



Firmware Release Note

Prestige 650H-31

Standard version

Release 3.40(IS.3)C0

Date: Aug 15, 2003
Author: Daphne Kuo

ZyXEL Prestige 650H-31 Standard Version release 3.40(IS.3)C0 Release Note

Date: Aug 15, 2003

Supported Platforms:

ZyXEL Prestige 650H-31

Versions:

ZyNOS Version : V3.40(IS.3) | 8/15/2003 13:15:12
Bootbase Version : V1.11 | 3/4/2003 10:26:13

Notes:

The P650H-31 is a small-office and home device that will allow a small LAN to access the Internet. By integrating ADSL, WLAN, NAT, P650H-31 provides the ease of installation and Internet access.

The P650H-31 provides an PCMCIA wireless card slot for 802.11b 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 port for connection to ADSL line.

The version of Alcatel modem code is **3.9.122**

Known Issues:

1. Bandwidth Management:
Not support on-line adding class operation.
2. SIP passthrough:
Currently, only support single user passthrough.
3. In Web GUI, the help page of Firewall only supports English version currently.
4. Update firmware issue :
 - a. Update firmware by FTP and Web: Can't update firmware from 3.40(IS.0), 3.40(IS.1) and 3.40(IS.2) to 3.40(IS.3) by FTP and Web
 - b. Only update firmware by console

Features:

Modifications in V 3.40(IS.3)C0 | 08/15/2003

1. [FEATURE ENHANCED]
Symptom:Support Firewall

ZyXEL Confidential

2. [FEATURE ENHANCED]
Symptom: Support Content filter
3. [FEATURE ENHANCED]
Symptom: Support IPSec with 10 VPN tunnels
1. [FEATURE ENHANCED]
Symptom: Support ZyAir B-120 driver
4. [FEATURE ENHANCED]
Symptom: Support the CI command “ip adjmss [<mss>]” to adjust mss value.
5. [BUG FIXED] SIP pass-through bug fixed
Symptom: The exception will be occurred if using the Telia puhekaista.msi sip userAgent software.
Condition: The callID had no ipAddress. This will cause the system get null point for cpOffset[CALLID]

Modifications in V 3.40(IS.2) | 06/16/2003

1. Change to FCS version.

Modifications in V 3.40(IS.2)b2 | 06/02/2003

1. [NEW FEATURE]
Support Bandwidth Management. See [Appendix 1](#)
2. [FEATURE ENHANCED]
Support SIP passthrough.
3. [FEATURE ENHANCED]
Add time server setup page at eWC.
4. [BUG FIXED]
Symptom: Can't play XBox Live via NAT router.
5. [BUG FIXED]
Symptom: If the traffic for Polycom camera pass our router, the router would be reboot.
6. [FEATURE ENHANCED]
Symptom: Enhance SPTGEN feature
Condition:
 - 1) Add RIP direction and version for SMT menu4.
 - 2) Add active and protocol option for SMT menu15 (NAT).
 - 3) Extend filter set from 1 to 2 set.
 - 4) Support ADSL opencmd function.

Modifications in V 3.40(IS.2)b1 | 04/21/2003

1. [FEATURE ENHANCED]
Support Multi-Lingual Web (English, France, Germany)
2. [FEATURE ENHANCED]
Support 802.1X
3. [FEATURE ENHANCED]
Add Web pages to configure 802.1x: (1)Local user database and Radius (in Advance Panel) ; (2)Association list and Channel usage (in Maintenance Panel)
4. [FEATURE CHANGED]

ZyXEL Confidential

Turn off some wireless related web-pages and SMT menu item(menu3.5 Wireless LAN Setup) when wireless card isn't installed in the device.

5. [FEATURE ENHANCED]
Enlarge the size of WLAN MAC filter number to be 32

Modifications in V 3.40(IS.1) | 03/12/2003

6. Change version to FCS version.

Modifications in V 3.40(IS.1)b6 | 03/07/2003

1. [BUG FIXED]
Symptom: 8 PVCs can't work fine.
Condition: Not plug wireless card, 8 PVCs test will fail.

