ZyXEL

Firmware Release Note

Prestige 662HW-63/67

Standard Version

Release 3.40(SC.3)C0

Date: **Nov 30, 2005**
Author: **Vignette Zhang**

ZyXEL Prestige 662HW-63/67 Standard Version Release 3.40(SC.3)C0 Release Note

Date: Nov 30, 2005

Supported Platforms:

ZyXEL Prestige 662HW-63/67

Versions:

ZyNOS Version : V3.40(SC.3) | 11/30/2005 13:10:52
Bootbase Version : V1.06 | 04/01/2004 11:22:33

Notes:

The Prestige 662HW-63/67, 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. P662HW-63/67 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.
P662HW-63/67 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.

Known Issues:

1. US Robotics modem is not supported for dial backup
2. If user wants to register to extend expired date, packet-Scan engine won't send out expired date request until 6th checking with Packet-Scanning server.
3. If device LAN is connected with a switch, and device reboots, then the PC with Any-IP can't connect with device until ARP entry is cleared by PC.
4. WLAN has Beacon failure problem when the channel is in very busy/dirty condition
5. In Web/GUI, the MBM wizard successful page is English only.
6. L2TP can't pass through NAT(Use windows XP as L2TP client).
7. Upgrading firmware from V3.40(SC.1) to V3.40(SC.2) need to use firmware upgrade tool to update new firmware. This tool only support change firmware from V3.40(SC.1) to V3.40(SC.2) and change romfile to V3.40(SC.2)C1, you can't use this tool to upgrade firmware from others version. See Appendix 4.
8. In SMT menu 4 and menu3.5 the ISP's name and ESSID can not accept special characters such as #$%^, but in eWC can accept it, they are not accordant.
9. Upgrading firmware from V3.40(SC.2) to V3.40(SC.3) need to use firmware upgrade tool to update new firmware. This tool only support change firmware from V3.40(SC.2) to V3.40(SC.3). you can't use this tool to upgrade firmware from others version.

Features:

Modifications in V3.40(SC.3)C0 | 11/30/2005

1. Change to FCS.

Modifications in V3.40(SC.3)b1 | 11/11/2005

1. build this firmware based on 3.40(QR.8)C1
2. [FEATURE ENHANCE]
   Reset button function is added for TE test.
3. Change modem code to: TI AR7 01.01.07.00
4. [BUG FIX] SPRID: 051111830
   Symtpom: When you configure a VPN rule with PSF (DH1 or DH2) enabled on P662HHW-61 (340QR8C0), the problem would occur: the tunnel is up but there is no traffic.
   Condition: N/A
5. Change default romfile to avoid romfile data converting.

Modifications in V3.40(SC.2)C1 | 11/09/2004

1. [BUG FIXED]
Symptom: Change default Romfile to avoid Romfile data converting.
Condition: N/A

Modifications in V3.40(SC.2)C0 | 11/05/2004

1. [FEATURE CHANGE]
Symptom: Change to FCS version.
Condition: N/A

Modifications in V3.40(SC.2)b3 | 11/04/2004

1. [BUG FIXED]
Symptom: Customer reported he cannot build VPN tunnel between 2 P662HW-61 when using DES/3DES encrpt. But after we changing the AES encryption and then tunnel was

built.
Condition: There are two ADSL lines in customer's lab.
1. PPPoA/VC, 64/256Kbps
2. PPPoE, 32/128Kbps
When using DES for the VPN rules, we found there were always some packets lost when the IPSec hand shaking at phase 1 or phase2. After change to AES at customer's env., the VPN can be built successfully.
2. [BUG FIXED]
Symptom: In Web/GUI, changing the setting of Windows Networking (NetBIOS over TCP/IP) in DMZ setting page will cause system reboot.
Condition: There are two reasons that cause system reboot.
1. Continuous ROM file program, that might causes system reset by watch dog timer.
2. System exception due to the NULL pointer access.

Modifications in V 3.40(SC.2)b2 | 10/26/2004
1. [BUG FIXED]
Symptom: Firewall ACL set LAN to WAN is disappeared
Condition: N/A
2. [BUG FIXED]
Symptom: Romfile data converting occurs after restore default ROM file
Condition:N/A
Modifications in V 3.40(SC.2)b1 | 10/07/2004
1. [FEATURE CHANGE]
Symptom: Based on P662HW-61 3.40(QR.4)C0, and change modem code to version 1.1.8.0
Condition: N/A
2. [BUG FIX]
Symptom: If we ping from LAN PC to WAN and changes encapsulation to PPPoA or PPPoE will cause ping failed
Condition: Use Web/GUI to configure WAN page and change encapsulation will cause ping failed.
3. [BUG FIX]
Symptom: When delete SMT4 the mode changes to multi mode, even we configured as G.DMT
Condition: N/A
4. [BUG FIX]
Symptom: ARP request packets comes from first PVC (Enet encap) but it will be replied to another PVC(RFC1483 bridge)
Condition: Device is configured as 2 PVCs. The first is Enet Encap, and the other is RFC1483 bridge. The packets, e.g. ARP, which have to be sent to the 1st PVC, will be sent to the 2nd PVC. The problem makes the remote VLAN enabled router confused and the communication will fail.

Modifications in V 3.40(SC.1)C0 | 07/13/2004
1. [FEATURE CHANGE]
Symptom: Change to FCS version

Condition: N/A

Modifications in V 3.40(SC.1)b1 | 07/12/2004
1. [BUG FIX]
Symptom: Any-IP doesn't work fine if PC uses Windows XP OS.
Condition: Only happens when PC uses Windows XP
2. [BUG FIX]
Symptom: The Redirected page of Zero-Configuration has Java Script error.
Condition: N/A
3. [BUG FIX]
Symptom: Memory leakage happens in size 64, when reset WLAN
Condition: N/A

Modifications in V 3.40(SC.0)C0 | 06/18/2004
1. [FEATURE CHANGE]
Symptom: Change to FCS version.
Condition: N/A

Modifications in V 3.40(SC.0)b3 | 06/17/2004

1. [FEATURE CHANGE]
Symptom: Wireless AP F/W 5.0.8 has bad throughput, change back to AP F/W 5.0.7
Condition:N/A

2. [BUG FIX]
Symptom: In SMT4, and SMT11 the system will limit the usage when VPI is 0 and VCI is 32 or under.
Condition: N/A

Modifications in V 3.40(SC.0)b2 | 06/8/2004
1. [BUG FIX]
Symptom: Delete SMT menu 4 ISP node, then the ADSL standard will become multi-mode, but TI Annex B only support G.DMT.
Condition: N/A

Modifications in V 3.40(SC.0)b1 | 05/28/2004
1. [FEATURE CHANGE]
Symptom: Create model P662HW-63/67, and change the version of ADSL modem code to 01.01.03.00
Condition: N/A

Appendix 1: Zero-Configuration and VC auto-hunting

The Zero-Configuration feature can hunt the encapsulation and VPI/VCI value, and system will automatically configure itself if the hunting result is successfully and system will response suitable Web pages if it's still hunting or failed or need user to provide information. But this feature has one assumption that system supposes the ADSL line from ISP only provides one kind of service, otherwise the hunting will get confusing and failed.

Whenever system ADSL links up system will send out some probing patterns, system will analyze the packets returned from ISP, and decide which services the ISP may provide.

System sends out a limited number of patterns which is pre-configured in a hunting pool. Each entry of hunting pool must contain the VPI, VCI, and which kinds of hunting patterns you want to send.

Whenever system send out all the probing patterns with specific VPI/VCI, system will wait for 5~10 seconds and get the response from ISP, the reply patterns from ISP will decide which kinds of ADSL services of the line will be. After that, system will save back the correct VPI, VCI and also service (encapsulation) type into profile of WAN interface.

Follows are the CI commands that system provides for VC auto-hunting

Command				Description
wan	atm	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

Appendix 2: Media Bandwidth Management Wizard

Media Bandwidth Management (MBM) is for user to control the QoS for different services but the configurations of MBM is too complicated to end-users. So, we develop MBM Wizard to reduce the loading of user configurations. In current design, we just support 6 services which include XBOX, VoIP(SIP), FTP, Email, eMule, WWW, and follows are the classes design details for each interfaces.

Service	**Classes**	**Comment**
XBOX	Create classes on WAN, LAN, WLAN interface which will need to bind filter on TCP port 3074, and UDP port 3074	
VoIP(SIP)	Create classes on WAN, LAN, WLAN interface which need to bind filter with dynamic ALG for SIP	
FTP	Create classes on WAN, LAN, WLAN interface which need to bind a filter with dynamic ALG for FTP.	
E-Mail	1.Create classes on WAN interface which need to bind filter with TCP port 25. 2. Create classes on LAN, WLAN interface which need to bind filter with TCP port 110.	
eMule	Create classes on WAN, LAN, WLAN interface which need to bind filter with TCP port 4662	
WWW	Create classes on LAN, WLAN interface which need to bind filter with TCP port 80.	The most of HTTP traffic is coming from downstream directions. So we only create classes in LAN, and WLAN side.

