ZyXEL

Firmware Release Note

P964 APR

Release 3.60(YD.19)C0

Date: **Nov 8, 2005**

Author: **Jues Liu**

ZyXEL P964APR Standard Version

release 3.60(YD.19)C0

Release Note

Date: Nov 8, 2005

Supported Platforms：

ZyXEL P964APR

Versions:

F/W : 360YD19C0.img V3.60.19 | 11/08/2005 18:53:50 1,591,188 bytes

Notes:

1. An “arpFlush” must be added to the last line of VSIF configuration file.
2. Before using “remote_manage” and “pfwd_enable” commands on CLI, users must check the DHCP server and DHCP Pool under the same SUBNET.
3. DHCP server only supports a temporary IP for DHCP clients for diagnostic purpose when P964 can not get on line.
4. Reset to factory button can only work when cable is off line and scanning down stream.
5. At the network authentication mode of “802.1x”, P964APR don’t support user to set the PassPhrase key or manual keys.
6. When user want to modify the mac restrict table, P964APR doesn’t difference if the mac was added before or not, and doesn’t have any CLI command to delete it from mac restrict table. If user wants to delete it from this table, the following command can be used.

   wl_mac n 00:00:00:00:00:00

   “n” is the index number of the mac address you want to remove from the mac restrict table.

Features:

Modification in 3.60(YD.19)B2 | 11/4/2005

1. [BUG FIXED]
   Fix nat11 can't ping remote pc but can ftp.

2. [BUG FIXED]
   Fix after setting static_ip2 and static_ip3, static_ip can't be accessed.

Modification in 3.60(YD.19)B1 | 10/27/2005

3. [BUG FIXED]
   Fix lost one-to-one NAT, remote manage flag when upgrade from old versions.

4. [BUG FIXED]
   Fix Radius UDP port 1030 attack causing modem crash.

5. [BUG FIXED]
   Change back the SNMP access behavior as 3.60(YD.17)C0 and previous versions.

6. [CHANGE]
   Remove snmp_set command.

Modification in 3.60(YD.18)C2 | 10/07/2005

1. [BUG FIXED]
   Modify code for upgrade from any old version of image and keep setting intact.

Modification in 3.60(YD.18)C1 | 9/15/2005

1. [BUG FIXED]
   Modify code for upgrade from 3.60(YD.17)C0. There will be a side effect happened when users set SNMP IP and community for security. Upgrade will reset the SNMP security to factory setting. Users will need to set it again after upgrade. Or users could use "cmd_tftp" command to backup configuration and restore it after upgrade.

Modification in 3.60(YD.18)B8 | 8/19/2005

1. [ENHANCE]
   Add the Shared key Authentication in WLAN security page.
2. [ENHANCE]
   Modified the CLI command "wl_auth". When user want to change the network authentication mode to "disable", the SHARED KEY AUTHENTICATION can be selected to "optional" or "shared_key" mode.
3. [CHANGE]
   Modified the WLAN basic page. The channel can be selected by user.
4. [CHANGE]
   Modified the WLAN security page. Add an confirm message for user to submit

the new NETWORK AUTHENTICATION mode. When user select a new network authentication mode, there is a confirmation window for user to confirm new network authentication.

5. [BUG FIXED]
   When user changes the SSID from web, the country code will be change at the same time.
6. [BUG FIXED]
   The CLI command "cmd_show" will show some security key unnecessarily, like the manual keys of wireless data encryption.
7. [BUG FIXED]
   The WLAN security web page didn't show actually what kind of setting of wep key. In other word, the security page can't differentiate that the current data encryption key is PassPhrase or munual keys.
8. [BUG FIXED]
   The CLI command "wl_auth" didn't hide PassPhrase key.
9. [BUG FIXED]
   At the WPA-PSK network authentication mode, the user can't set WPA Preshared Key immediately. User must try again to set the WPA Preshared Key and it take effect at this time.
10. [BUG FIXED]
    When user want change the address of RADIUS server, it didn't take effect once. User must try again to set the address of RADIDUS server.
11. [BUG FIXED]
    When user change the setting of Network Type, the country code will be changed at the same time.
12. [BUG FIXED]
    When user enable or disable the wireless interface, the country code will be changed at the same time.

Modification in 3.60(YD.18)B7 | 8/10/2005

1. [ENHANCE]
   Add CLI command "inetshow" to display current inet information.
2. [BUG FIXED]
   When data encryption mode is wep64, the wl_auth command didn't show the all settings of wireless authentication.
3. [BUG FIXED]
   PassPhrase key and manual keys can't be set simultaneously. In other words, the manual keys is generating from passphrase or direct input manual keys.
4. [BUG FIXED]
   The CLI command "wl_show" and "wl_auth" always show the PassPhrase key we set before and will make user confuse about how the manual keys generated.
5. [ENHANCE]
   In wireless security web page, we add a check box. If the check box is enabled, the user can generate manual keys from passphrase key. Else, manual keys must be input one by one.
6. [BUG FIXED]
   When network authentication is changed to "disable" mode, the shared key authentication will be changed to "optional" automatically.
7. [CHANGE]
   Remove the Shared Key Authentication function on the security page of

wireless.