Modifications in V 3.40(IS.1)b5 | 03/04/2003

1. [BUG FIXED]
Symptom: Telnet to device cause system reboot.
Condition: Close adsl line, when adsl up, then telnet to device will cause system reboot.
2. [BUG FIXED]
Symptom: Can't change UBR to CBR in eWC.
3. [FEATURE ENHANCED]
Symptom: Add web help for WAN setup page.
4. [BUG FIXED]
Symptom: In wizard setup, OAM test will fail.
Condition: Configure device to PPPoA encap. and Nailed up is turn off

Modifications in V 3.40(IS.1)b4 | 02/25/2003

1. [FEATURE ENHANCED]
Symptom: Support SDRAM auto-detect for 8MB-32bit x1 & 8MB-16bit x2
Condition: Need to update bootbase version to 1.10
2. [FEATURE ENHANCED]
Symptom: Support generic filter for wireless channel.
Usage: wlan filter <incoming|outgoing> <generic> [set#1] [set#2] [set#3] [set#4]
3. [FEATURE ENHANCED]
Symptom: Update wireless available channels for certain countries.
4. [FEATURE ENHANCED]
Symptom: Support wireless basicrate and txrate.
Condition: Can't adjust basicrate and txrate for Intersil Card.
5. [FEATURE ENHANCED]
Symptom: Add WAN setup page in eWC.
6. [BUG FIXED]
Symptom: Video pixel issue
Condition: While downstream have multicast traffic(Video stream) and upstream have data traffic(FTP upload). There is pixel occurred every 2~3 mins.

Modifications in V 3.40(IS.1)b3 | 01/07/2003

ZyXEL Confidential

1. [FEATURE CHANGED]
Create new model ID for standard version. Hence, must update bootbase to 1.06

Modifications in V 3.40(IS.1)b1 | 12/24/2002

1. [BUG FIXED]
Sympton: Decompress error.
Condition: When system reboot, if Ethernet have traffic will cause system decompress error after "wan chann init ... done".

Modifications in V 3.40(IS.0)b5 | 12/19/2002

1. [BUG FIXED]
Sympton: When system reboot, sometimes exception occurred.
Condition: While ADSL initializing, reboot the system, then exception occurred.
2. [BUG FIXED]
Sympton: FTP uploading, there are many ping timeout.
Condition: When traffic is upstream direction, there are many ping timeout.
3. [BUG FIXED]
Sympton: HTP fail at AT commond "ATTI" test.
Condition: While doing ATTI HTP test, LAN Internal test will fail.
4. [BUG FIXED]
Sympton: WLAN LED status error.
Condition: While WLAN stop send/receive, the WALN LED still blinking.
5. [FEATURE ENHANCED]
Sympton: Adopt new compress algorithm to reduce firmware size.
6. [BUG FIXED]
Sympton: There is downstream cell loss under 64, 128, 256 frame size.
Condition: Connect to AX4000 with Alcatel DSLAM for testing cell loss.
7. [BUG FIXED]
Sympton: In menu 24.1, the status of Ethernet always display "100M/Full Duplex".

Modifications in V 3.40(IS.0)b4 | 12/2/2002

1. Hardware Test Program ready.

Modifications in V 3.40(IS.0)b3 | 11/22/2002

1. WLAN and LED ready.

Modifications in V 3.40(IS.0)b2 | 11/13/2002

1. Hub feature ready.

Modifications in V 3.40(IS.0)b1 | 11/11/2002

2. Create this project.

Appendix 1 Bandwidth Management

Introduction

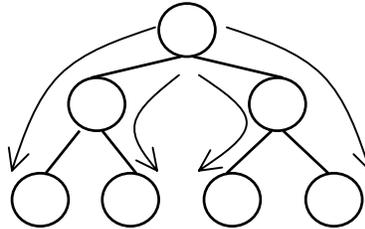


Figure 1.

The typical architecture of CBQ is drawn in figure 1. There are two major components in CBQ configuration. One is “class” and the other is “filter”. Each circle means a class and the hierarchy architecture shows the relation between ancestors and successors. The arrows mean the filters, which classify the incoming packets to the specific class. All of them, classes and filters, are constructed for a “physical” interface. To enable bandwidth management in more than two interfaces, users must configure the settings for each “physical” interface. The word “interface” we mentioned in the rest is meant “physical interface”.