MBM has a borrow mechanism and now we use it for MBM Wizard. System only assign 10k budget (by default) for each class, for sure it's not enough for usage. System also configures the class that can borrow from parent class(root class), but if there are two or more services online at the same time, the borrow mechanism will depend on the priority that we configured in each class. That means the class with higher priority value will get the parent (root) bandwidth first.

Appendix 3: Anti-Virus (Packet Scan)

Virus is one of the most threats of internet security. They spread rapidly and cause huge damage in the world. For virus against, Ani-virus application becomes a popular resolution. But it usually works on a complicate system with many loopholes (ex, Windows series) which provide more changes for virus infection. The main medium for viruses to spread is network. If we want to defense viruses form network, the simpler and securer network devices would play a key role.
Packet Scan is good for virus against. It re-sites in common network device (Ex ADSL router) and scans each network packet fragment. It can quickly discover and destroy virus before entering user's computer.
In current design, we support FTP, HTP, SMTP, and POP3 network scanning.

Feature

1 Support downstream packets scanning for FTP, HTP, and POP3 network protocol.
2 Support upstream packets scanning for SMTP network protocol.
3 Support automatic and manual online update for scanning engine form GGreat server.
4 Providing centralize log and alert while virus detection.
5 Support Windows Messages for virus notification. (Win98, WinME, Win2K, WinXp)

Limitation

1 Each network protocol FTP, HTP, POP3 and SMTP must use standard port number, FTP is 21, HTP is 80, POP3 is 110 and SMTP is 25.
2 Compression file scanning doesn't support (Ex ZIP, RAR).
3 Doesn't support multi-session download (flashGet).
4 The maximum session number is 300 that can be created simultaneous
5 There exists the extension file name limitation.
  5.1 Available extension file name is following.
  mhtm,mhtml,asp,bat,com,class,cpl,cmd,doc,dot, dll, drv, exe, eml, htm, html, hta, htt, hlp, js, jse, jsp, lnk, nws, obj, ocx, pif, ppt, php, rtf, rar, scr, shtml, swf, vbs, vba, vbe, vxd, xml, xls, xla, wml, zip
6 Support following virus types detection.

The representative virus in recent four years:			
X1 _Virus	LENA_Virus	SW Flash_Virus	Fable_Worm
NOTEPAD TROJAN	JASEMIN_Virus	Myparty_Worm	Cult_Worm
VIRUS	DESIRE_Virus	MYSYS_Worm	Spybot_Worm
ILOVEYOU_Virus	SEEKER.JS	LOTTO_Worm	Kindal_Worm
MTX_Virus	DELBIOS.INF	PATCH_Worm	Fizzer_Worm
CIH Killer 1.1	PHP.Alf_Virus	SHARP_Worm	Kwbot_Worm
WEIRD_Virus	PHAGE.PALM_Virus	GIBE_Worm	Electron_Worm
Plage 2000_Virus	CODEGREEN_Virus	Cervivec_Worm	Hawawi_Worm
WORD 97 MACRO	ANTHRAX_Virus	Valentin_Worm	Palyh_Worm
VIRUS	PET-TICK_Virus	MyLife_Worm	Oror_Worm
EXCEL 97 MACRO	Winmem_Html	Yarner_Worm	GPIX_Virus
VIRUS	ADDY.PL_Virus	IFRAME-Mail_Worm	Venzu_Worm
NAVIDAD_Virus	DEAD0H_Virus	BirdSpy_Worm	Sdbot_Worm
CREATIVE_Virus	Invictus infector_Virus	Fix2001_Worm	Mumu_Worm
JOKE-GHOST_Virus	TRION_Virus	Perrun_Worm	Gaobot_Worm
Ghost _Virus	EMBRION_Virus	Simile_W32	Lolol_Worm

Hdfill32_Virus	TROOD_Virus	GAY_Worm	Sodabot_Worm
EMANUEL_Virus	SABIA_Virus	Runouce_Worm	Webauto_Worm
Cabanas PE_Virus	BINLADEN_Virus	Msvxd_Worm	Redist_Worm
HYBRIS_Virus	LAZYVX_Virus	Yourpassword_Worm	Opax_Worm
Demiurg_Virus	REDALART_Virus	Startme_Html	Lorraine_Worm
Blebla_Virus	Unknown VBS Virus	PWsteal Server	Valla_Virus
Kenston PE_Virus	JAVAKILLER_Virus	Scrsvr_Worm	Klexe_Worm
Dark Akuma_Virus	SPACES_Virus	Bugbear_Worm	Fortnight_Worm
Windows Bomb_Virus	WINSTART_BAT_Virus	Redlof_Worm	Nebiwo_Worm
Back Door Setup_Virus	SYS602_BAT_Virus	Rawtocash_Worm	Deloder_Worm
Bymer Wininit_Virus	PENFOLD_BAT_Virus	Henpeck_Worm	Mimail_Worm
Etymo-Crypt.1308	IKX_Virus	Brasil_Worm	Msblast_Worm
VBS.ANNA_Virus	Halen_Virus	HAI_Worm	Welchi_Worm
Explorer Inf PE	DION_Virus	Bymer Msi211	Randex_Worm
Cih v1.2x_Virus	Evil_Virus	Pate_Virus	Swen_Worm
Winux PE_ELF virus	MARKJ_Virus	Bride_Worm	Mapson_Worm
Bad Transmission_Virus	ALIZEE_Virus	Cblade_Worm	Trojan_Worm
CfgWiz32 Virus	LARA.THEME_Virus	Iraq_Worm	Qint_Worm
SIRCAM_W32_Virus	NACH_Virus	DUPATOR	Dozer_Worm
EICAR _Virus	LASTWORLD_Virus	Setver_Worm	Inmotecd_Worm
APOST_Virus	QUEST_Virus	WinHaelp_Worm	Galil_Worm
MYPICS_Virus	XANAX_Virus	Recovery_Worm	MSN_Worm
1NFO.A RTF_Virus	PARROT_Virus	Sobig_Worm	Sober_Worm
DOGGIE_Virus	CICHOSZ_Virus	Lirva_Worm	Beagle_Worm
INVALID_Virus	ALMA_Virus	Cupid_Worm	Mydoom_Worm
KETAMINE_Virus	EXPL0RER_Virus	Supova_Worm	DeadHat_Worm
STREAM_Virus	KRIZ_Virus	Handy_Worm	Netsky_Worm
VAMPIRE_Virus	XPUPDATE_BAT_Virus	Lovegate_Worm	Femot_Worm
SEX URL_Virus	BACKDOOR_WORM_Virus	Zoek_Worm	Flat_Worm
TRINOO_Virus	BYTEBAND_Virus	Holar_Worm	Netav_Worm
NIMDA_Virus	VBS_Engine_Virus	Kaiten_Virus	Serot_Worm
SUBSEVEN_Virus	Pentagone_Worm	WHOG_Virus	Elerad_Virus
WinCAW_Virus	Weird_Trojan	Sachiel_Worm	Paroc_Virus
ROACH_Virus	WINL0G0N_WORM	Ganda_Worm	Trilissa_Virus
UNCENSORED_Virus	Scherzo_Worm	Sysupd_Worm	Sasser_Worm
INTA_Virus	GOP_Worm	Scchost_Worm	Explet_mm
ARIS_Virus	Dotnet_Virus	Ultimax_Worm	Xabot_Worm
BUBICA_Virus	Happy Time	Lovelorn_Worm	Protoride_Worm
BUMDOC_Virus	Klez Series_Virus	Flood_Worm	Erkez_Worm
CEREBRUS_Virus			
DOB_Virus			
GUNMAN_Virus			

Virus infect through by special port:

Iraq_Worm—invade through (SMB Server message service) port 445
Msblast_Worm-- Invade through TCP Port 135 and open TCP port 4444 then open UDP port 69
Welchi_Worm --Invade through TCP Port 135.
Fizzer _Worm --Open 81 Port to be HTTP Server and open 2018 to 2021 Port to be backdoor.
Sasser _Worm—The vulnerability of LSASS in port 445.
Bobax _Worm-- The vulnerability of LSASS in port 445.
Korgo_Worm-- The vulnerability of LSASS in port 445.
CODERED_IIS
CodeBlue_IIS

Appendix 3: Content Access Control (CAC)

Content Access Control (CAC) provides ability to manage each user host for internet access. Through CAC, network administrator can arrange the time schedule of internet access, set up which network service can be used and manage which web site can be browsed for each group user. There are 4 groups and 32 user profiles provided in this system currently, each group provides different internet access rule, there are 3 types of parameters to define the access rule. Time schedule type of parameters that specifies the time interval for internet access, Service type of parameters that specifies which internet services can be provided, such as Telnet, FTP, and HTTP and so on. Web browsing type of parameters that restricts access some categories of web sit. In each user profile, there are 3 parameters, the first is user name, the second is password and the third is group index, each user who wants to access internet must login to device successfully first by entering user name and password through web browser and the group index specifies which group profile is used to define internet access rule

Feature

1 Provide 4 groups to define 4 different rules for internet access. Each group contains 3 types of parameter to define the internet access rule.
   - 1.1 Time Schedule: To arrange the internet access time by specifying time interval and time budget.
   - 1.2 Service: Provide the ability to restrict some specific internet service usage.
   - 1.3 Web Browsing: To restricts access some types of web sit. Provide two methord.
     - 1.3.1 Pre-defined Web Content Categories: User can define which web categories should be blocked. To classify each web URL, device connects to Cerberian's server that will provide the category of this web URL.
     - 1.3.2 Keyword blocking: User can create a set of keyword. Device will search of those keywords in every web URL. If match, then block is web browsing.
2 Provide 32 user profile
3 Provide Centralize log.