8. [ENCHANCE]
   When use the “wl_auth” CLI command, the manual keys can enter the character string as key.

Modification in 3.60(YD.18)B6 | 7/12/2005

1. [BUG FIXED]
   If we set trigger range only <UDP protocol> for port trig forwarding, but TCP packet can also pass through the port range too.
2. [CHANGE]
   Remove the Filter Proxy function.

Modification in 3.60(YD.18)B5 | 7/11/2005

1. [BUG FIXED]
   There is a wrong example in “dload” command example.
2. [BUG FIXED]
   Public manage IP can’t be accessed by LAN and WAN side.
3. [BUG FIXED]
   The wl_show command don’t show the correct MAC address of access point.
4. [BUG FIXED]
   In the webpage, the current system time wrong.
5. [BUG FIXED]
   In the Wireless – Basic webpage, the country code and channel is opened to user use.
6. [BUG FIXED]
   In the Firewall – web Filter webpage, Filter JavaApplets fail.
7. [BUG FIXED]
   In the Firewall – web Filter webpage, Filter ActiveX fail.
8. [BUG FIXED]
   In the Firewall – web Filter webpage, Filter Popup Windows fail.
9. [BUG FIXED]
   In the Firewall – web Filter webpage, Block Framented IP Packets fail.
10. [BUG FIXED]
    In the Firewall – web Filter webpage, PortScan Detection fail.
11. [CHANGE]
    Remove the Trust Computer function.

Modification in 3.60(YD.18)B4 | 7/6/2005

1. [BUG FIXED]
   When user telnet to the cable modem, there is no command prompt.
2. [BUG FIXED]
   The show_conf command will show the HTTP user name and password.
3. [BUG FIXED]
   “dsdiag” command show the wrong unit of power level.

4. [BUG FIXED]
   "monitor" command show the wrong unit of power level.
5. [BUG FIXED]
   In the Firewall – ToD Filter page, the block function do not work.

Modification in 3.60(YD.18)B0 | 6/24/2005

1. [BUG FIXED]
   Remote management fails in "Public DHCP mode".
2. [BUG FIXED]
   DHCP commands are not necessary for "Basic static IP mode".
3. [BUG FIXED]
   RIP commands are not necessary when RIP is disabled.
4. [ENHANCE]
   Change the prompt to match the host name.
5. [ENHANCE]
   Extended TACACS string length to 32 bytes
6. [ENHANCE]
   Add firewall enable CLI commands and related web pages.
7. [ENHANCE]
   Speed up through put as twice as before.

Modification in 3.60(YD.17) | 6/09/2005

8. [BUG FIXED]
   Eliminate verbose debugging messages. "monitor" can benefit from it.
9. [BUG FIXED]
   Modify "defaults" command reset button to real factory defaults. It includes pflt, pfwd, rip, passthrough, dns, and scan band.
10. [BUG FIXED]
    Fix "pfwd_enable", "pfwd_disable", "pfwd_show" commands defect.
11. [BUG FIXED]
    "pflt_enable", "pflt_disable", "pflt_show" commands defect.
12. [BUG FIXED]
    "routeShow" command now will show static route.
13. [BUG FIXED]
    Fix "sysObjectID" to ZyXEL MIB code.

14. [BUG FIXED]
    Fix 3.60.15 and 3.60.16 “ip_blk”, “trust_ip” nonvol location error.

Change List:

Functional Changes in 3.60.16

(1) Fix Cisco GRE VPN interoperate issue.

(2) Modify Telnet messages when users are rejected to connect to. The new message is “Connection Refused…”

(3) Add “trust_add”, “trust_clear”, and “trust_show” commands. “trust_add” specify a specific IP subnet which a host can TELNET to a P964 in the subnet. “trust_clear” clears all trusted IP subnets. And “trust_show” shows all trusted IP subnets.

(4) Add “arpFlush” to clear the ARP table.

Functional Changes in 3.60.15

(5) Base on P964 CR firmware release 3.60.14 to add/fix the following functions

(6) Add “ipblk_add”, “ipblk_clear”, and “ipblk_show” commands. “ipblk_add” will block a specific static IP from access Internet. “ipblk_clear” will clear all blocked IPs. And “ipblk_show” will show all blocked IPs.

(7) Change the messages, “A CPE (Ethernet) is attempting to hijack the MAC : address for IP Stack1! Thwarting the villian's malicious plot...”, to as follows:

“An IP/MAC conflict has been detected. Please check the IP address of any connected device and make sure it is not using an IP address of another connected device.

Functional Changes in 3.60.14

(8) Modify the RIP packet broadcast/multicast to WAN port, Cable side, only. This fix prevents

RIP packet flooding to LAN port, Ethernet side.

Functional Changes in 3.60.13

(9) Base on P964CR firmware release 3.60.11 to add/fix the following functions

(10) Fix “wan_ip” by adding a third gateway parameter and enable RIP. Although RIP is enabled it is not necessary for CMTS to enable RIP. Besides users can lengthen the RIP report interval up to 65535 seconds to avoid network traffic. “wan_ip” functions the same as P944S’s WAN static mode.