The major mission of bandwidth management is to control the output rate of the flows. To archive this goal, the bandwidth management contains two modules, classifier and scheduler. If there is an outgoing packet, the classifier will classify the packet into a specific class and enqueue it in the queue belong to the class. The scheduler selects one class to dequeue one packet from its queue and makes sure that the output rate for each class is as expected.

There are two schedule mechanisms: Priority Round Robin (PRR) and Weighted Round Robin (WRR). The unused bandwidth will be offered to the class with higher priority under PRR mechanism; the unused bandwidth will be allotted in proportion. PRR is priority-based and WRR is fairness-based. Among these, the action of WRR is confusing. So we use an example to describe the action of WRR mechanism.

	Reserved BW	Actual BW (total bandwidth =100 Mbps)	Actual BW (total bandwidth =10 Mbps)	Actual BW (total bandwidth = 1 Mbps)
Class 1	5 Mbps	5 Mbps	5 Mbps	0.5 Mbps
Class 2	5 Mbps	5 Mbps	5 Mbps	0.5 Mbps

The actual bandwidth for each class should be 5 Mbps when the total bandwidth of the output interface is more than 10 Mbps. But it is impossible to reserve 5 Mbps when the total bandwidth of the output interface is just 1 Mbps. According to the characteristics of

WRR, the actual bandwidth for each class should be 0.5 Mbps. The conclusions are the actual bandwidth will be equal to the reserved bandwidth if the total bandwidth of the output interface is enough, and the actual bandwidth will be decreased in proportion to the total bandwidth of the output interface in the contrast condition. And the behavior is the same as PRR when the actual bandwidth is less than the required bandwidth.

Work-conserving means that the transmission is kept on going. When the work-serving is enabled, the unused bandwidth will be allotted to the classes, which have packets in queue, from the class with high priority to low priority. The work-conserving makes the bandwidth efficient.

CI commands

The basic syntax of command interface (CI) to configure bandwidth management is described below:

```
bm interface if_name enable/disable [wrr/prr] [efficient] [bandwidth bps]
bm class if_name add/del/mod class [name class_name] [priority X] [borrow on/off]
[bandwidth bps]
bm filter if_name add/del class dst_addr [mask xx] dst_port src_addr [mask xx] src_port
proto
bm show interface/class/filter/statistics if_name
bm config save/load/clear
bm monitor if_name [class_name]
```

For example, the configuration to construct the architecture of figure 1 is as follow:

```
bm interface LAN/WLAN/MPOA enable bandwidth 100m

bm class LAN/WLAN/MPOA add 1 name agencyA bandwidth 30m
bm class LAN/WLAN/MPOA add 1.1 name TA1_class bandwidth 10m
bm class LAN/WLAN/MPOA add 1.2 name TA2_class bandwidth 20m

bm class LAN/WLAN/MPOA add 2 name agencyB bandwidth 70m
bm class LAN/WLAN/MPOA add 2.1 name TB1_class bandwidth 30m
bm class LAN/WLAN/MPOA add 2.2 name TB2_class bandwidth 40m

bm filter LAN/WLAN/MPOA add 1.1 0 0 0 20 6
bm filter LAN/WLAN/MPOA add 1.2 0 0 0 30 6
bm filter LAN/WLAN/MPOA add 2.1 0 0 0 40 6
bm filter LAN/WLAN/MPOA add 2.2 0 0 0 50 6
```

In the configuration, the output rate of interface LAN/WLAN/MPOA is set 100Mbps. The first level classes, 1 (named agencyA) and 2 (named agencyB), get 30Mbps and 70Mbps. The leaf classes, 1.1 (named TA1_class), 1.2 (named TA2_class), 2.1 (named TB1_class) and 2.2 (named TB2_class), get 10Mbps, 20Mbps 30Mbps and 40Mbps. The four filters

classify packets into different classes by protocol type and source port. For example, the filter of class 1.1 classifies a packet into class 1.1 if the packet's protocol type is TCP and source port is 20.