Limitation

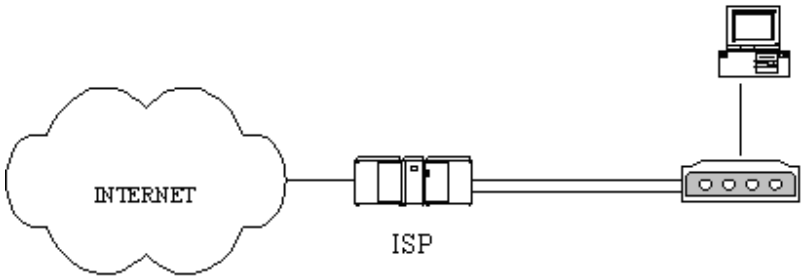
1 Content filter will be disabled while CAC enable.
2 Any user host that belongs to NAT server set can access internet at will. CAC doesn't take effect for this host.
3 Pre-defined Web Content Categories will be disabled automatically if the Cerberian's server connection failure -"request error".

Appendix 4: ZyXEL F/W Upgrade Tool

Network Environment:

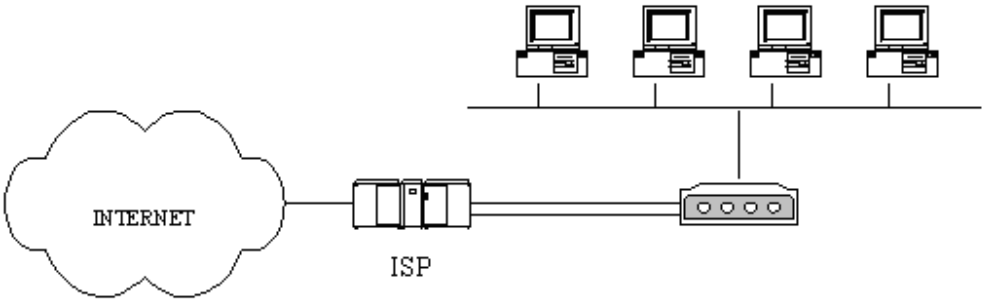
1. Prestige Modem Series

The target network environment is a PC connected to Prestige modem directly. The below figure shows a typical Internet access application. (If there is any IP sharing devices, like router, or switch between PC and Prestige modem, users must connect the PC to Prestige modem directly first before running the program.)



2. Prestige Router Series

The target network environment is a small number of PCs using the Prestige DHCP service for IP address assignment. Following figure shows a typical Internet access application.



Firmware Upgrade Procedure

1. Change the Router's password to "1234".
2. Change the Router's LAN IP to "192.168.1.1" and make sure that PC can connect to Router.
   - ⇨ If your PC's IP is dynamic assigned by router, please release original IP and renew it from router's DHCP service.
   - ⇨ If your PC's IP is static assigned, please change it and make sure the new IP address at same subnet with router. (Ex: Set PC's IP to 192.168.1.33).
3. Executing the upgrade tool and wait about 6 minutes to wait firmware upgrade procedure finished.
4. If the original password is not "1234", change back to original setting.
5. Restore the original IP setting of router and reboot it if necessary.

Annex B CI Command List

Command Class List Table		
System Related Command	Exit Command	Ethernet Related Command
WAN Related Command	WLAN_Related_Command	IP Related Command
PPP Related Command	Bridge Related Command	Radius Related Command
8021x Related Command	Firewall Related Command	Configuration Related Command
SMT Related Command		

System Related Command Home

Command				Description
sys				
	adjtime			retrive date and time from Internet
	cbuf			
		display	[a|f|u]	display cbuf a: all f: free u: used
		cnt		cbuf static
			display	display cbuf static
			clear	clear cbuf static
	baud		<1..5>	change console speed
	callhist			
		display		display call history
		remove	<index>	remove entry from call history
	clear			clear the counters in GUI status menu
	countrycode		[countrycode]	set country code
	date		[year month date]	set/display date
	domainname			display domain name
	edit		<filename>	edit a text file
	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	display trace event
			clear <num>	clear trace event
	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
	fid			
		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
	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
		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
	mbuf			
		cnt		
			disp	display system mbuf count
			clear	clear system mbuf count
		link	link	list system mbuf link
		pool	<id> [type]	list system mbuf pool
		status		display system mbuf status
		disp	<address>	display mbuf status

		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
	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
		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
	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
		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
		cnt	<ch-name>	show channel connection related counter
	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

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
			clear <name>	clear ether driver counters
		iface	<ch_name> <num>	send driver iface
		ioctl	<ch_name>	Useless in this stage.
		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
	version			see ethernet device type
	pkttest			
		disp		
			packet <level>	set ether test packet display level
			event <ch> [on|off]	turn on/off ether test event display
		sap	[ch_name]	send sap packet
		arp	<ch_name> <ip-addr>	send arp packet to ip-addr
		mem	<addr> <data> [type]	write memory data in address
	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

WAN Related Command Home

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
			Gdmt	
			multimode	

		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		
			sendes	Send current error second information immediately
		targetnoise	[value]	Adjust target noise offset
wan	atm	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
	hwsar	disp		Display hwsar packets incoming/outgoing information
		clear		Clear hwsar packets information

WLAN Related Command Home

Command				Description
Wlan				
	active	[on|off]	[0|1]	Turn on/off wireless lan
	association			Show association list
	load			Load WLAN configuration into buffer.
	Display			Display WLAN configuration data.
	chid			Configure channel ID
	essid			Configure ESSID
	hiddenssid		[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
		Key	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.
	Power		[1:19dbm, 2:18dbm, 3:16dbm, 4:15dbm, 5:14dbm]	Change TX power level.
	reset			Reset WLAN
	filter			
		[incoming | outgoing]	<generic>[set#1][set#2][set#3][set#4]	To set generic filter for wireless channel
	fildisp			Display wireless filter setting
	1130cmd			Internal usage.
		restart_stat		Show WLAN restart statistics
		chg_dot11mode		Set WLAN state to mix mode, B only or G only
		show_rxDesc		Show number of Rx host descriptors
		acxstat		Show acx run time statistics

IP Related Command Home

Command				Description
ip				
	address		[addr]	display host ip address
	loopbackaddr		<IP1> [IP2]	Set loopback 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
		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 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			
		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
		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>	chaek if iface is available.
	ping		<hostid>	ping remote host
	pong		<hostid> [<size> <time-interval>]	pong remote host
	extping		<target address>	
			[-t]	Continue to send ECHO_REQ until Ctrl-C input
			[-c]	Validate the reply data
			[-d] [Data]	Data pattern. The maximum length of data is 255 characters.
			[-f]	Set DF flag.
			[-l] [Data size]	Datagram size in bytes (with 28 bytes Header).
			[-v] [TOS value]	Specify the value of TOS flag.
			[-n] [Repeat value]	The number of times to send ECHO_REQ packet.
			[-w] [Timeout value]	Specify the value of Timeout in seconds.
			[-o] [IP address/IFace]	To specify one IP address or interface to be the

				Source IP address.
			[-p] [Min MTU] [Max MTU] [Interval size]	Sweep range of sizes.
	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	[tcb] [<interval>]	display TCP statistic counters
		syndata	[on|off]	TCP syndata piggyback
		trace	[on|off]	turn on/off trace for debugging
		window	[tcb]	TCP input window size
	samenet		<iface1> [<iface2>]	display the ifaces that in the same net
	uninet		<iface>	set the iface to uninet
	tftp			
		support		pritn if tfpt is support
		stats		display tftp status

	xparent			
		join	<iface1> [<iface2>]	join iface2 to iface1 group
		break	<iface>	break iface to leave ipxparent group
	antiprobe		<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			
		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
			tcpother [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

PPP Related Command Home

Command				Description
ppp				
	autotrigger			
		on	<remoteNodeIndex>	turn on packet trigger, default is enable
		off	<remoteNodeIndex>	turn off packet trigger
		status		show autotrigger status
	retry		<interval>	adjust PPP retrial interval