(11) Add “dhcp_enable” an extra lease time parameter. User can assign a dhcp server lease time for CPEs range from 3600 to 65535 seconds. For backward compatibility issues this parameter is optional and its default value is 3600 seconds.

(12) Add “hostname” command to assign P964 a hostname, its length is up to 254 bytes. And tie it with SNMP MIB “sys.Name”.

(13) Add CPU usage and Cable/LAN TX/RX information in “monitor” command.

(14) Add VSIF function.

(15) Fix ARP packet flooding.

(16) Add accessing SNMP from trusted IP and correct community string.

(17) Always enable hardware reset function. Cancel “fac_enable” command.

Functional Changes in 3.60.12

(18) Base on P964CR firmware release 3.60.11 to add/fix the following functions

(19) Fix “wan_ip” by adding a third gateway parameter and enable RIP. Although RIP is enabled it is not necessary for CMTS to enable RIP. Besides users can lengthen the RIP report interval up to 65535 seconds to avoid network traffic. “wan_ip” functions the same as P944S’s WAN static mode.

(20) Add “dhcp_enable” an extra lease time parameter. User can assign a dhcp server lease time for CPEs range from 3600 to 65535 seconds. For backward compatibility issues this parameter is optional and its default value is 3600 seconds.

(21) Add “hostname” command to assign P964 a hostname, its length is up to 254 bytes.

Functional Changes in 3.60.11

(22) Base on P964CR firmware release 3.60.10 to add/fix the following functions

(23) Fix ARP interoperability issue with VSG1000, CISCO PIX and other routers.

(24) Fix pressing reset button to reset to factory default without customers’ proprietary information. To use this function, users should follow the following procedure: unplug the HFC then power on P964CR. Press the reset button and hold at least 10 seconds when P964CR’s CABLE LED starting slow flash (2 seconds interval). After P964CR rebooted, the P964CR will be back to factory default. The “fac_reset” will also reset to be disabled.

(25) Add “cmd_show” to show commands that set the current configuration.

(26) Add “rip2_broadcast” command to support broadcast and RIP report time interval.

(27) Add “cmd_tftp” to tftp commands that set the current configuration to a tftp server.

(28) Add “man_ip” to configure a static IP for management, e.g. TELNET.

(29) Add “tel_conf” to accept telnet from WAN, LAN or BOTH.

(30) Add “tel_port” to configure TELNET servers’ listening port.

(31) Add “tel_ip” to accept only this IP to connect TELNET server.

(32) Re-involve the “scan” plan functions.

(33) Add one to one NAT function, including commands “nat11”, “nat_add”, “nat_remove” and “nat_show”.

(34) Add static route, include a command “route_add”. Obsolete commands “static_ip2”

“static_ip3”, but there is no harm to use them.

(35) Add “wan_ip” command for some customers who use only one static IP with RIP disabled.

(36) Fix “ping” now cannot work properly in windows/Linux TELNET client sessions.

Functional Changes in 3.60.10

(37) Base on P964CR firmware release 3.60.05r1 to add/fix the following functions

(38) Rip key string length changes from 16 bytes to 24 bytes.

(39) Hold Reset button exceed 10 secodes will reset user name and password back to factory default.

This function is disabled again from 3.60.05 to 3.60.10.

(40) Add bootdelay commands which make P964CR delay 15 seconds when booting.

(41) Base on P964CR firmware release 3.60.05(20040108) to add/fix the following functions

(42) Add a system status monitor function. Please refer to the operators’ guide.

(43) Add a fac_reset command. Operators can enable/disable reset button function.

(44) Add WAN-DATA interface TELNET support when P964CR is in IP SHARING mode.

(45) Add port forwarding commands, which does same things as web page.

1. pfwd_enable
2. pfwd_disable

3. pfwd_show

(46) Add port filtering commands, which does same things as web page.

1. pflt_enable
2. pflt_disable
3. pflt_show

(47) Do not show the RIP/TACACS key string and TELNET password when show_conf

(48) Add static IP support for SNMP

(49) Fix RF reading problem

(50) Move the web service to port 8080

(51) Fix LED behavior issue

(52) Fix Mutex error

Internal Information:

Versions:

F/W : 360YD19B1.bin V3.60.19 | 10/27/2005 18:45:40 1,588,782 bytes

Bootbase Version : V2.1.5 | 3/12/2004 10:27:36 32,282 bytes

Known Issues

1. The DATA LED won't flash if it only exists up stream packets.
2. Down stream power reading error. The value maybe slight over DOCSIS 2.0 specification.
3. Users can not TELNET to WAN-DATA IP from WAN side when in IP sharing mode.
4. The "static IP support for SNMP" function could not support accessing from LAN to this static IP.
5. Users can not ping the static IP of P964 when packet sizes are greater than 1472.
6. LAN IP can not access web through 192.168.100.1 and CM IP
7. WAN IP can not access web through CM IP
8. WAN IP can not access web through static IP when "Public DHCP configuration" and "remote_manage" is set.
9. Use "cmd_show" or "cmd_tftp" to get the command list then execute it will display some error message on console, but it does affect the result.
10. "tel_conf" can not control the incoming connection from LAN side to CM IP.
11. "man_ip" is only effective for WAN side access. And it only effective for TFTP, TELNET, TACACS, and SNMP.
12. The hardware reset button is not workable when "monitor" command is running.
13. The ptrig_disable and pfwd_disable commands can't reset the settings to defaults value.
14. "hostshow" command show some information that is unnecessary.
15. When telnet to CM, the command prompt will often show unnecessary message.