Annex A CI Command List

Command Class List Table		
System Related Command	Exit Command	Ethernet Related Command
IP Related Command	Bridge Related Command	WAN Related Command
WLAN Related Command	Radius Related Command	802.1x Related Command
Bandwidth Management	Firewall Related Command	IPSec Related Command

System Related Command

[Home](#)

Command		Description
sys		
	adjtime	retrive date and time from Internet
	cbuf	
	display	[a f u]
	cnt	display cbuf a: all f: free u: used
		cbuf static
		display cbuf static
		clear cbuf static
	baud	<1..5>
	callhist	
	add	<phone dir [rate] [uptime]>
	display	
	remove	<index>
	clear	
	clock	
	display	display system clock
	countrycode	[countrycode]
	date	[year month date]
	dir	display file directory
	domainname	display domain name
	edit	<filename>
	enhanced	return OK if commands are supported for PWC purposes
	errctl	[level]
		set the error control level 0:crash no save,not in debug mode (default) 1:crash no save,in debug mode 2:crash save,not in debug mode 3:crash save,in debug mode
	event	
	display	display tag flags information
	trace	display system event information
		display
		clear <num>
	extraphnum	
	add	<set 1-3> <1st phone num> [2nd phone num]
	display	display extra phone numbers
	node	<num>
		set all extend phone number to remote node <num>
	remove	<set 1-3>
	reset	remove extra phone numbers
		reset flag and mask
	feature	display feature bit
	fid	

ZyXEL Confidential

	display		display function id list
firmware			display ISDN firmware type
hostname		[hostname]	display system hostname
iface			
	disp	[#]	display iface list
isr		[all used free]	display interrupt service routine
interrupt			display interrupt status
log			
	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
		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		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
	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
map			display whole memory map content
mbuf			

ZyXEL Confidential

	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]	
memory		<address> <length>	display memory content
memwrite		<address> <len> [data list ...]	write some data to memory at <address>
memwl		<address>	write long word to memory at <address>
memrl		<address>	read long word at <address>
memutil			
	usage		display memory allocate and heap status
	mqueue	<address> <len>	display memory queues
	mcell	mid [f u]	display memory cells by given ID
	msecs	[a f u]	display memory sections
	mtstart	<n-mcell>	start memory test
	mtstop		stop memory test
	mtalloc	<size> [n-mcell]	allocate memory for testing
	mtfree	<start-idx> [end-idx]	free the test memory
model			display server model name
proc			
	display		display all process information
	stack	[tag]	display process's stack by a give TAG
	pstatus		display process's status by a give TAG
pwc			sends information to PWC via telnet
queue			
	display	[a f u] [start#] [end#]	display queue by given status and range numbers
	ndisp	[qid]	display a queue by a given number
quit			quit CI command mode
reboot		[code]	reboot system code = 0 cold boot, = 1 immediately boot = 2 bootModule debug mode
reslog			
	disp		display resources trace
	clear		clear resources trace
stdio		[second]	change terminal timeout value
time		[hour [min [sec]]]	display/set system time
timer			
	disp		display timer cell
	trace	[on off]	set/display timer information online
	start	[tmvalue]	start a timer
	stop	<id>	stop a timer
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

ZyXEL Confidential

	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, fir0 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
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
	dead		let watch dog take place using while loop
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
spt			
	dump		dump spt raw data
		root	dump spt root data
		rn	dump spt remote node data
		user	dump spt user data
		slot	dump spt slot data
	set	<offset> <len> <value...>	set spt value in memory address
	save		save spt data
	size		display spt record size
	clear		clear spt data
cmgr			
	trace		
		disp <ch-name>	show the connection trace of this channel
		clear <ch-name>	clear the connection trace of this channel
	data	<ch-name>	show channel connection related data
	cnt	<ch-name>	show channel connection related counter
socket			display system socket information
filter			

ZyXEL Confidential

		clear		clear filter statistic counter
		disp		display filter statistic counters
		sw	[on/off]	set filter status switch
		rule	<iface>	display iface filter flag
		set	<set>	display filter rule
		addnetbios		add netbios filter
		removenetbios		remove netbios filter
		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
		blockbc	[on/off]	set/display broadcast filter mode
	ddns			
		debug	<level>	enable/disable ddns service
		display	<iface name>	display ddns information
		restart	<iface name>	restart ddns
		logout	<iface name>	logout ddns
	cpu			
		display		display CPU utilization

Exit Command

[Home](#)

Command		Description
exit		exit smt menu

Ethernet Related Command

[Home](#)