Bridge Related Command Home

Command				Description
bridge				
	mode		<1/0> (enable/disable)	turn on/off (1/0) LAN promiscious 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 traffice monotor. 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

Radius Related Command Home

Command				Description
radius				
	auth			show current radius authentication server configuration
	acco			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

Configuration Related Command Home

Command					Description
config					The parameters of config are listed below.
edit	firewall	active <yes|no>			Activate or deactivate the saved firewall settings
retrieve	firewall				Retrieve current saved firewall settings
save	firewall				Save the current firewall settings
display	firewall				Displays all the firewall settings
		set <set#>			Display current entries of a set configuration; including timeout values, name, default-permit, and number of rules in the set.
		set <set#>	rule <rule#>		Display current entries of a rule in a set.
		attack			Display all the attack alert settings in PNC
		e-mail			Display all the e-mail settings in PNC
		?			Display all the available sub commands
		e-mail	mail-server <mail server IP>		Edit the mail server IP to send the alert
			return-addr <e-mail address>		Edit the mail address for returning an email alert
			e-mail-to <e-mail address>		Edit the mail address to send the alert
			policy <full | hourly |daily | weekly>		Edit email schedule when log is full or per hour, day, week.
			day <sunday | monday | tuesday | wednesday | thursday | friday | saturday>		Edit the day to send the log when the email policy is set to Weekly
			hour <0~23>		Edit the hour to send the log when the email policy is set to daily or weekly
			minute <0~59>		Edit the minute to send to log when the email policy is set to daily or weekly
			Subject <mail subject>		Edit the email subject
		attack	send-alert <yes|no>		Activate or deactivate the firewall DoS attacks notification emails
			block <yes|no>		Yes: Block the traffic when exceeds the tcp-max-incomplete threshold
					No: Delete the oldest half-open session when exceeds the tcp-max-incomplete threshold
			block-minute <0~255>		Only valid when sets 'Block' to yes. The unit is minute
			minute-high <0~255>		The threshold to start to delete the old half-opened sessions to minute-low
			minute-low <0~255>		The threshold to stop deleting the old half-opened session
			max-incomplete-high <0~255>		The threshold to start to delete the old half-opened sessions to max-incomplete-low
			max-incomplete-low <0~255>		The threshold to stop deleting the half-opened session
			tcp-max-incomplete <0~255>		The threshold to start executing the block field
		set <set#>	name <desired name>		Edit the name for a set

			default-permit <forward|block>		Edit whether a packet is dropped or allowed when it does not match the default set
			icmp-timeout <seconds>		Edit the timeout for an idle ICMP session before it is terminated
			udp-idle-timeout <seconds>		Edit the timeout for an idle UDP session before it is terminated
			connection-timeout <seconds>		Edit the wait time for the SYN TCP sessions before it is terminated
			fin-wait-timeout <seconds>		Edit the wait time for FIN in concluding a TCP session before it is terminated
			tcp-idle-timeout <seconds>		Edit the timeout for an idle TCP session before it is terminated
			pnc <yes|no>		PNC is allowed when 'yes' is set even there is a rule to block PNC
			log <yes|no>		Switch on/off sending the log for matching the default permit
			rule <rule#>	permit <forward|block>	Edit whether a packet is dropped or allowed when it matches this rule
				active <yes|no>	Edit whether a rule is enabled or not
				protocol <0~255>	Edit the protocol number for a rule. 1=ICMP, 6=TCP, 17=UDP...
				log <none|match|not-match|both>	Sending a log for a rule when the packet none|matches|not match|both the rule
				alert <yes|no>	Activate or deactivate the notification when a DoS attack occurs or there is a violation of any alert settings. In case of such instances, the function will send an email to the SMTP destination address and log an alert.
				srcaddr-single <ip address>	Select and edit a source address of a packet which complies to this rule
				srcaddr-subnet <ip address> <subnet mask>	Select and edit a source address and subnet mask if a packet which complies to this rule.
				srcaddr-range <start ip address> <end ip address>	Select and edit a source address range of a packet which complies to this rule.
				destaddr-single <ip address>	Select and edit a destination address of a packet which complies to this rule
				destaddr-subnet <ip address> <subnet mask>	Select and edit a destination address and subnet mask if a packet which complies to this rule.
				destaddr-range <start ip address> <end ip address>	Select and edit a destination address range of a packet which complies to this rule.
				tcp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, the user may repeat this command line to enter the multiple port numbers.
				tcp destport-range <start port#> <end port#>	Select and edit a destination port range of a packet which comply to this rule.
				udp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, users may repeat this command line

					to enter the multiple port numbers.
				udp destport-range <start port#> <end port#>	Select and edit a destination port range of a packet which comply to this rule.
				desport-custom <desired custom port name>	Type in the desired custom port name
delete	firewall	e-mail			Remove all email alert settings
		attack			Reset all alert settings to defaults
		set <set#>			Remove a specified set from the firewall configuration
		set <set#>	rule <rule#>		Remove a specified rule in a set from the firewall configuration
insert	firewall	e-mail			Insert email alert settings
		attack			Insert attack alert settings
		set <set#>			Insert a specified rule set to the firewall configuration
		set <set#>	rule <rule#>		Insert a specified rule in a set to the firewall configuration
cli					Display the choices of command list.

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

SMT Related command Home

No	Command	Description	Comment
	sys bridge [on|off]	Set system bridge on/off	Menu 1
	sys routeip [on|off]	Set system IP routing on/off	Menu 1

	sys hostname [hostname]	Set system name	Menu 1
	sys display	Display hostname, routing/bridge mode information in menu 1	Display Menu 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	
	wan backup mechanism [dsl | icmp]	Set wan backup mechanism to DSL link or ICMP	Menu 2
	wan backup addr [index] [IP addr]	Set wan ip address <index>	Menu 2
	wan backup tolerance [number]	Set keepalive fail tolerance	Menu 2
	wan backup recovery [interval(sec)]	Set recovery interval	Menu 2
	wan backup timeout [number]	Set ICMP timeout	Menu 2
	wan backup save	Save wan backup related parameters	Menu 2
	wan backup display	Display wan backup configurations	Menu 2
	wan tredir active [on|off]	Set traffic redirect on/off	Menu 2.1
	wan tredir ip [IP addr]	Set traffic redirect gateway IP address	Menu 2.1
	wan tredir metric [number]	Set traffic redirect metric	Menu 2.1
	wan tredir save	Save traffic redirect related parameters ** Have to apply "wan backup save" command thereafter	Menu 2.1
	wan tredir display	Display traffic redirect configurations	Menu 2.1
	lan index [1|2|3|4] 1: Select main LAN Interface 2: Select IP Alias 1 3: Select IP Alias 2 4.DMZ	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	Menu 11.1

		the index number for pointing to specific PVC (remote node), and for consequent commands reference, if index = 1 means it's ISP node	
	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 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 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 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
	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 may 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 [new password]	Set system password [save immediately]	Menu 23 system password
	sys baud [1-5]	Index 12,3 will be 38400,19200, 9600, 57600, 115200 bps [save immediately]	Menu 24.2.2 console speed
	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, [1] means display buffer	
	sys server save	Save the embedded server (remote management) parameters	
	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 [#=1~11]	Set channel ID 1-11	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	

Internal Information:

1.Support ADSL2+ by TI modem code: TI AR7 01.01.07.00
2.Support Multi-Boot client V2.1

1. Features

Modifications in V 3.40(SC.2)b1 | 10/07/2004

1. [FEATURE ENHANCE]
   Symptom: Support multicast firmware upgrade tools on PC, please refer to related document for details.
   Condition: N/A
18. [FEATURE ENHANCE]
   Symptom: If WLAN card is not existed, system will change product name automatically to "P662H-63".
   Condition: N/A

2. Manufactory Data in Bootbase

```
atsh
ZyNOS Version           : V3.40(SC.3) | 11/30/2005 13:10:52
Bootbase Version        : V1.06 | 04/01/2004 11:22:33
Vendor Name             : ZyXEL Communications Corp.
Product Model           : Prestige 662HW-63/67
ZyNOS Code Model        : P662HW-63 ATU-R
HTP Code Model          : HTP_P662 V 0.06
ZyNOS ROM address       : b0020000
System Type             : 7
MAC Address             : 001349000001
Default Country Code    : FF
Boot Module Debug Flag : 01
RomFile Version         : 3C
RomFile Checksum        : ec41
ZyNOS Checksum          : 11ef
Core Checksum           : 0892
SNMP MIB level & OID    :
060102030405060708091011121314151617181920
Main Feature Bits       : C0
Other Feature Bits      :
          92 58 00 00 00 00 00 00-00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00-01 41 13 00 00 00

OK
```

Notes:

- Debug Flag should be 0 after production. In our default release will be 1. Because in the manufacture process will need it to set the MAC address.
- MAC address will be change by production process. Only the fist 3 octets will be correct. The last 3 octets will depend on the production process.
- Country code value will be change by production process. It will depend on the shipping country.

