ZyXEL

Firmware Release Note

Prestige 314 PLUS

Release 3.60(CX.1)c0

Date: Oct 28, 2002

Author: Gilbert Cheng

Prestige 314 PLUS Standard Version
release 3.60(CX.1)c0
Release Note

Date: Oct 28, 2002

Supported Platforms:

Prestige 314 PLUS

Versions:

ZyNOS Version : V3.60(CX.1) | 10/28/2002 13:32:40
Bootbase Version : V2.10 | 03/22/2002 14:38:58

Notes:

1. Click here to check CI command lists

Known Issues:

1. Port Status is not support for this firmware (Hardware limitation).
2. Viewing the LOG via CI command might cause system to crash.

Features:

Modifications in V 3.60(CX.1)c0 | 10/28/2002
1.[BUG FIX]
Symptom: Can not access help page in Upnp page.
Condition: Web configurator, the user can not access help page in Upnp page.
2.[BUG FIX]
Symptom: WAN Web page wording error.
Condition: The WAN web page have unnecessary option for "WAN to DMZ " setting of netbios filter.
3.[ENHANCEMENT]If the user setting use Time server to NONE and save, then change it to Daytime, Time or NTP, the Time Server IP Address is emptied. It should be restore default setting (time-b.nist.gov).
4.[BUG FIX]
Symptom: ARP table overflow.
Condition: If the user configure the WAN encapsulation type as PPPOE, the P314PLUS still learn the ARP from "enif1" interface.
5.[BUG FIX]
Symptom: ARP table overflow.
Condition: The router will learn the ARP from different network segment from WAN port.
6[BUG FIX]
Symptom: Device filter did not work.
Condition: When the user apply any device filter in the SMT menu 3.1 or SMT menu 11.5, these filters do not work.

Modifications in V 3.60(CX.0)c0 | 10/15/2002

1.First release.

2.[NEW FEATURE] Support UPNP. For more information, please refer Appendix 1.

3.[NEW FEATURE] Add traffic redirection. For more information, please refer to Appendix 2.

4.[NEW FEATURE] Add NetBIOS over TCP/IP (NBT) packet filter function. Please remove filter setting in SMT menu 21, SMT menu 3.1, and SMT menu 11.5 as necessary. Please refer to Appendix 4 for detailed information.

5. [NEW FEATURE]Add Centralize Log, for more infotmation, please refer to Appendix 5.

6. [ENHANCEMENT] DDNS enhancement to prevent update with private IP address, please refer to Appendix 6.

Appendix 1 UPnP

1. **What is UPnP:** Universal Plug and Play(UPnP) is an architecture for pervasive peer-to-peer network connectively of PCs and intelligent devices or appliances, particularly within the home. UPnP builds on Internet standards and technologies, such as TCP/IP, HTTP, and XML, to enable these devices to automatically connect with one another and work together to make networking- particularly home networking- possible for more people.
2. **Discovery:** Once devices are attached to the network and addressed appropriately, discovery can take place. If you attach your router to the Windows XP or Me then you can find your device in Network Place.
3. **NAT Traversal:** Put simply: NAT can "break" many of the compelling new PC and home networking experiences, such as multiplayer games, real time communications, and other peer-to-peer services, that people increasingly want to use in their homes or small businesses. These applications will break if they use private address on the public Internet or simultaneous use of the same port number. Application must use a public address and for each session a unique port number. Large organizations have professional IT staff on hand to ensure their corporate applications can work with NAT, but smaller organizations and consumers do not have this luxury. UPnP NAT Traversal can automatically solve many of the problems the NAT imposes on applications, making this an ideal solution for small businesses and consumers.

Appendix 2 Traffic Redirect

1. Introduction

These features is used to keep Internet connectivity of the P314. The Connectivity Monitor is running at interval to detect if the P314 can reach a desired host/address or the adjacent upstream gateway. Once the P314 has detected the connectivity is broken, it tries to forward the traffic to another gateway that user has specified.