16. Static_ip2 and Static_ip3 can't be accessed from LAN or WAN side.
17. When someone try to scan the CM's port, the local log will show the message but there isn't in the syslog server.
18. The Filter Cookies don't work normally when contact with www.micorsoft.com web site
19. Remote pc can't use SNMP access public ip (10.13.41.1).remote pc can't use Telnet access public ip (10.13.41.1).
20. When wan_ip remote pc can't use Browser , SNMP , Telnet access
21. WAN PC and LAN PC can connect to CM web pages when web_enable false.
22. Radius Server setting can't connect port 1030.
23. When change Data Encryption on web page (wireless security) would be error message.

Notes

1. There are some private SNMP MIB is defined as Broadcom's OID 4413.

Modification

NA

Manufactory Data in Bootbase

NA

Appendix 1: CLI Command List

Note: 802.11 HAL commands and wl_* commands and only valid in P-964APR.

Command Class List Table		
Root	802.11 HAL	Heap Manager
Cable Home	CM HAL	Docsis Control
Ethernet HAL	Event Log	Forwarder
IP HAL	Message Log	Ping Helper
Propane Control	Remote Access	SNMP
USB HAL		

Root commands Home

Command		Description
add_passthrough	[index] [MAC address]	Add a MAC address which will not be NATed or Routed but pass through the CM directly.
arpflush		Clear the current ARP table information
arpshow		Displays current arp table information.
bootdelay	[true|false]	In some environment the CMTS can not sense that CM is rebooting. Use this command to let CMTS has much more time to know that CM is rebooting.
cmd_show		Show current setting command
cmd_tftp		Backup current setting commands to tftp server
defaults		This command is to reset the configuration to default. The P964CR must be rebooted to make it effective.
del_passthrough	[Passthrough Index{1..20}]	Delete an entry which was added by "add_passthrough" command.
dhcp_enable	[true|false] [Lease time{3600..65535}]	This command is to enable or disable the LAN DHCP service and DHCP lease time in seconds, from 3600 to65535, for CPEs. The LeaseTime parameter is optional and its default value is 3600 seconds.
dhcp_pool	[DhcpStart] [DhcpSize{1..65536}]	Set LAN DHCP IP range starting from [DhcpStartAddress]. The pool size is [IpSize] IpSize: IpSize number, range between 1..65535.
dhcp_server	[DhcpServer] [DhcpNetmask]	Set LAN DHCP server IP address and its net mask. It is also the LAN IP address. It can be set even when DHCP server is disabled.
dns_server	[DnsServer1] [DnsServer2] [DnsServer3]	This command is to setup the DNS server IP addresses. The IP address will be included in the DHCP reply to pc.
exit		Stop showing system status monitor.
hostname	[HostName{0..254}]	Set static Wan hostname
hostshow		Display current host table.
icmpshow		Display current icmp stat information.
ifshow		Displays current interface information.
ip_sharing	[true|false]	Enable/disable IP sharing mode. If disabled, the P964CR will not assign IP address for its WAN interface. This value will be true when "router_enable" is setting true. For Time Warner static IP services, this must be set to false.
ipblk_add	[Index{1..5}] [BlockIP]	Add IP block.
ipblk_clear		Clear IP Block Table

ipblk_show		Show IP Block Table
ipshow		Display current ip stat information.
load_config	[IpAddress] [Filename]	This command is to load a text based configuration from a TFTP server. After loaded, the commands inside the file will be executed line by line. This can be used for easy configuration.
logout		For Telnet clients, this lets the user log out cleanly.
man_ip	[ManageIP]	Set a static public for management the P964 router.
mbufshow		Display current mbuf allocation
memshow		Display current memory allocation.
monitor		Show system status monitor.
nat11	[true|false]	This command is to enable/disable the 1 to 1 NAT
nat_add	[Private IP] [Public IP]	This command sets the 1 to 1 NAT mapping
nat_remove		This command removes all 1 to 1 NAT mapping entries.
nat_show		This command shows all 1 to 1 NAT mapping entries.
pflt_disable	[Entry{0..10}]	Disable port filter entry. Entry = 1 to 10
pflt_enable	[Entry{0..10}] [Start] [Port] [End] [Port] [Protocol]	Enable port filter entry. Entry = 1 to 10
pflt_show		Show port filter content.
pfwd_disable	[Entry]	Disable port forwarding entry.
pfwd_enable	[Entry] [IpAddress] [Start] [Port] [End] [Port] [Protocol]	Enable port forwarding entry.
pfwd_show		Show port forwarding table content.
ping	[IpAddress]	Ping the specified target IP address, sending 3 64-byte packets, and waiting up 5 seconds for a response. This is a basic 'standard' ping. For more option or control over ping parameters and behavior, you will need to go to the ping command table(cd pinghelper). In order for this to work, the CM must either have successfully completed DHCP, or must otherwise have been configured with a valid IP address. Note that this command causes the ping option to be reset to their default state. This may be disabled if the platform doesn't provide an implementation of ping.
ptrig_disable	[Entry{1..10}]	Disable trigger entry. Entry = 1 to 10.
ptrig_enable	[Entry{1..10}] [Start TrigPort{0..65534}] [End TrigPort{0..65534}] [Start Port{0..65}]	Enable trigger entry. Entry = 1 to 10. Start TrigPort = Set start TrigPort number End TrigPort = set end TrigPort number Sart Port = start port number End Port = End port number Protocol = 1→TCP, 2→UDP, 3→BOTH.
ptrig_show		Show trigger table content.
remote_manage	[true|false]	This command is used to enable or disable remote access to the Prestige web interface through port 8080.
reset		This command is to resets the system (warm boot). The hardware reset line is triggered, causing the application to be reloaded from scratch. On host-based app simulators, this will cause the application to exit.
rip2_broadcast	[BroadcastFlag]	Set sending RIP2 packet broadcast(true) or