3. Default ROM File Value Setting

·

· Main menu

```
                Copyright (c) 1994 - 2005 ZyXEL Communications Corp.

                          Prestige 662HW-63/67 Main Menu

Getting Started                         Advanced Management
  1. General Setup                        21. Filter and Firewall Setup
  2. WAN Backup Setup                     22. SNMP Configuration
  3. LAN Setup                            23. System Security
  4. Internet Access Setup                24. System Maintenance
  5. DMZ Setup                            25. IP Routing Policy Setup
Advanced Applications                     26. Schedule Setup
  11. Remote Node Setup                   27. VPN/IPSec Setup
  12. Static Routing Setup
  14. Dial-in User Setup                  99. Exit
  15. NAT Setup




                        Enter Menu Selection Number:
```

·

· Menu 1: General Setup

```
                            Menu 1 - General Setup

                    System Name= ?
                    Location=
                    Contact Person's Name=
                    Domain Name=
                    Edit Dynamic DNS= No

                    Route IP= Yes
                    Bridge= No


                    Press ENTER to Confirm or ESC to Cancel:
```

· Menu 2 - Wan Backup Setup

```
                    Menu 2 - Wan Backup Setup

                Check Mechanism = DSL Link
                Check WAN IP Address1 = 0.0.0.0
                Check WAN IP Address2 = 0.0.0.0
                Check WAN IP Address3 = 0.0.0.0
                  KeepAlive Fail Tolerance = 0
                  Recovery Interval(sec) = 0
                  ICMP Timeout(sec) = 0
                Traffic Redirect = No
                Dial Backup = No


              Press ENTER to Confirm or ESC to Cancel:
```

- Menu 2.1 - Advanced Dial Backup Setup

```
                    Menu 2.1 - Traffic Redirect Setup

              Active= No
              Configuration:
                Backup Gateway IP Address= 0.0.0.0
                Metric= 15


              Press ENTER to Confirm or ESC to Cancel:
```

- Menu 3: LAN Setup

```
                            Menu 3 - LAN Setup

                 1. LAN Port Filter Setup
                 2. TCP/IP and DHCP Setup


                 5. Wireless LAN Setup
                 6. Port Based VLAN Setup


                       Enter Menu Selection Number:
```

- Menu 3.1: LAN Port Filter Setup

```
                Menu 3.1 - LAN Port Filter Setup

                Input Filter Sets:
                  protocol filters=
                    device filters=
                Output Filter Sets:
                  protocol filters=
                    device filters=

                Press ENTER to Confirm or ESC to Cancel:
```

- Menu 3.2 TCP/IP and DHCP Setup

```
                Menu 3.2 - TCP/IP and DHCP Ethernet Setup


                DHCP Setup
                  DHCP= Server
```

```
                        Client IP Pool Starting Address= 192.168.1.33
                        Size of Client IP Pool= 32
                        Primary DNS Server= 0.0.0.0
                        Secondary DNS Server= 0.0.0.0
                        Remote DHCP Server= N/A
                      TCP/IP Setup:
                        IP Address= 192.168.1.1
                        IP Subnet Mask= 255.255.255.0
                        RIP Direction= Both
                          Version= RIP-1
                        Multicast= None
                        IP Policies=
                        Edit IP Alias= No


                      Press ENTER to Confirm or ESC to Cancel:
```

- Menu 3.5 Wireless LAN Setup

```
                      Menu 3.5- Wireless LAN Setup

                      ESSID= Wireless
                      Hide ESSID= No
                      Channel ID= CH06 2437MHz
                      RTS Threshold= 2432
                      Frag. Threshold= 2432
                      WEP= Disable
                        Default Key= N/A
                        Key1= N/A
                        Key2= N/A
                        Key3= N/A
                        Key4= N/A
                      Edit MAC Address Filter= No

                      Press ENTER to Confirm or ESC to Cancel:
```

- Menu 3.5.1 WLAN MAC Address Filter

```
                     Menu 3.5.1 - WLAN MAC Address Filter

                   Active= No
                   Filter Action= Allowed Association
------------------------------------------------------------------------------
  1=   00:00:00:00:00:00   13=   00:00:00:00:00:00   25=   00:00:00:00:00:00
  2=   00:00:00:00:00:00   14=   00:00:00:00:00:00   26=   00:00:00:00:00:00
  3=   00:00:00:00:00:00   15=   00:00:00:00:00:00   27=   00:00:00:00:00:00
  4=   00:00:00:00:00:00   16=   00:00:00:00:00:00   28=   00:00:00:00:00:00
  5=   00:00:00:00:00:00   17=   00:00:00:00:00:00   29=   00:00:00:00:00:00
  6=   00:00:00:00:00:00   18=   00:00:00:00:00:00   30=   00:00:00:00:00:00
  7=   00:00:00:00:00:00   19=   00:00:00:00:00:00   31=   00:00:00:00:00:00
  8=   00:00:00:00:00:00   20=   00:00:00:00:00:00   32=   00:00:00:00:00:00
  9=   00:00:00:00:00:00   21=   00:00:00:00:00:00
 10=   00:00:00:00:00:00   22=   00:00:00:00:00:00
 11=   00:00:00:00:00:00   23=   00:00:00:00:00:00
 12=   00:00:00:00:00:00   24=   00:00:00:00:00:00
------------------------------------------------------------------------------
                     Enter here to CONFIRM or ESC to CANCEL:
```

- Menu 3.6 - Port Based VLAN Setup

```
                    Menu 3.6 - Port Based VLAN Setup

                       1    2    3    4
                  1    -    N/A  N/A  N/A
                  2         -    Yes  Yes
                  3              -    Yes
                  4                   -



                Press ENTER to Confirm or ESC to Cancel:
```

· Menu 4 Internet Access Setup

```
                         Menu 4 - Internet Access Setup

                  ISP's Name= MyISP
                  Encapsulation= ENET ENCAP
                  Multiplexing= LLC-based
                  VPI #= 8
                  VCI #= 35
                  ATM QoS Type= UBR
                    Peak Cell Rate (PCR)= 0
                    Sustain Cell Rate (SCR)= 0
                    Maximum Burst Size (MBS)= 0
                  My Login= N/A
                  My Password= N/A
                  ENET ENCAP Gateway= N/A
                  IP Address Assignment= Dynamic
                    IP Address= N/A
                  Network Address Translation= SUA Only
                    Address Mapping Set= N/A

                  Press ENTER to Confirm or ESC to Cancel:
```

- Menu 5 - DMZ Setup

```
                              Menu 5 - DMZ Setup

                  1. DMZ Port Filter Setup
                  2. TCP/IP Setup

                         Enter Menu Selection Number:
```

- Menu 5.1 - DMZ Port Filter Setup

```
                      Menu 5.1 - DMZ Port Filter Setup

                  Input Filter Sets:
                    protocol filters=
                      device filters=
                  Output Filter Sets:
                    protocol filters=
                      device filters=


                  Press ENTER to Confirm or ESC to Cancel:
```

- Menu 5.2 - TCP/IP Ethernet Setup

```
                    Menu 5.2 - TCP/IP Ethernet Setup

                  TCP/IP Setup:
                    IP Address= 192.168.2.1
                    IP Subnet Mask= 255.255.255.0
                    RIP Direction= None
                      Version= N/A
                    Multicast= None



                  Press ENTER to Confirm or ESC to Cancel:
```

- Menu 11 Remote Node Setup

```
                    Menu 11 - Remote Node Setup

                    1. MyISP (ISP, SUA)
                    2. _________
                    3. _________
                    4. _________
                    5. _________
                    6. _________
                    7. _________
                    8. _________


                  Enter Node # to Edit:
```

- Menu 11.1 Remote Node Profile

```
                        Menu 11.1 - Remote Node Profile

    Rem Node Name= MyISP                Route= IP
    Active= Yes                         Bridge= No

    Encapsulation= ENET ENCAP           Edit IP/Bridge= No
    Multiplexing= LLC-based             Edit ATM Options= No
    Service Name= N/A                   Edit Advance Options= N/A
    Incoming:                           Telco Option:
      Rem Login= N/A                      Allocated Budget(min)= N/A
      Rem Password= N/A                   Period(hr)= N/A
    Outgoing:                             Schedule Sets= N/A
      My Login= N/A                       Nailed-Up Connection= N/A
      My Password= N/A                  Session Options:
      Authen= N/A                         Edit Filter Sets= No
                                          Idle Timeout(sec)= N/A



                    Press ENTER to Confirm or ESC to Cancel:
```

