forwarded	Menu 15.2
ip nat server edit [rule#] protocol <TCP|UDP|ALL>	Configure the protocol to be used TCP , UDP or ALL (it must be capital)	Menu 15.2
sys filter set index [set#] [rule#]	Set the index of filter set rule, you must apply this command first before you begin to configure the filter rules	Menu 21 filter sets
sys filter set name [set name]	Set the name of filter set	Menu 21 filter sets
sys filter set type [tcpip	generic]	Set the type of filter rule	Menu 21 filter sets
sys filter set enable	Enable the rule	Menu 21 filter sets
sys filter set disable	Disable the rule	Menu 21 filter sets
sys filter set protocol [protocol #]	Set the protocol ID of the rule	Menu 21 filter sets
sys filter set sourceroute [yes|no]	Set the sourceroute yes/no	Menu 21 filter sets
sys filter set destip [address] [subnet mask]	Set the destination IP address and subnet mask of the rule	Menu 21 filter sets
sys filter set destport [port#] [compare type = none|equal|notequal|less|greater]	Set the destination port and compare type (compare type could be 0(none)|1(equal)|2(not equal)|3(less)|4(greater))	Menu 21 filter sets
sys filter set srcip [address] [subnet mask]	Set the source IP address and subnet mask	Menu 21 filter sets
sys filter set srcport [port#] [compare type = none|equal|not equal|less|greater]	Set the source port and compare type (compare type could be 0(none)|1(equal)|2(not equal)|3(less)|4(greater))	Menu 21 filter sets
sys filter set tcpEstab [yes|no]	Set TCP establish option	
sys filter set more [yes|no]	Set the more option to yes/no	Menu 21 filter sets
sys filter set log [type 0-3= none	match| notmatch	both]	Set the log type (it could be 0-3 =none, match, not match, both)	Menu 21 filter sets
sys filter set actmatch[type 0-2 = checknext	forward	drop]	Set the action for match	Menu 21 filter sets
sys filter set actnomatch [type 0-2 = checknext	forward	drop]	Set the action for not match	Menu 21 filter sets
sys filter set offset [#]	Set offset for the generic rule	Menu 21, it's for generic filter
sys filter set length [#]	Set the length for generic rule	Menu 21, it's for

			generic filter
	sys filter set mask [#]	Set the mask for generic rule	Menu 21, it's for generic filter
	sys filter set value [(depend on length in hex)]	Set the value for generic rule	Menu 21, it's for generic filter
	sys filter set clear	Clear the current filter set	Menu 21
	sys filter set save	Save the filter set parameters	
	sys filter set display [set#][rule#]	Display Filter set information. W/o parameter, it will display buffer information.	
	sys filter set freememory	Discard Changes	
	sys snmp disp	Display SNMP parameters	Menu 22
	sys snmp get [community]	Set the community string of get	Menu 22 SNMP
	sys snmp set [community]	Set the community string of set	Menu 22 SNMP
	sys snmp trusthost [IP address]	Set the IP address of trusted host	Menu 22 SNMP
	sys snmp trap community [community]	Set the community string of trap	Menu 22 SNMP
	sys snmp trap destination [IP address]	Set the destination address of trap	Menu 22 SNMP
	sys snmp discard	Discard changes	
	sys snmp clear	Clear Working Buffer	
	sys snmp save	Set the SNMP parameters	Menu 22 SNMP
	sys password	Set system password: input current password->input new password-> confirm new password	Menu 23 system password
	sys baud [1:38400|2:19200|3:9600|4:57600|5:115200]	Index 12,3 will be 38400,19200, 9600, 57600, 115200 bps [save immediately]	Menu 24.2.2 console speed
	Wan adsl version	Display chipset vendor and modem code version	Menu 24.2.1
	Wan adsl opmode display	Display DSL setting mode	Menu 24.2.1
	sys timeserver load	Load time server info to buffer.	Menu 24.10 time server
	sys timeserver protocol [0: daytime RFC 867 | 1:time RFC 868 | 2: NTP RFC 1305]	Set time protocol	Menu 24.10 time server