2. Menu 11.6 - Traffic Redirect Setup

```
   Menu 11.1 - Remote Node Profile  Rem Node Name= Normal_route
Route= IP Active= Yes  Encapsulation= Ethernet       Edit IP= No
Service Type= Standard       Session Options: Service Name= N/A
Edit Filter Sets= No Outgoing:  My Login= N/A              Edit
Traffic Redirect= YES  My Password= N/A   Server IP= N/A  Press
ENTER to Confirm or ESC to Cancel:
```

```
 Menu 11.6 - Traffic Redirect Setup  Active= No Configuration:
Backup Gateway IP Address= 0.0.0.0   Metric= 2   Check WAN IP
Address= 0.0.0.0     Fail Tolerance= 0     Period(sec)= 0
Timeout(sec)= 0  Press ENTER to Confirm or ESC to Cancel:
```

1) Configure "Active" to "YES" if you want this feature work.

(1) "Backup Gateway". When the primary ISP or the check point is unreachable, traffic will be handed over to this backup gateway. [In IP address format]

(2) "Metric". Please reference section "**Metric**"

(3) "Check WAN IP Address". The Connectivity Monitor will probe the connectivity to a check-point. In general case, this check-point is the adjacent upstream gateway, which is typically assigned by ISP. However, if user desires to check a more significant point on the Internet, it can be specified here. A special case should be noticed that, even the ISP is online, this check-point maybe not reachable. The hand-over mechanism will function when the check-point failed. Leave it to 0.0.0.0, and the P314 will take the upstream gateway as the default check-point.

(4) "Fail Tolerance" is the check failure upper limit. For example, if this value is 2. When P314 failed to reach the check-point at the 3rd try, Connectivity Monitor will invalidate the corresponding route and promote candidate to be the default route.

(5) "Period". The Connectivity Monitor will examine physical link signal and then probe the check-point at a interval of "period" seconds.

(6) "Timeout". The check-point is expected to response P314's probe within a reasonable time. After that, P314 will log a failure. When the fail tolerance is exceeded, traffic will be handed over to the candidate route.

The probing mechanism employs ICMP echo request/reply. Some hosts or routers on Internet may discard such packets.

3. Metric

Once the traffic redirect and dial-backup mechanism were activated, P314 will have 3 default routes to Internet. The first one is the normal route that designated by ISP or the static route mechanism; the second one is the traffic-redirect route (i.e. the backup gateway); the third one is the dial-backup route.

Customable metrics are provided in the menu 11.6 (Traffic Redirect) and menu 11.3 (Dial-backup) to determine the priority of the 3 default routes. For example, if the normal route has a metric "1" and traffic-redirect route has a metric "2" and dial-backup route has a metric "3", then the normal route is the first priority candidate to be the primary default route. If the normal route failed to get on Internet, the traffic-redirect route will be the successor. By the same theorem, dial-backup route is the successor after traffic-redirect route failed. For any two of the default routes match the same metric, a pre-defined priority is taken:

Normal route > Traffic-redirect route

For another example, if user want P314 to use dial-backup route prior than traffic-redirect route or even the normal route, all need to do is to make metric of dial-backup route to be "1" and the others to be equal to "2" (or greater).

4. C/I commands

A set of C/I commands are provided.

(1) "ip tredir active [on/off]" to enable/disable traffic redirect.
(2) "ip tredir partner" IP address of the backup gateway.
(3) "ip tredir target" IP address of the check target.
(4) "ip tredir failcount" to setup fail tolerance.
(5) "ip tredir checktime" to setup checking period.
(6) "ip tredir timeout" to setup check timeout.
(7) "ip tredir disp" to show system value and run time value.
(8) "ip tredir save" will save the configuration.

5.Note

(1) Turn off "RIP" in SMT3.2 is recommended.
(2) When traffic redirect is turned on, and encapsulation type is PPPOE or PPTP, "Nail-UP" function in SMT11.1 will be enabled
(3) A useful WINDOWS commands "tracert" can be used to verify the packet routing.
(4) Connectivity Monitor can not be disabled. However, traffic redirect and dial-backup mechanism can be enabled/disabled independently.

Appendix 3 SUA Support Table

The required settings of Menu 15 for some applications are listed in the following table.