- Menu 11.3 Remote Node Network Layer Options

```
          Menu 11.3 - Remote Node Network Layer Options

    IP Options:                         Bridge Options:
```

```
        IP Address Assignment = Dynamic      Ethernet Addr Timeout(min)= N/A
        Rem IP Addr = 0.0.0.0
        Rem Subnet Mask= 0.0.0.0
        My WAN Addr= N/A
        NAT= SUA Only
          Address Mapping Set= N/A
        Metric= 2
        Private= No
        RIP Direction= None
          Version= RIP-1
        Multicast= None
        IP Policies=

                          Enter here to CONFIRM or ESC to CANCEL:
```

- Menu 11.5 Remote Node Filter

```
                          Menu 11.5 - Remote Node Filter

                      Input Filter Sets:
                        protocol filters=
                          device filters=
                      Output Filter Sets:
                        protocol filters=
                          device filters=


                       Enter here to CONFIRM or ESC to CANCEL:
```

- Menu 11.6 Remote Node ATM Layer Options

```
                    Menu 11.6 - Remote Node ATM Layer Options
                    VPI/VCI (LLC-Multiplexing or PPP-Encapsulation)

                            VPI #= 8
                            VCI #= 35
                            ATM QoS Type= UBR
                            Peak Cell Rate (PCR)= 0
                            Sustain Cell Rate (SCR)= 0
                            Maximum Burst Size (MBS)= 0

                       Enter here to CONFIRM or ESC to CANCEL:
```

- Menu 12 Static Route Setup

```
                          Menu 12 - Static Route Setup

                      1. IP Static Route
                      3. Bridge Static Route

                                Please enter selection:
```

- Menu 12.1 IP Static Route Setup

```
                          Menu 12.1 - IP Static Route Setup

                      1. _________
                      2. _________
                      3. _________
                      4. _________
                      5. _________
                      6. _________
                      7. _________
                      8. _________
                      9. _________
```

```
                        10. _________
                        11. _________
                        12. _________
                        13. _________
                        14. _________
                        15. _________
                        16. _________

                                  Enter selection number:
```

- Menu 12.1.1 Edit IP Static Route

```
                           Menu 12.1.1 - Edit IP Static Route

                        Route #: 1
                        Route Name= ?
                        Active= No
                        Destination IP Address= ?
                        IP Subnet Mask= ?
                        Gateway IP Address= ?
                        Metric= 2
                        Private= No

                        Press ENTER to Confirm or ESC to Cancel:
```

- Menu 12.3 Bridge Static Route Setup

```
                          Menu 12.3 - Bridge Static Route Setup

                        1. _________
                        2. _________
                        3. _________
                        4. _________

                      Enter selection number:
```

- Menu 12.3.1 - Edit Bridge Static Route

```
                         Menu 12.3.1 - Edit Bridge Static Route

                        Route #: 1
                        Route Name= ?
                        Active= No
                        Ether Address= ?
                        IP Address=
                        Gateway Node= 1

                        Press ENTER to Confirm or ESC to Cancel:
```

- Menu 15 - NAT Setup

```
                                  Menu 15 - NAT Setup

                        1. Address Mapping Sets
                        2. NAT Server Sets

                        Enter Menu Selection Number:
```

- Menu 15.1 - Address Mapping Sets

```
                           Menu 15.1 - Address Mapping Sets

                          1.
                          2.
                          3.
```

```
                        4.
                        5.
                        6.
                        7.
                        8.
                      255. SUA (read only)

                      Enter Menu Selection Number:
```

- Menu 15.1.1 – Address Mapping Rules

```
                    Menu 15.1.1 - Address Mapping Rules

 Set Name= ?

Idx  Local Start IP   Local End IP    Global Start IP  Global End IP    Type
--- --------------- --------------- --------------- --------------- ------
 1.
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.
                    Action= None          Select Rule= N/A

                    Press ENTER to Confirm or ESC to Cancel:
```

- Menu 15.2 – NAT Server Sets

```
                            Menu 15.2 - NAT Server Sets

                        1. Server Set 1 (Used for SUA Only)
                        2. Server Set 2
                        3. Server Set 3
                        4. Server Set 4
                        5. Server Set 5
                        6. Server Set 6
                        7. Server Set 7
                        8. Server Set 8
                        9. Server Set 9
                       10. Server Set 10


                       Enter Set Number to Edit:
```

- Menu 15.2.1 –NAT Server Setup (Used for SUA Only)

```
                Menu 15.2.1 - NAT Server Setup (Used for SUA Only)


              Rule   Start Port No.   End Port No.   IP Address
             ------------------------------------------------
                1.    Default          Default        0.0.0.0
                2.      0                0            0.0.0.0
                3.      0                0            0.0.0.0
                4.      0                0            0.0.0.0
                5.      0                0            0.0.0.0
                6.      0                0            0.0.0.0
                7.      0                0            0.0.0.0
                8.      0                0            0.0.0.0
```

```
                 9.      0                0            0.0.0.0
                10.      0                0            0.0.0.0
                11.      0                0            0.0.0.0
                12.      0                0            0.0.0.0


                     Press ENTER to Confirm or ESC to Cancel:
```

· Menu 21 Filter Set Configuration

```
                      Menu 21 - Filter Set Configuration


      Filter                                Filter
    Set #        Comments                Set #        Comments
    ------  -----------------            ------  -----------------
      1      ________________              7      ________________
      2      NetBIOS_WAN                   8      ________________
      3      NetBIOS_LAN                   9      ________________
      4      IGMP                         10      ________________
      5      ________________             11      ________________
      6      ________________             12      ________________


                  Enter Filter Set Number to Configure= 0

                  Edit Comments= N/A

                  Press ENTER to Confirm or ESC to Cancel:
```

· Menu 21.1.2 - Filter Rules Summary

```
                          Menu 21.1.2 - Filter Rules Summary

# A Type                        Filter Rules                          M m n
- - ---- ------------------------------------------------------------ - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137                         N D N
2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138                         N D N
3 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139                         N D N
4 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137                        N D N
5 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138                        N D N
6 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139                        N D F




                     Enter Filter Rule Number (1-6) to Configure:
```

· Menu 21.1.3 - Filter Rules Summary

```
                          Menu 21.1.3 - Filter Rules Summary

# A Type                        Filter Rules                          M m n
- - ---- ------------------------------------------------------------ - - -
1 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53                 N D F
2 N
3 N
4 N
5 N
6 N
```

```
                    Enter Filter Rule Number (1-6) to Configure:
```

- Menu 21.1.4 - Filter Rules Summary

```
                          Menu 21.1.4 - Filter Rules Summary

# A Type                        Filter Rules                              M m n
- - ---- ------------------------------------------------------------------ - - -
1 Y Gen  Off=0, Len=3, Mask=ffffff, Value=01005e                          N D F
2 N
3 N
4 N
5 N
6 N




                    Enter Filter Rule Number (1-6) to Configure:
```

- Menu 21.2 - Firewall Setup

```
                          Menu 21.2 - Firewall Setup

     The firewall protects against Denial of Service (DoS) attacks when
     it is active. The default Policy sets

         1. allow all sessions originating from the LAN to the WAN and
         2. deny all sessions originating from the WAN to the LAN

     You may define additional Policy rules or modify existing ones but
     please exercise extreme caution in doing so

         Active: Yes

         LAN-to-WAN Set Name: ACL Default Set
         WAN-to-LAN Set Name: ACL Default Set

     Please configure the Firewall function through Web Configurator

                   Press ENTER to Confirm or ESC to Cancel:
```

- Menu 22 - SNMP Configuration:

```
                          Menu 22 - SNMP Configuration

                    SNMP:
                      Get Community= public
                      Set Community= public
                      Trusted Host= 0.0.0.0
                      Trap:
                        Community= public
                        Destination= 0.0.0.0

                      Press ENTER to Confirm or ESC to Cancel:
```

- Menu 23 – System Security:

```
                              Menu 23 - System Security
```

```
                    1. Change Password
                    2. RADIUS Server

                    4. IEEE802.1x


                  Enter Menu Selection Number:
```

- Menu 23 – System Security- Change Password

```
                 Menu 23.1 - System Security - Change Password

                   Old Password= ?
                   New Password= ?
                   Retype to confirm= ?


                    Enter here to CONFIRM or ESC to CANCEL:
```

- Menu 23 – System Security –RADIUS Server

```
                  Menu 23.2 - System Security - RADIUS Server

                   Authentication Server:
                     Active= No
                     Server Address= 0.0.0.0
                     Port #= 1812
                     Shared Secret= ********

                   Accounting Server:
                     Active= No
                     Server Address= 0.0.0.0
                     Port #= 1813
                     Shared Secret= ********







                   Press ENTER to Confirm or ESC to Cancel:
```