	[TimeInterval{30..65535}]	multicast(false)
rip2_debug	[true|false]	This command is to enable/disable the RIP debug message. If enabled, the console will display RIP broadcast massage every 30 seconds.
rip2_keyid	[KeyId{0..4294967294}]	This command is to set the RIP2 key id. The key-id number can be in range between 0..4294967294.
rip2_keystr	[KeyString{24}]	This command is to set the RIP2 key string. The parameter key-string can not exceed 24 characters.
rip2_md5	[true|false]	This command is to enable/disable the RIP2 MD5 feature.
rip_enable	[true|false]	This command is to enable/disable the RIP2 routing protocol.
route_add	[Index{1..2}] [NetworkIP] [NetMask Gateway]	Add static route to cable router. Sometimes we have subnets in LAN and need a function to route packets. We limit the number of subnets to 2, Index=1 or Index = 2.
router_enable	[true|false]	Enables/disables the route mode. If enabled, the P964CR operates in router mode, otherwise bridge mode.
routeshow		Display current routing information.
run_app		If the application was stopped at the console (either via keypress or via non-vol setting that automatically stopped it), then this command will allow it to start running. This command is not available if the application is already running.
save		This command is to write the configuration into Flash ROM.
scan_band	[Band{0..31}]	The command is to set the predefined scanning frequency plan via the hexadecimal bitmap. 0x01: FREQ_PLAN_EIA 0x02: FREQ_PLAN_HRC 0x04: FREQ_PLAN_EURO 0x08: FREQ_PLAN_OIRT 0x10: FREQ_PLAN_BG
scan_set	[index{0..4}] [Band{1..5}] [start] [end] [freq_offset(for EURO)]	This command sets the predefined frequency range in a specified frequency plan. The Prestige supports 5 sets of predefined frequency ranges indexing from 0 to 4.
scan_set_clear		Clear the predefined frequency scanning set.
scan_show		Scan show
scan_stop		Stop downstream scan
shell		Causes the application to jump to vxwork shell
show_conf		This command is to show the current configuration.
snmp_set	[IP] [Community]	This command sets trust SNMP IP and community string which can connect to the P964's SNMP agent. The default values are 0.0.0.0 and "public". The IP 0.0.0.0 represents no limitation.
static_ip	[IpAddress] [NetMask]	Setup the static IP and netmask. It is used for setting a public IP subnet on P964CR
static_ip2	[IpAddress] [NetMask]	Setup the second static IP and netmask. It is used for setting the second public IP subnet on P964CR
static_ip3	[IpAddress] [NetMask]	Setup the third static IP and netmask. It is used for setting the third public IP subnet on P964CR
tac_enable	[true | false]	This command is used to disable or enable the

		TACACS authentication service.
tac_ip	[TACACS SourceIpType]	This command is used to set the TACACS source Ip Type value.
tac_key	[TACACS Keystring]	This command is used to set the TACACS MD5 key string value. Of cause it is only needed when MD5 encryption is used.
tac_md5	[true|false]	This command is used to disable or enable the TACACS authentication service with MD5 encryption.
tac_server	[IpAddress] [IpAddress]	This command setup TACACS servers. The primary server is necessary and the secondary is optional
tcpshow		Display current tcp stat information
tel_conf	[setting]	This command is to set telnet to accept connection request from LAN, WAN, or BOTH.
tel_ip	[IpAddress]	This command is to set a IP which TELNET server can trust.
tel_port	[Port]	This command is to set telnet to listen on a specific port.
telnet_pass	[Password]	This command is to set telnet password.
telnet_user	[Username]	This command is to set the telnet user name.
trust_add	[Index{1..5}] [TrustedIpNet] [TrustedIpMsk]	Add trusted TELNET IP subnet
trust_clear		Clear trusted TELNET IP subnet table.
trust_show		Show trusted TELNET IP subnet table.
udpshow		Display current udp stat information
version		Display the current firmware version.
wan_ip	[IPAddress NetMask Gateway]	Setup the static wan IP, netmask, and gateway.
web_admin_id	[WebAdminId]	This command is to set the user name for Administrator web.
web_admin_password	[WebAdminPass]	This command is to set the password for Administrator web.
web_enable	[true|false]	This command is used to enable or disable the Web interface.
web_user	[WebUserId] [WebUserPass]	This command is to set the user name and password for User web page.
wl_auth	[[[disable] [WEP64|WEP128] [Pass Phrase|Key Index(1..4)] [Key1 Key2 Key3 Key4]] | [[802.1x] [Radius Server IP] [Port(0..65535)] [Key]] | [[WPA] [Radius Server IP] [Port] [Key] [Re-Key Interval(0..65535)] [AES|TKIP]] | [[WPA-PSK] [WPA Pre-Shared Key] [Re-Key Interval] [AES|TKIP]]]	Enable wireless LAN authentication.
wl_beacon	[Number{0..65535}]	Sets the beacon interval (0-65535 ms).
wl_country	[country] [Channel]	Set Country code and it associated channel. The following is the wireless LAN channel defined by countries country channel worldwide 1~13 Thailand 1~14 Israel 5~7 Jordan 10~13 China 1~13 Japan 1~14 USA 1~11 Europe 1~13 All channel 1~14