	sys timeserver address [address]	Set time server address, it can be an IP address or domain name	Menu 24.10 time server
	sys timeserver timezone [-12 ~12]	Set time zone, -12 means GMT-12, 0 mean GMT, 12 means GMT+12.	Menu 24.10 time server
	sys timeserver daylightsaving active[yes | no]	Set daylight saving	Menu 24.10 time zone
	sys timeserver daylightSaving start [month] [day]	Set daylight saving start day	Menu 24.10 daylight saving
	sys timeserver daylightSaving end [month] [day]	Set daylight saving end day	Menu 24.10 daylight saving
	sys timeserver save	Save time server and daylight saving setting	Menu 24.10 daylight saving
	sys timeserver checktime	Connect to time server and check time.	Menu 24
	sys timeserver display	Display time server and daylight saving setting	Menu 24
	sys server load	Load setting before editing	
	sys server access [ftp|telnet|web] [access type]	Set the server access type to be 0: ALL, 1: None, 2:LAN only, 3:WAN only	Menu 24.11 remote management
	sys server port [ftp|telnet|web] [port]	Set the server port number	Menu 24.11 remote

			management
	sys server secureip[ftp|telnet|web] [address]	Set the server security IP address	Menu 24.11 remote management
	sys server disp [1]	Display server settings in buffer, [1] means display flash	
	sys server save	Save the embedded server (remote management) parameters	
	ip policyRouting set index [set#] [rule#]	Set the index of IP routing policy set rule. You must apply this command first before you begin to configure the IP routing policy rules	Menu 25 IP routing policy
	ip policyRouting set name [set name]	Set the name of IP routing policy set	Menu 25 IP routing policy
	ip policyRouting set active [yes |no]	Enable/Disable the rule	Menu 25 IP routing policy
	ip policyRouting set criteria protocol [protocol #]	Set the protocol ID of the rule	Menu 25 IP routing policy
	ip policyRouting set criteria serviceType [0: don't care | 1: normal | 2: min delay | 3: max thruput | 4: max reliable| 5: min cost]	Set the IP routing policy criteria type of service	Menu 25 IP routing policy
	ip policyRouting set criteria precedence [0~7 | 8 =don't care]	Set the IP routing policy precedence	Menu 25 IP routing policy
	ip policyRouting set criteria packetlength [#]	Set the IP routing policy packet length	Menu 25 IP routing policy
	ip policyRouting set criteria lencomp [0: greater | 1: less or equal | 2: greater or equal | 3: equal | 4: not equal | 5: less]	Set the IP routing policy len comp	Menu 25 IP routing policy
	ip policyRouting set criteria srcip [start ip] [end ip]	Set the IP routing policy source IP address	Menu 25 IP routing policy
	ip policyRouting set criteria srcport [start port] [end port]	Set the IP routing policy source port	Menu 25 IP routing policy
	ip policyRouting set criteria destip [start ip] [end ip]	Set the IP routing policy destination IP address	Menu 25 IP routing policy
	ip policyRouting set criteria destport [start port] [end port]	Set the IP routing policy destination port	Menu 25 IP routing policy
	ip policyRouting set action actmatched	Set the IP routing policy matched action	Menu 25 IP routing policy
	ip policyRouting set action actnomatched	Set the IP routing policy no matched action	Menu 25 IP routing policy
	ip policyRouting set action gatewaytype [1 gateway node | 0 gateway addr]	Set IP routing policy gateway type	Menu 25 IP routing policy
	ip policyRouting set action gatewayaddr [gateway address #]	Set IP routing policy gateway address	Menu 25 IP routing policy
	ip policyRouting set action gatewaynode [gateway node #]	Set IP routing policy gateway node	Menu 25 IP routing policy
	ip policyRouting set action serviceType [0: don't care | 1: normal | 2: min delay | 3: max thruput | 4: max reliable| 5: min cost]	Set IP routing policy type of service	Menu 25 IP routing policy