- Menu 23 – System Security – IEEE802.1x

```
                    Menu 23.4 - System Security - IEEE802.1x

      Wireless Port Control= No Authentication Required
      ReAuthentication Timer (in second)= N/A
      Idle Timeout (in second)= N/A


      Key Management Protocol= N/A
      Dynamic WEP Key Exchange= N/A
      PSK= N/A
      WPA Mixed Mode= N/A
      Data Privacy for Broadcast/Multicast packets= N/A
      WPA Broadcast/Multicast Key Update Timer= N/A

      Authentication Databases= N/A



                    Press ENTER to Confirm or ESC to Cancel:
```

- Menu 24.2.1: System Maintenance –Information

```
                Menu 24.2.1 - System Maintenance - Information


                   Name:
                   Routing: IP
                   ZyNOS F/W Version: V3.40(SC.3) | 11/30/2005
                   ADSL Chipset Vendor: TI AR7 01.01.07.00
                   Standard: ADSL_G.dmt

                   LAN
                     Ethernet Address: 00:13:49:00:00:01
                     IP Address: 192.168.1.1
                     IP Mask: 255.255.255.0
                     DHCP: Server


                         Press ESC or RETURN to Exit:
```

- Menu 24.2.2: System Maintenance – Change Console Port Speed

```
          Menu 24.2.2 - System Maintenance - Change Console Port Speed

                   Console Port Speed: 9600

                   Press ENTER to Confirm or ESC to Cancel:
```

- Menu 24.3.2: System Maintenance – UNIX Syslog

```
                Menu 24.3.2 - System Maintenance - UNIX Syslog

                   UNIX Syslog:
                   Active= No
                   Syslog IP Address= 0.0.0.0
                   Log Facility= Local 1


                   Press ENTER to Confirm or ESC to Cancel:
```

- Menu 24.10: System Maintenance – Time and Date Setting

```
             Menu 24.10 - System Maintenance - Time and Date Setting

          Use Time Server when Bootup= None
          Time Server Address= N/A

          Current Time:                          00 : 12 : 48
          New Time (hh:mm:ss):                   00 : 12 : 46

          Current Date:                          2000 - 01 - 01
          New Date (yyyy-mm-dd):                 2000 - 01 - 01

          Time Zone= GMT

          Daylight Saving= No
          Start Date (mm-dd):                          01 - 01
          End Date (mm-dd):                            01 - 01


                   Press ENTER to Confirm or ESC to Cancel:
```

- Menu 24.11: System Maintenance – Remote Management Control

```
                Menu 24.11 - Remote Management Control

TELNET Server:
  Server Port = 23                  Server Access = ALL
  Secured Client IP = 0.0.0.0

FTP Server:
  Server Port = 21                  Server Access = ALL
  Secured Client IP = 0.0.0.0

Web Server:
  Server Port = 80                  Server Access = ALL
  Secured Client IP = 0.0.0.0

                Press ENTER to Confirm or ESC to Cancel:
```

- Menu 25: IP Routing Policy Setup

```
                    Menu 25 - IP Routing Policy Setup

Policy                                  Policy
Set #         Name                      Set #         Name
------  ----------------------          ------  ----------------------
  1     ______________________            7     ______________________
  2     ______________________            8     ______________________
  3     ______________________            9     ______________________
  4     ______________________           10     ______________________
  5     ______________________           11     ______________________
  6     ______________________           12     ______________________


                Enter Policy Set Number to Configure= 0

                Edit Name= N/A

                Press ENTER to Confirm or ESC to Cancel:
```

- Menu 26: Schedule Setup

```
                          Menu 26 - Schedule Setup

Schedule                                Schedule
Set #         Name                      Set #         Name
------  ----------------------          ------  ----------------------
  1     ______________________            7     ______________________
  2     ______________________            8     ______________________
  3     ______________________            9     ______________________
  4     ______________________           10     ______________________
  5     ______________________           11     ______________________
  6     ______________________           12     ______________________
```

```
                    Enter Schedule Set Number to Configure= 0

                    Edit Name= N/A

                    Press ENTER to Confirm or ESC to Cancel:
```

- Menu 27 - VPN/IPSec Setup

```
                        Menu 27 - VPN/IPSec Setup

                    1. IPSec Summary
                    2. SA Monitor


                           Enter Menu Selection Number:
```

- Menu 27.1 - IPSec Summary

```
                              Menu 27.1 - IPSec Summary

#      Name    A Local Addr Start  - Addr End / Mask   Encap  IPSec Algorithm
     Key Mgt     Remote Addr Start - Addr End / Mask          Secure Gw Addr
--- ---------- - -----------------  ----------------- ------ ----------------
001

002

003

004

005


             Select Command=  None          Select Rule=  N/A

                   Press ENTER to Confirm or ESC to Cancel:
```

- Menu 27.2 - SA Monitor

```
                              Menu 27.2 - SA Monitor

#                    Name                            Encap.  IPSec Algorithm
--- ------------------------------------------ -------- ---------------
001
002
003
004
005
006
007
008
009
010
```

```
                    Select Command= Refresh
                    Select Connection= N/A

                    Press ENTER to Confirm or ESC to Cancel:
```

- Default commands in autoexec.net

· ras > sys view autoexec.net

```
 sys errctl 0
 sys trcl level 5
 sys trcl type 1180
 sys trcp cr 64 96
 sys trcl sw off
 sys trcp sw off
 ip tcp mss 512
 ip tcp limit 2
 ip tcp irtt 65000
 ip tcp window 2
 ip tcp ceiling 6000
 ip rip activate
 ip rip merge on
 ppp ipcp compress off
 ip icmp discovery enif0 off
 bridge mode 1
 sys quick enable
 sys wdog sw on
```

- Default settings by CI-commands

- ras > wlan filter outgoing generic 4
-
- ras > sys firewall ignore triangle all on
-
- ras > wlan active 1
-
- ras > ip anyip status

```
Any IP turn on ...
Aging Timer is 300 seconds
The max number of any IP entry is 30
Total 0 Any IP entry in arp table
It allow the connection between any ip client.
```

- ras> wan atm vc disp

```
(1) Configure Buffer

(2) RemoteNode (Read Only)

 RN VPI   VCI | RN VPI   VCI | RN VPI   VCI | RN VPI   VCI |
```

```
-------------------------------------------------------------

  1   8    35 |  2   0     0 |  3   0     0 |  4   0     0 |

  5   0     0 |  6   0     0 |  7   0     0 |  8   0     0 |

(3) VC Hunt Table: (User setting)

 Flags: Active(1)

 RN VPI   VCI serv| RN VPI   VCI serv| RN VPI   VCI serv| RN VPI  VCI serv

-------------------------------------------------------------

  1   0  33   3fH|  1   0  35   3fH|  1   1  35   3fH|  1   8  32   3fH|

  1   0 101   3fH|  1   0  50   3fH|  1   0  32   3fH|  1  14  24   3fH|

  0   0   0    0H|  0   0   0    0H|

ras > bm defaultClassBw
Default class bandwidth in MBM Wizard: 10 kbps

ras> ip url general disp
General:
    Enable
Web Control:
    Disable
Resrict Web Feature:
    ActiveX: Forward
    Java   : Forward
    Cookie : Forward
    Proxy  : Forward
exemptTypeFlag:
    CYBER_NOT_POLICY_ALL: disable
    CYBER_NOT_POLICY_INCLUDE: disable
    CYBER_NOT_POLICY_EXCLUDE: disable
Exempt Range:
    start IP        ----        end   IP
    ----------------------------------------
    Filter Not Always On
Time of Day:
    block from 00:00 to 00:00

ras> sys regurl
Current URL = www.myzyxel.com/myzyxel

ras> sys pack di

---- AntiVirus Packet Scan State ----

  Registration:No

  Active: No

  HTTP: No

  FTP: No
```

```
EMail: No
Automatic online update schedule: none
Default action when session overflow: Forward Packet
Scan Engine Version: 0.18
Scan Pattern Version: 200411301836
Licence Expire Date : 1970/01/01
```

- Default settings on Web/GUI

Firewall - Default Policy

☑ Enable Firewall

☑ Allow Asymmetrical Route

CAUTION: When Allow Asymmetrical Route is checked, all LAN to LAN, WAN to WAN and DMZ to DMZ packets will bypass the Firewall check.