SUA Support Table

Traffic Type	**Application Version**	**Required Settings in Menu 15 Port/IP**	
		Outgoing Connection	**Incoming Connection**
HTTP	Netscape, IE	None	80/client IP
FTP	Windows FTP, Cuteftp	None	21/client IP
TELNET	Windows Telnet, Neterm	None	23/client IP (and remove Telnet filter in WAN port)
POP3	Eudora	None	110/clinet IP
SMTP	Eudora	None	25/client IP
IRC	mIRC,Microsoft Chat	None for Chat. DCC support: MIRC < 5.31	None
PPTP	Windows PPTP	None	1723/client IP
ICQ	ICQ 99a	None for Chat. For file transfer, we must enable ICQ-preference-connections-firewall and set the firewall time out to 80 seconds in firewall setting.	Default/client IP
Cu-SeeMe	Cornell 1.1	None	7648/client IP
	White Pine 3.1.2	7648/client IP & 24032/client IP	Default/client IP
	White Pine 4.0 (CuSeeMe Pro)	7648/client IP & 24032/client IP	Default/client IP
NetMeeting	Microsoft NetMeeting 2.1 & 2.11	None	1720/client IP 1503/client IP
Cisco IP/TV	Cisco IP/TV 2.0.0	Default/client IP	
RealPlayer	RealPlayer G2	None	
VDOLive		None	
Quake	Quake1.06	None	Default/client IP
QuakeII	QuakeII2.30	None	Default/client IP
QuakeIII	QuakeIII1.05beta	None	
StartCraft		6112/client IP	
Quick Time	Quick Time 4.0	None	
IPSEC (ESP)		None (only one client)	Default
MSNP	Microsoft Messenger service V4.6	None	None

Appendix 4 Hard-coded packet filter for "NetBIOS over TCP/IP" (NBT)

The new set C/I commands is under "sys filter netbios" sub-command.

There are two CI commands:
(1) "sys filter netbios disp": It will display the current filter mode.

Example ouput:
```
================ NetBIOS Filter Status ================
        LAN to WAN:         Forward
        WAN to LAN:         Forward
        IPSec Packets:      Forward
        Trigger Dial:       Disabled
```

(2) "sys filter netbios config <type> {on|off}": To configure the filter mode for each type.
Current filter types and their description are:

Type	Description	Default mode
0	LAN to WAN	Forward
1	WAN to LAN	Forward
6	IPSec pass through	Forward
7	Trigger dial	Disabled

Example commands:
sys filter netbios config 0 on => block LAN to WAN NBT packets
sys filter netbios config 1 off => pass LAN to DMZ NBT packets
sys filter netbios config 6 on => block IPSec NBT packets
sys filter netbios config 7 off => disable trigger dail

Appendix 5 Centralize Log

1. Introduction:

In the past our system existed two email functions in content filter and firewall, it's unnecessary and surplus. We must integrate these functions to the centralized mail system. And the error log, sys log, content filter log, firewall log and IPSec log, we can integrate all these logs to the centralized log and support the sort and display by different category functions. We will provide the centralized management for log in all products.

2. Policy:

I. Integrate content filter email and firewall email.
II. Integrate error log, sys log, content filter log, firewall log and IPSec log.
III. Unify log format for various rule.
IV. Send all logs to the sys log server.

3. CI commands:

sys 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
		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				
		disp			display log error
		clear			clear log error
		online		[on|off]	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
			hour	[0-23]	hour time to send the logs
			minute	[0-59]	minute time to send the logs
			policy	[0:full/1:hourly/2:daily/3:weekly/4:none]	mail schedule policy
			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

Appendix 6 New DDNS Enhancement

Introduction

This enhacement provides solutions to presevent the embedded DDNS client of the Prestige update router's WAN IP address with a private IP address. Currently, the prestige DDNS embedded client will provide the router's WAN port ip address to DDNS server, but it may be a private IP address, it is not a leagel update IP address. Figure 1 is an example of this case. The router should provide functions to update the DDNS with public IP address. And the router need to handle the multiple error return code from the server in multi-host update case

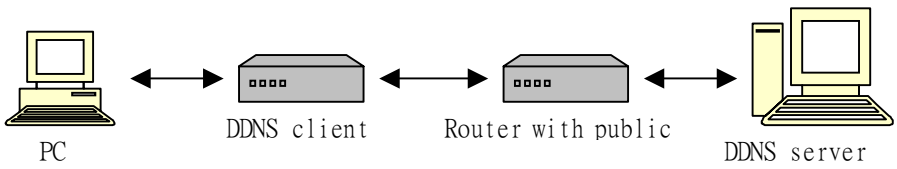

Figure 1

Extermal Spec

What to do

To prevent the DDNS client from providing the DDNS server with private IP address. This enhancement support 2 functions:

1. User specify the public address by himself.
2. Use the server detected public address.

SMT menu

```
                    Menu 1.1 - Configure Dynamic DNS
Service Provider= WWW.DynDNS.ORG
Active= Yes
DDNSType= DynamicDNS
Host1=
Host2=
Host3=
USER=
Password= ********
Enable Wildcard= No
Offline= N/A
Edit Update IP Address:
  Use Server Detected IP= Yes
  User Specified IP Addr= N/A
  IP Addr= N/A
```

Annex A CI Commands

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

System Related Command

Home

Command				Description
Sys				
	adjtime			retrive date and time from Internet
			display	display cbuf static
	callhist			
		display		display call history
		remove	<index>	remove entry from call history
	country code		[countrycode]	set country code
	date		[year month date]	set/display date
	domain name			display domain name
	edit		<filename>	edit a text file
	extraph num			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
	hostna me		[hostname]	display system hostname
	logs			
		category		
			access [0:none/1:log]	record the access control logs
			display	display the category setting
			error [0:none/1:log/2:alert/3:both]	record and alert the system error 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
	rn			
		load	<entry no.>	load remote node information
		disp	<entry no.>(0:working buffer)	display remote node information
		nat	<none|sua|full_feature>	config remote node nat
		nailup	<no|yes>	config remote node nailup
		save	[entry no.]	save remote node information
	stdio		[second]	change terminal timeout value
	time		[hour [min [sec]]]	display/set system time
	trcdisp			monitor packets
	trclog			
	trcpacket			
	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
	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, 6:IPSec passthrough, 7:Trigger Dial> <on|off>	config netbios filter
	roadrunner			

		debug	<level>	enable/disable roadrunner service 0: diable <default> 1: enable
		display	<iface name>	display roadrunner information iface-name: enif0, wanif0
		restart	<iface name>	restart roadrunner
	ddns			
		debug	<level>	enable/disable ddns service
		display	<iface name>	display ddns information
		restart	<iface name>	restart ddns
		logout	<iface name>	logout ddns
	cpu			
		display		display CPU utilization

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
		ioctl	<ch_name>	Useless in this stage.
		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
		status		show dhcp status
	dns			
		query		

		server	<primary> [secondary] [third]	set dns server
		stats		
	httpd			
	icmp			
		status		display icmp statistic counter
		discovery	<iface> [on|off]	set icmp router discovery flag
	ifconfig		[iface] [ipaddr] [broadcast <addr> |mtu <value>|dynamic]	configure network interface
	ping		<hostid>	ping remote host
	route			
		status	[if]	display routing table
		add	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add route
		addiface	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add an entry to the routing table to iface
		addprivate	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add private route
		drop	<host addr> [/<bits>]	drop a route
	smtp			
	status			display ip statistic counters
	udp			
		status		display udp status
	rip			
	tcp			
		status	[tcb] [<interval>]	display TCP statistic counters
	tftp			
	xparent			
		join	<iface1> [<iface2>]	join iface2 to iface1 group
		break	<iface>	break iface to leave ipxparent group
	urlfilter			
		exemptZone		
			display	display exemptzone information
			actionFlags [type(1-3)][enable/disable]	set action flags
			add [ip1] [ip2]	add exempt range
			delete [ip1] [ip2]	delete exempt range
			clearAll	clear exemptzone information
		customize		
			display	display customize action flags
			actionFlags [act(1-6)][enable/disable]	set action flags
			logFlags [type(1-3)][enable/disable]	set log flags
			add [string] [trust/untrust/keyword]	add url string
			delete [string] [trust/untrust/keyword]	delete url string
			clearAll	clear all information
	tredir			
		failcount	<count>	set tredir failcount
		partner	<ipaddr>	set tredir partner
		target	<ipaddr>	set tredir target
		timeout	<timeout>	set tredir timeout

		checktime	<period>	set tredir checktime
		active	<on|off>	set tredir active
		save		save tredir information
		disp		display tredir information
		debug	<value>	set tredir debug value