wl_dtim	[Number{1..255}]	Sets the DTIM interval (1-255).
wl_enable	[true|false]	Enable wireless LAN interface or not.
wl_frag	[Number{256..2346}]	Sets the fragmentation threshold (256-2346 bytes).
wl_mac	StationNum{1..16} [MacAddress]	StationNum{1..16} [MacAddress]
wl_mode	[compatibility|gonly|performance]	Sets the mode of the 54g interface.
wl_power	[Number{25..100}]	Sets the output power level(25, 50, 75, 100)
wl_protect	[off|auto]	Sets 54g Protection mode
wl_rate	[Number{0..54000}]	Sets rate control
wl_restrict	[disabled|allow|deny]	Sets behavior of MAC table
wl_rts	[Number{0..3000}]	Sets the RTS threshold (0-3000).
wl_show		Show the Settings of Wireless.
wl_ssid	[ssid]	This command is to set wireless LAN SSID. The maximum length of SSID is 32 bytes.
wl_type	[open|closed]	Set P964APR to a closed network true, if you do not want to send SSID on air.
zone	[bitmask{0xffff}]	Prints or sets the hal debug zones; this determines what debug messages will be display by HAL driver. This bit correspond to the HAL debug zones: 0x0001 – INIt 0x0002 – TEST1 0x0004 – TEST2 0x0008 –TEST3 0x0010 – TEST4 0x0020 – TEST5 0x0040 – TEST6 0x0080 – BPI 0x0100 – DOWNSTREAM 0x0200 – UPSTREAM 0x0400 – TUNNER 0x0800 – RANGING 0x1000 – TESTSRAM 0x2000 – TESTREG 0x4000 – WARNING 0x8000 – ERROR

802.11 Hal relation

Home

Command		Description
antenna	[AntSelect]	Causes the 802.11 HAL to set/display its current antenna setting.
bssid		Causes the 802.11 HAL to display the current BSSID address.
channel	[ChanNum]	Causes the 802.11 HAL to set/display its current channel setting.
clr_counts		Causes the 802.11 HAL to clear driver maintained statistics.
csenable	[CsEn]	Causes the 802.11 HAL to set/display the carrier suppression transmit setting.
hal_show		Causes the 802.11 HAL to display its internal state.
Regdomain		Causes the 802.11 HAL to display the current regulatory domain.
Rxenable	[RxEn]	Causes the 802.11 HAL to set/display the force radio receive only setting. 0 = Stop RX only test 1 = Start RX only test
Rxfer		Causes the 802.11 HAL to display the current FER counter.
show		Causes the HalIf object to display its state.
ssid		Causes the 802.11 HAL to display its current SSID string.
txenable	[TxEn] [Rate]	Causes the 802.11 HAL to set/display the force radio transmit setting. First Parameter: 0 = CW Transmit Test 1 = EVM Transmit Test 2 = Turn Off all Tests Second parameter (for EVM only): test rate in MBits (1, 2, 5.5, 11).
txpwrlevel	[TxPower]	Causes the 802.11 HAL to set/display the current transmit power level.
wl	[CmdLine{31}]	Sends commands to the 802.11 diagnostic and manufacturing utility.

Heap Manager

Home

Command		Description
bcheck		Runs a bounds check in the heap manager (if compiled in).
bcheck_crash	[true|false]	Sets the behavior when an on-the-fly bounds checking error is detected. Turning this on will cause the offending thread to crash after we print relevant information.
bcheck_enable	[true|false]	Turns on-the-fly bounds checking on or off in the heap manager (if compiled in). When this is on, we will validate pointers, seed values, and other heap state during each alloc and free. When off, you must run bcheck manually to detect errors.
last_error		Displays the last error that was detected by the heap manager.
maxAlloc		Displays the maximum number of bytes that can currently be allocated in a single call to malloc.

		This takes into account all of the overhead for node tracking and bounds checking, as well as the current fragmentation state of the heap.
memShow		Displays summary of available heap.
stats		Displays detailed heap manager counters and statistics.
walk		Displays all of the free memory blocks.
walk_alloc		Displays all of the allocated memory blocks. WARNING: This can print a LOT of information!