Packet Direction	Default Action	Log
LAN to LAN / Router	○ Block ◉ Forward	☐
LAN to WAN	○ Block ◉ Forward	☑
LAN to DMZ	○ Block ◉ Forward	☑
WAN to LAN	◉ Block ○ Forward	☑
WAN to WAN / Router	◉ Block ○ Forward	☑
WAN to DMZ	○ Block ◉ Forward	☑
DMZ to LAN	◉ Block ○ Forward	☑
DMZ to WAN	○ Block ◉ Forward	☑
DMZ to DMZ / Router	◉ Block ○ Forward	☑

Back Apply Cancel

Firewall Rules Storage Space in Use (2%)

0% 100%

Packet Direction WAN to WAN / Router

Default Policy: Block, Log

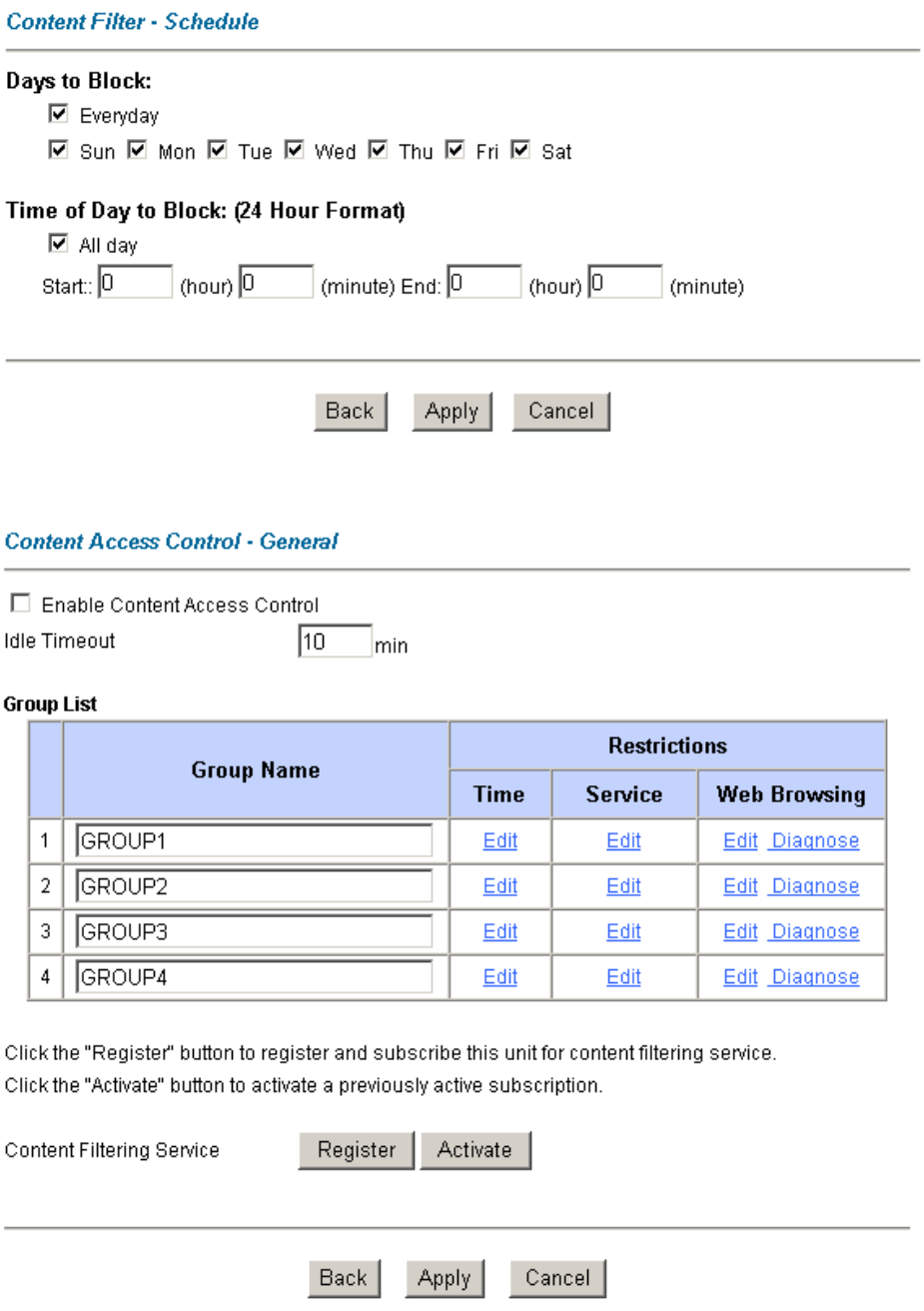
Rule	Active	Source IP	Destination IP	Service	Action	Schedule	Log	Alert
1	Y	Any	Any	BOOTP_CLIENT(UDP:68)	Forward	No	Disable	No

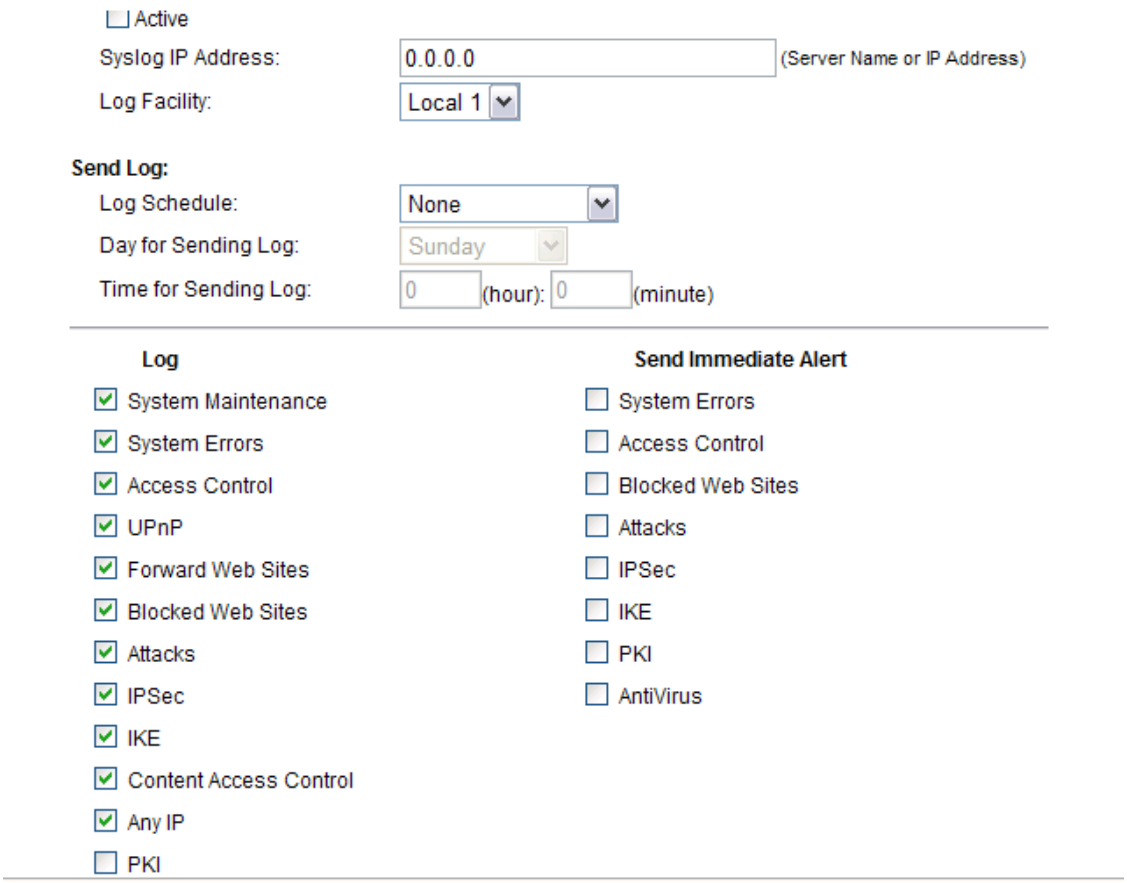
BOOTP_CLIENT(UDP:68)
IKE(UDP:500)

Create Rule: Insert new rule before rule number 1 Insert Append

Rules Reorder: Move rule number 0 to rule number 0 Move

Back Apply Cancel


Content Filter - Schedule
Days to Block:
Everyday
Sun Mon Tue Wed Thu Fri Sat
Time of Day to Block: (24 Hour Format)
All day
Start:: 0 (hour) 0 (minute) End: 0 (hour) 0 (minute)
Back
Apply
Cancel
Content Access Control - General
Enable Content Access Control
Idle Timeout 10 min
Group List
Group Name
Restrictions
Time
Service
Web Browsing
1 GROUP1 Edit Edit Edit Diagnose
2 GROUP2 Edit Edit Edit Diagnose
3 GROUP3 Edit Edit Edit Diagnose
4 GROUP4 Edit Edit Edit Diagnose
Click the "Register" button to register and subscribe this unit for content filtering service.
Click the "Activate" button to activate a previously active subscription.
Content Filtering Service
Register
Activate
Back
Apply
Cancel


Active
Syslog IP Address:
0.0.0.0
(Server Name or IP Address)
Log Facility:
Local 1
Send Log:
Log Schedule:
None
Day for Sending Log:
Sunday
Time for Sending Log:
0
(hour):
0
(minute)
Log
Send Immediate Alert
System Maintenance
System Errors
Access Control
UPnP
Forward Web Sites
Blocked Web Sites
Attacks
IPSec
IKE
Content Access Control
Any IP
PKI
System Errors
Access Control
Blocked Web Sites
Attacks
IPSec
IKE
PKI
AntiVirus