Command		Description
ether		
	config	display LAN configuration information
	driver	
	cnt	
		disp <name>
		clear <name>
	iface	<ch name> <num>
	ioctl	<ch name>
	mac	<ch name> <mac addr>
	reg	<ch name>
	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>
	init	<ch name>
	version	see ethernet device type
	pkttest	
	disp	
		packet <level>
		event <ch> [on/off]
	sap	[ch name]
	arp	<ch name> <ip-addr>
	mem	<addr> <data> [type]
test		<ch_id> <test_id> [arg3] [arg4]
		do LAN test

pncconfig		<ch_name>	do pnc config
mac		<src_ch> <dest_ch> <ipaddr>	fake mac address

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
	add	<hostid> ether <ether addr>	add arp information
	resolve	<hostid>	resolve ip-addr
	replydif	[<0:no 1:yes>]	reply different inteface ip-addr's arp request
	drop	<hostid> [hardware]	drop arp
	flush		flush arp table
	publish		add proxy arp
	dhcp	<iface>	
	client		
		release	release DHCP client IP
		renew	renew DHCP client IP
	mode	<server relay none client>	set dhcp mode
	relay	server <serverip>	set dicip relay server ip-addr
	reset		reset dhcp table
	server		
		probecount <num>	set dhcp probe count
		dnsserver <ip1> [ip2] [ip3]	set dns server ip-addr
		winsserver <winsip1> [<winsip2>]	set wins server ip-addr
		gateway <gatewayip>	set gateway
		hostname <hostname>	set hostname
		initialize	fills in DHCP parameters and initializes (for PWC purposes)
		leasetime <period>	set dhcp leasetime
		netmask <netmask>	set dhcp netmask
		pool <startip> <numip>	set dhcp ip pool
		renewaltime <period>	set dhcp renew time
		rebindtime <period>	set dhcp rebind time
		reset	reset dhcp table
		server <serverip>	set dhcp server ip for relay
		dnsorder [router isp]	set dhcp dns order
	status	[option]	show dhcp status
	static		
		delete <num> all	delete static dhcp mac table
		display	display static dhcp mac table
		update <num> <mac> <ip>	update static dhcp mac table
	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
	server	<primary> [secondary] [third]	set dns server

		stats		
			clear	clear dns statistics
			disp	display dns statistics
		table		display dns table
httpd				
		debug	[on off]	set http debug flag
icmp				
		echo	[on off]	set icmp echo response flag
		data	<option>	select general data type
		check		
			cmd [on off]	check icmp echo reply command data
			rsp [on off]	check icmp response
			indication [i r l p]	set icmp indication
		status		display icmp statistic counter
		trace	[on off]	turn on/off trace for debugging
		discovery	<iface> [on off]	set icmp router discovery flag
ifconfig			[iface] [ipaddr] [broadcast <addr> mtu <value> dynamic]	configure network interface
ifdrop			<iface>	check if iface is available.
ping			<hostid>	ping remote host
pong			<hostid> [<size> <time-interval>]	pong 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
		flush		flush route table
		lookup	<addr>	find a route to the destination
		errcnt		
			disp	display routing statistic counters
			clear	clear routing statistic counters
status				display ip statistic counters
adjtcp			<iface> [<mss>]	adjust the TCP mss of iface
udp				
		status		display udp status
rip				
		accept	<gateway>	drop an entry from the RIP refuse list
		activate		enable rip
		merge	[on off]	set RIP merge flag
		refuse	<gateway>	add an entry to the rip refuse list
		request	<addr> [port]	send rip request to some address and port
		reverse	[on off]	RIP Poisoned Reverse
		status		display rip statistic counters
		trace		enable debug rip trace
		mode		
			<iface> in [mode]	set rip in mode
			<iface> out [mode]	set rip out mode
		dialin_user	[show in out both none]	show dialin user rip direction
tcp				
		ceiling	[value]	TCP maximum round trip time

