ZyXEL

Firmware Release Note

Prestige 202H

Standard version

Release 3.40(NV.2)C0

Date: **Oct. 9 2003**
Author: **June Lee**

ZyXEL Prestige 202H Standard Version release 3.40(NV.2)C0 Release Note

Date: Oct. 9, 2003

Supported Platforms:

ZyXEL P202H

Versions:

ZyNOS F/W Version : V3.40(NV.2) | 10/9/2003 17:10:06
BootBase : V2.09 | 9/6/2002 16:06:05

Notes:

The P202H, is 3rd generation of ZyXEL ISDN product family. It is a ISDN router for small/medium office to have Internet access and LAN-to-LAN application through ISDN connection over the ISDN line.

Known Issues:

1. Remote management feature can be configured via SMT only.
2. Firmware upgrade from eWC via WAN side does not work.
3. P202H does not update "Time and Date Setting" automatically.
4. If using Linux to access device via telnet and staying in menu 24.1 for a few hours, P202H will reboot.

Features:

Modifications in V 3.40(NV.2) | 10/09/2003

1. Change to FCS version.

Modifications in V 3.40(NV.2)b1 | 10/07/2003

1. [BUG FIXED]
   Symptom: Device makes unwanted calls due to DNS query mechanism in VPN feature.
   Condition: Device makes unwanted calls due to DNS query mechanism in VPN feature when users set security gateway by domain name type.
2. [FEATURE ENHANCED]
   Make protection for users not to configure idle timeout larger than the VPN update peer IP time.

3. [FEATURE ENHANCED]
   Support “sys romreset” CI command to replace “sys spt default” CI command.
4. [FEATURE ENHANCED]
   Support “ATLD” command.
5. [BUG FIXED]
   Symptom: Configure two connections with SUA to the menu 11 and second remote node doesn't work.
   Condition: Configure two connections with SUA to the menu 11 and second remote node doesn't work. The connection is up correctly, but there is no traffic.
6. [BUG FIXED]
   Symptom: Showing “POTS log” in smt 24.3.2, which is not illegal.
   Condition: Showing “POTS log” in smt 24.3.2, which is not illegal.
7. [FEATURE ENHANCED]
   Add Netbios filters setting in menu 3.1 and 11.5 by default.

Modifications in V 3.40(NV.1) | 08/20/2003

2. Change to FCS version.

Modifications in V 3.40(NV.1)b2 | 08/08/2003

1. [FEATURE ENHANCED]
   Support DDNS feature.
2. [FEATURE ENHANCED]
   Support time server feature.

Modifications in V 3.40(NV.1)b1 | 07/04/2003

1. [FEATURE ENHANCED]
   Integrate web help pages.
2. [FEATURE ENHANCED]
   Merge remote management feature.

Modifications in V 3.40(NV.0) | 06/17/2003

3. Change to FCS version.

Modifications in V 3.40(NV.0)b2 | 05/27/2003

1. [FEATURE ENHANCED]
   Integrate Web GUI.
2. [FEATURE ENHANCED]
   Merge Phase III VPN feature.

Modifications in V 3.40(NV.0)b1 | 04/18/2003

1. [FEATURE CHANGED]
   Porting P202H for OBM from P202H for DT (with source code 3.40(IJ.0)b5)

Annex A CI Command List

Command Class List Table		
System Related Command	Exit Command	Ethernet Related Command
IP Related Command	IPSec Related Command	

System Related Command Home

Command				Description
sys				
	callhist			
		display		display call history
		remove	<index>	remove entry from call history
	countrycode		[countrycode]	set country code
	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
	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		
			triangle	set if firewall ignore triangle route in lan/wan/dmz/wlan
	hostname		[hostname]	display system hostname
	log			
		clear		clear log error
		disp		display log error
		online	[on|off]	turn on/off error log online display
	stdio		[second]	change terminal timeout value

	trcdisp			monitor packets
	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
	atsh			display MRD field
	socket			display system socket information
	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
	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>	display ether driver counters
		status	<ch_name>	see LAN status
	version			see ethernet device type

IP Related Command Home

Command				Description
ip				
	address		[addr]	display host ip address
	alias		<iface>	alias iface
	aliasdis		<0|1>	disable alias
	arp			
		status	<iface>	display ip arp status
	dhcp		<iface>	
		client		
			release	release DHCP client IP
			renew	renew DHCP client IP
		mode	<server|relay|none|client>	set dhcp mode

		relay	server <serverIP>	set dicp 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			
		stats		
			clear	clear dns statistics
			disp	display dns statistics
	icmp			
		status		display icmp statistic counter
		discovery	<iface> [on|off]	set icmp router discovery flag
	ifconfig		[iface] [ipaddr] [broadcast <addr> |mtu <value>|dynamic]	configure network interface
	ping		<hostid>	ping remote host
	route			
		status	[if]	display routing table
		add	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add route
		addiface	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add an entry to the routing table to iface
		addprivate	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add private route
	status			display ip statistic counters
	udp			
		status		display udp status
	tcp			
		status	[tcb] [<interval>]	display TCP statistic counters
	xparent			
		join	<iface1> [<iface2>]	join iface2 to iface1 group
		break	<iface>	break iface to leave ipxparent group

IPSecRelated Command Home

Command				Description
ipsec				

	debug	<1|0>		turn on|off trace for IPsec debug information
	ipsec_log_disp			show IPSec log, same as menu 27.3
	route	lan	<on|off>	After a packet is IPSec processed and will be sent to LAN side, this switch is to control if this packet can be applied IPSec again.
				Remark: Command available since 3.50(WA.3)
		wan	<on|off>	After a packet is IPSec processed and will be sent to WAN side, this switch is to control if this packet can be applied IPSec again.
				Remark: Command available since 3.50(WA.3)
	show_runtime	sa		display runtime phase 1 and phase 2 SA information
		spd		When a dynamic rule accepts a request and a tunnel is established, a runtime SPD is created according to peer local IP address. This command is to show these runtime SPD.
	switch	<on|off>		As long as there exists one active IPSec rule, all packets will run into IPSec process to check SPD. This switch is to control if a packet should do this. If it is turned on, even there exists active IPSec rules, packets will not run IPSec process.
	timer	chk_my_ip	<1~3600>	- Adjust timer to check if WAN IP in menu is changed
				- Interval is in seconds
				- Default is 10 seconds
				- 0 is not a valid value
		chk_conn.	<0~255>	- Adjust auto-timer to check if any IPsec connection has no traffic for certain period. If yes, system will disconnect it.
				- Interval is in minutes
				- Default is 2 minuets
				- 0 means never timeout
		update_peer	<0~255>	- Adjust auto-timer to update IPSec rules which use domain name as the secure gateway IP.
				- Interval is in minutes
				- Default is 30 minutes
				- 0 means never update
				Remark: Command available since 3.50(WA.3)
	updatePeerIp			Force system to update IPSec rules which use domain name as the secure gateway IP right away.
				Remark: Command available since 3.50(WA.3)
	dial	<rule #>		Initiate IPSec rule <#> from ZyWALL box
				Remark: Command available since 3.50(WA.3)
	display	<rule #>		Display IPSec rule #