	ip policyRouting set action precedence [0~7 | 8 =don't care]	Set IP routing policy precedence	Menu 25 IP routing policy
	ip policyRouting set action log [yes | no]	Set IP routing policy log	Menu 25 IP routing policy
	ip policyRouting set display	Display the current IP routing policy setting	Menu 25 IP routing policy
	ip policyRouting set save	Save the current IP routing policy setting	Menu 25 IP routing policy

	ip policyRouting set freememory	free the current IP routing policy setting	Menu 25 IP routing policy
	ip policyRouting set clear	Clear the IP routing policy setting	Menu 25 IP routing policy
	ip policyRouting clear	Clear the IP routing policy count	Menu 25 IP routing policy
	ip policyRouting display	Display the IP routing policy count	Menu 25 IP routing policy
	ip policyRouting switch	Switch on or off IP routing policy count.	Menu 25 IP routing policy
	wan callsch index [set#]	Set call schedule index #. You must apply this command first before you begin to configure call schedule	Menu 26 schedule
	wan callsch name [set name]	Set the schedule name	Menu 26 schedule
	wan callsch active [Yes | No]	Enable/Disable schedule	Menu 26 schedule
	wan callsch startday [year] [month] [day]	Set schedule start day	Menu 26 schedule
	wan callsch onceday [year] [month] [day]	Set schedule once day	Menu 26 schedule
	wan callsch weeklyday Sunday [1:active|0:inactive]	Set schedule weekly day	Menu 26 schedule
	wan callsch weeklyday Monday [1:active|0:inactive]	Set schedule weekly day	Menu 26 schedule
	wan callsch weeklyday Tuesday [1:active|0:inactive]	Set schedule weekly day	Menu 26 schedule
	wan callsch weeklyday Wednesday [1:active|0:inactive]	Set schedule weekly day	Menu 26 schedule
	wan callsch weeklyday Thursday [1:active|0:inactive]	Set schedule weekly day	Menu 26 schedule
	wan callsch weeklyday Friday [1:active|0:inactive]	Set schedule weekly day	Menu 26 schedule
	wan callsch weeklyday Saturday [1:active|0:inactive]	Set schedule weekly day	Menu 26 schedule
	wan callsch starttime [hour] [minute]	Set schedule start time	Menu 26 schedule
	wan callsch duration [hour] [minute]	Set schedule duration time	Menu 26 schedule
	wan callsch action [0:fource on | 1 force down | 2: enable dial-on-demand | 3: disable dial-on-demand]	Set action	Menu 26 schedule
	wan callsch display	display the current call schedule set	Menu 26 schedule
	wan callsch save	Save the current call schedule set	Menu 26 schedule
	wan callsch freememory	free the current call schedule set	Menu 26 schedule
	wan callsch clear	Clear the call schedule set	Menu 26 schedule
	wlan load	Load system parameters into working buffer	Menu 3.5 for Wireless LAN
	wlan disp	Display the working buffer	Menu 3.5 for Wireless LAN
	wlan essid [name]	Set the wireless ESSID	Menu 3.5 for wireless LAN
	wlan hideessid [on|off]	Set to hide ESSID or not	Menu 3.5 for wireless LAN
	wlan chid [#=1~13]	Set channel ID 1-13	Menu 3.5 for wireless LAN
	wlan threshold rts [value]	Set the RTS threshold value	Menu 3.5 for wireless LAN
	wlan threshold fragment [value]	Set fragment threshold	Menu 3.5 for

			wireless LAN
	wlan wep type [none|64|128]	Set the wep type to be none, 64bit or 128bits	Menu 3.5 for wireless LAN
	wlan wep key set [key set#1-4] [key value]	Set wep key value	Menu 3.5 for wireless LAN
	wlan wep key default [key set # 1-4]	Set default key set value	Menu 3.5 for wireless LAN
	wlan macfilter enable	Enable mac filter	Menu 3.5.1 for wireless LAN
	wlan macfilter disable	Disable mac filter	Menu 3.5.1 for wireless LAN
	wlan macfilter action [allow|deny]	Set the action type of filter	Menu 3.5.1 for wireless LAN
	wlan macfilter set [set# 1-12] [mac address]	Set the mac address of filter	Menu 3.5.1 for wireless LAN
	wlan clear	Clear Working Buffer	
	wlan save	Save wireless MAC filter parameters	