Cable Home Home

Command		Description
arp_show		Displays the current ARP table information.
arppacket_show		Displays the current ARP Packet information.
capt_show		Displays the current CAPT (Passthrough) contents.
debug_kerb	[DebugLevel{0..3360}]	Sets the Kerberos debug level where level is an int from 0 (silent) to 9 (verbose).
dhcps_add_lease		Adds a Dhcp server lease associating client id with Ip address.
dhcps_remove_lease		Removes a Dhcp server lease, the user will be prompted for a client id
dhcps_show		Displays the current DHCP server information.
dns_debug	[number{0..1}]	Enables/Disables DNS debug information.
dns_show		Displays current DNS information.
fwr_show		Displays current firewall ruleset.
kerb_test	[Realm] [KDC IP Addr] [ProvServer IP Addr]	Start kerberos for SNMP (debug).
nat_show		Displays the current NAT info.
reload_lan_config		This reconfigures the LAN side using the current non-vol settings.
reload_routedsubnet		This reconfigures the routed subnets using the current non-vol settings.
rip_show		Displays current RIP (Routing Information Protocol) settings.
route_entry	[-d]	Prompts user to add or remove a route.
routed_subnet_show		Displays current Routed Subnet settings.
upnp_show		Displays current UPnP (Universal Plug-n-Plug) settings.
usfs_show		Displays the current USFS table contents.
wandata_show		Displays the current Wan Data Address table contents.

CM Hal Home

Command		Description
bcmalloc_show	[-c]	Displays a snapshot of the current BcmAlloc memory pool statistics. If -c is specified, then the counters are also cleared.
bist_test		Runs the CM MAC h/w BIST Tests.
cache_test		Tests cache flush/invalidate performance.
change	[-s] [-c] cos|cls|phs|flow [index]	Changes information about Classifiers, Service Flows, PHS, DOCSIS 1.0 Class of Service, and other objects in the system. cos -- Selects the DOCSIS 1.0 Class of Service object. cls -- Selects Classifiers. phs -- Selects PHS Rules. flow -- Selects Service Flows.

		-s -- Changes the settings for the selected object (you will beprompted for the values). -c -- Clears the counters for the selected object. index -- Selects a specific instance of the object type. The index is shown when you list the objects with the 'show' command. You must specify one of each of the object type and -s or -c parameters; there are no defaults. The index is optional; if missing, all instances are changed.
counters		Causes the CM HAL to print the hardware counter values.
cpe_add	[MacAddress]	Adds the specified MAC address to the CPE learning table. An SNMP MIB item is created for it, and it is added to the downstream data CAM. The address s added unassociated, since there isn't a good way to specify the HalIf that t should be associated with. The assoc will be locked in on the first acket that goes upstream.
cpe_del	[MacAddress] [index{-1..2147483647}]	Removes the CPE with the specified MAC address/table index from the learning able. The SNMP MIB item is also deleted. The index is 0-based, as printed y cpe_print. If you specify -1, all will be removed.
cpe_max	[max Cpe]	Sets/gets the max CPEs that can be added to the learning table.
cpe_print		Prints the CPE learning table.
ds_state		Prints the state of the DOCSIS downstream (frequency, modulation, etc.).
hal_show	[-l] [-s] [-c] [flow|descr|queue|all] [index]	Displays information about the CM DOCSIS HAL internal state: Service Flows, MA descriptors, Counters, HW/SW Queues. These are what the parameters mean: flow -- Selects Upstream Service Flow info descr -- Selects DMA Descriptor info queue -- Selects Hardware/Software Queue info -l -- lists the selected object(s) -s -- shows settings for the selected object(s) -c -- shows counters for the selected object(s) index -- selects a specific instance of the object type Th index is shown when you list the objects; it is not valid with 'all' or ith -l. 'all' and '-l' are the default options if none are specified.
ldaix_read	[numTimes{1..4294967295}]	Prints the current values for the LDAIT, LDAII, and LDAIF registers. This is primarily used for downstream power calibration. You can have it repeat the read/print very quickly, in case you are concerned that the values change during the read. It is up to you to decide what to do with the values (average, median, etc.).
lock_ds	[Frequency] [numTimes{1..4294967295}]	Causes the CM HAL to lock to the Ds Freq specified. If the numTimes parameter is present, the CM will try to lock that number of times, and will print a success rate at the conclusion of the testing. Selecting a freq of 0 will just check the