	floor	[value]	TCP minimum rtt
	irtt	[value]	TCP default init rtt
	kick	<tcb>	kick tcb
	limit	[value]	set tcp output window limit
	max-incomplete	[number]	Set the maximum number of TCP incomplete connection.
	mss	[value]	TCP input MSS
	reset	<tcb>	reset tcb
	rtt	<tcb> <value>	set round trip time for tcb
	status	[tcbl] [<interval>]	display TCP statistic counters
	syndata	[on off]	TCP syndata piggyback
	trace	[on off]	turn on/off trace for debugging
	window	[tcbl]	TCP input window size
samenet		<iface1> [<iface2>]	display the ifaces that in the same net
uninet		<iface>	set the iface to uninet
tftp			
	support		prtn if tftp is support
	stats		display tftp status
xparent			
	join	<iface1> [<iface2>]	join iface2 to iface1 group
	break	<iface>	break iface to leave ipxparent group
anitprobe		<0 1> 1:yes 0:no	set ip anti-probe 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			
	clear		clear ip pr table counter information
	disp		dump ip pr table counter information
	switch		turn on/off ip pr table counter flag
nat			
	debug	[on off]	turn on/off the nat debug flag
	period	[period]	set nat timer period
	port	[port]	set nat starting external port number
	checkport		verify all server tables are valid
	timeout		
		gre [timeout]	set nat gre timeout value
		iamt [timeout]	set nat iamt timeout value
		generic [timeout]	set nat generic timeout value
		reset [timeout]	set nat reset timeout value
		tcp [timeout]	set nat tcp timeout value

		tepoother [timeout]	set nat tcp other timeout value
		update	create nat system information from spSysParam
		iamt	display nat iamt information
		iface	<iface> show nat status of an interface
		lookup	<rule set> display nat lookup rule
		new-lookup	<rule set> display new nat lookup rule
		loopback	[on off] turn on/off nat loopback flag
		reset	<iface> reset nat table of an iface
		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
		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

Bridge Related Command

[Home](#)

Command		Description
bridge		
	mode	<1/0> (enable/disable) turn on/off (1/0) LAN promiscuous mode
	blt	related to bridge local table
	disp	<channel> display blt data
	reset	<channel> reset blt data
	traffic	display local LAN traffic table
	monitor	[on off] turn on/off traffic monitor. Default is off.
	time	<sec> set blt re-init interval
	brt	related to bridge route table
	disp	[id] display brt data
	reset	[id] reset brt data
	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
	disp	display bridge source table

WAN Related Command

[Home](#)

Command		Description	
wan	adsl	bert	ADSL ber
		chandata	ADSL channel data, line rate
		close	Close ADSL line
		coding	ADSL standard current
		ctrlent	ADSL CTRLLE response command

ZyXEL Confidential

		defbitmap		ADSL defect bitmap status
		dyinggasp		Send ADSL dyinggasp
		fwav		Test the ADSL F/W available ping
		fwdl		Download modem code, but must reset first
		linedata		
		linedata	near	Show ADSL near end noise margin
		linedata	far	Show ADSL far end noise margin
		open		Open ADSL line
		opencmd		Open ADSL line with specific standard
		opmode		Show the operational mode
		perfddata		Show performance information,CRC,FEC, error seconds..
		rdata	[start] [length]	Read DSP CTRL registers 512 bytes
		reset		Reset ADSL modem, and must reload the modem code again
		selftest		
		selftest	long	ADSL long loop test
		selftest	short	ADSL short loop test
		status		ADSL status (ex: up, down or wait for init)
		version		ADSL version information
		vendorid		ADSL vendor information
		utopia		Show ADSL utopia information
		cellcnt		Show ADSL cell counter
		display		
		display	shutdown	Show the counter of rate adaptive mechanism happening
		display	rateup	Show real status that rate adaptive mechanism happened
		rateadap	[on/off]	Turn on/off rate adaptive mechanism
		dumpcondition	[on/off]	Turn on/off online debug information of rate adaptive mechanism
		sampletime	[mins]	Tune the sample time of rate adaptive mechanism
		noisegt	[db]	if noise margin is 3db greater than before, and rate is worse than before, then system will do “L1 shutdown RA3”, default is 3db
		noisemargin	[db]	if noise margin is greater than this value, and rate is worse than before, then system will do “L1 shutdown RA3”, default is 8db
		persisttime	[time]	when the adaptive condition is matched system will continue to monitor the time period “persisttime” before doing “L1 shutdown RA3”, default is 30 seconds
		timeinterval	[mins]	when “L1 shutdown RA3” is done twice, and still can’t reach the max rate which system recorded, it will delay a time period that the period base time is”timeinterval” before starting again. The time-based default is 2 hrs
		defectcheck	[on/off]	Turn on/off detect table checking, default is on
		txgain	[value]	Set the CTRL register (0xc3), the value is from 0xfa to 0x06
		targetnoise	[value]	Set the CTRL register (0xc4), the value is from 0xfa to 0x06
		maxtonelimit	[value]	Set the CTRL register (0xc5), the value is from 0xfa to 0x06

ZyXEL Confidential

		rxgain	[value]	Set the CTRL register (0xc6), the value is from 0xfa to 0x06
		txoutputpwr	[value]	Set the CTRL register (0xc7), the value is from 0xfa to 0x06
		rxoutputpwr	[value]	Set the CTRL register (0xc8), the value is from 0xfa to 0x06
		maxoutputpwr	[value]	Set the CTRL register (0xc9), the value is from 0xfa to 0x06
		errorsecond		
		errorsecond	switch [1 0]	Turn on/off error sending to DSLAM side
		errorsecond	sendes	Send current error second information immediately
		dygasprecover		
		dygasprecover	level [value]	By default is 100, after receiving 100 dying gasp system will reboot
		dygasprecover	active [on off]	Turn on/off this mechanism
		rsploss	[1 0]	Turn on means to response signal loss of CTRL immediately, default is off
		watchdog	[1 0]	Watchdog for DSP
	atm	test	[fix rand period oam loopback]	Generate ATM traffic
wan	hwsar	disp		Display hwsar packets incoming/outgoing information
		clear		Clear hwsar packets information
		sendoam		Send OAM packets: <vpi> <vci> <f5> <end-to-end> <type:0(AIS) 1(RDI) 2(LoopBack)>

WLAN Related Command

[Home](#)

		Command		Description
wlan				
	ssid			Configure ESSID
	chid			Configure channel ID
	debug			Turn on /off debug information
	version			Show WLAN AP F/W version
	filter	< incoming outgoing >	< generic > [set#1][set#2][set#3][set#4]	To set generic filter for wireless channel

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

Bandwidth management Related Command

[Home](#)

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 pr>	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
		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 pr>	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
		mpona[00~07]	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 pr>	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
	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.
		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.
		mpos[00~07]	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.
	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.
		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.
		mpos[00~07]	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.
	show	interface	lan			Show the interface settings of LAN
			wlan			Show the interface settings of WLAN

			mpoa[0 0~07]		Show the interface settings of WAN
		class	lan		Show the classes settings of LAN
			wlan		Show the classes settings of WLAN
			mpoa[0 0~07]		Show the classes settings of WAN
		filter	lan		Show the filters settings of LAN
			wlan		Show the filters settings of WLAN
			mpoa[0 0~07]		Show the filters settings of WAN
		statistics	lan		Show the statistics of the classes in LAN
			wlan		Show the statistics of the classes in WLAN
			mpoa[0 0~07]		Show the statistics of the classes in WAN
	monitor	lan	<#>		Monitor the bandwidth of class # in LAN. If the class is not specific, all the classes in LAN 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.
		mpoa[00~ 07]	<#>		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.
	config	save			Save the configuration.
		load			Load the configuration.
		clear			Clear the configuration.

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
		tcprst	
		rst	Set TCP reset sending on/off.
		rst113	Set TCP reset sending for port 113 on/off.
		display	Display TCP reset sending setting.
		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

IPSec Related Command

[Home](#)

Command				Description
ipsec				
	debug	<1 0>		turn on/off trace for IPSec debug information
	ipsec_log_display			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.
		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.
	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 minutes - 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 15 minutes - 0 means never update
	updatePeerIP			Force system to update IPSec rules which use domain name as the secure gateway IP right away.
	dial	<rule #>		Initiate IPSec rule <#>
	display	<rule #>		Display IPSec rule #
	keep_alive	<rule #>	<on off>	Set ipsec keep_alive flag
	load	<rule #>		Load ipsec rule
	save			Save ipsec rules

ZyXEL Confidential

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
	keyAlive	<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 antireplay 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 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

ZyXEL Confidential

			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
	swSkipOverlapIp		<on off>	<ul style="list-style-type: none">- 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>	<ul style="list-style-type: none">- 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.