		lock status without re-running the scripts. Use only in test mode!
log	[Bitmask{0x40007f}]	Configures the message log settings for this class to enable or disable various app-specific severities. These are the bits supported: 0x000001 -- Tx MacMgt Msg Packet 0x000002 -- Rx MacMgt Msg Packet 0x000004 -- Tx Data Packet 0x000008 -- Rx Data Packet 0x000010 -- Add/Chng/Del Service Flow 0x000020 -- MIB Filters 0x000040 -- Downstream Scan 0x400000 -- Other API calls into the HalIf
packets_queued	[sfid]	Queries the HAL for the number of packets queued on the specified upstream flow. If the SFID is 0 or missing, then it prints the number of packets queued on all flows.
qosParms	[-p priority{0..7}] [-r maxRateBps] [-b maxBurstBytes{1522..4294967295}] [-c maxC]	Changes the QoS parameters associated with the specified service flow. Request/Transmit Policy bits: 0x0001 -- Disable bcast request 0x0002 -- Disable priority request 0x0004 -- Disable req/data for requests 0x0008 -- Disable req/data for data 0x0010 -- Disable piggyback request 0x0020 -- Disable concatenation 0x0040 -- Disable fragmentation 0x0080 -- Disable PHS 0x0100 -- Drop UGS packets too big
read_mbr	[opcode] [numBytes{1..4}]	Reads the multibyte register specified by the 'read' opcode, displaying the number of bytes specified. You MUST specify a valid read opcode, and the number of bytes must be valid; failure to do this can lead to unpredictable results!
read_posted	[Register] [numBytes{1..4}]	Reads the posted downstream register specified by the Register parameter, displaying the number of bytes specified. You MUST specify a valid register, and the number of bytes must be valid; failure to do this can lead to unpredictable results!
scan_ds	[Frequency] [ScanMode{0..2}]	Causes the Scan Thread to try to acquire the Ds Freq specified. If the frequency parameter is 0, then the Scan Thread selects the starting frequency on its own. The ScanMode parameter tells the thread how to limit the frequency selection: 0 - Scan all frequencies until stopped (default) 1 - Scan specified frequency once 2 - Scan specified frequency until stopped.
scan_stop		Causes the Scan Thread to stop scanning downstream frequencies.
sdram_test	[bufferSize]	Runs the SDRAM tests (stepping 1's on cached/uncached space). NOTE: This test runs forever! You must reboot to stop it.
set_mode	[OID] [true|false]	Calls the CM HAL SetMode entrypoint with the specified CM_HAL_MODE OID and the specified true/false value. The mode OID values come from cblmodem.h.
show	[-l] [-s] [-c] [cos|cls|phs|flow|all] [index]	Displays information about Classifiers, Service Flows, PHS, DOCSIS 1.0 Class of Service, and

		other objects in the system. cos -- Selects the DOCSIS 1.0 Class of Service object info. cls -- Selects Classifier info. phs -- Selects PHS info. flow -- Selects Service Flow info. all -- Selects all DOCSIS objects in the system. -l -- Lists the selected object(s). -s -- Shows settings for the selected object(s). -c -- Shows counters for the selected object(s). index -- Selects a specific instance of the object type. The index is shown when you list the objects; it is not valid with 'all' or with -l. 'all' and '-l' are the default options if none are specified.
show_halif		Causes the HalIf object to display its state.
test_bcmalloc		Tests the BcmAlloc/BcmFree module.
transmit	[-s PacketSize{64..1518}] [-t NumSeconds] [-r TimeBetweenPacketsMs] [-p FillPatte]	Transmits packets out the upstream interface. The packets will have a reasonable UDP/IP header, but otherwise have garbage data in them, so you probably don't want to do this on a live network. Packets will be sent as fast as possible unless overridden by the -r flag; you can specify the packet size and/or the number of seconds over which to send packets. If not otherwise specified, it will send 1518 byte packets until the system is power cycled. Flags: -s : The packet size; if not specified, 1518 bytes. -t : Number of seconds you want to transmit; default (0) = infinite. -r : Controls the packet rate. Specify the time (in ms) between each packet. Note that this value will be quantized based on the OS clock tick resolution (usually 10ms), so 1ms, 8ms, and 12ms are all the same as 10ms. A value of 0 means 'as fast as possible', i.e. no delay between packets. -p : Specifies the fill pattern for the buffer. The value specified will be used to fill the buffer. If not specified, then the buffer is filled with increasing values.
us_burst	[qpsk|8qam|16qam|32qam|64qam|128qam|256qam] [symbolRate] [Frequency] [power_dB] [RS_N] [RS_T]	Causes the CM HAL to constantly burst data upstream with the specified QAM/QPSK mode, symbol rate, frequency, and power level. The 3348 supports programmable RS_N and RS_T values. Use only in test mode!
us_cw_transmit	[Frequency] [power_dB]	Causes the CM HAL to constantly transmit a CW upstream at a specified frequency and power level. Use only in test mode!
us_debug	[qpsk|8qam|16qam|32qam|64qam|128qam|256qam] [symbolRate] [Frequency] [power_dB]	Causes the CM HAL to run an upstream debug sequence with the specified QAM/QPSK mode, symbol rate, frequency, and power level. Use only in test mode!
us_sweep	[startFreqMHz] [endFreqMHz] [stepFreqMHz] [power_dB] [sweepTimeSecs]	Causes the CM HAL to send an upstream sweep. The starting/ending frequencies, and the step size are specified in

		MHz. The duration of the sweep from start to end is specified in seconds. Power is in dB. Use only in test mode!
us_transmit	[qpsk|8qam|16qam|32qam|64qam|128qam|256qam] [symbolRate] [Frequency] [power_dB] [tdma|sa]	Causes the CM HAL to constantly transmit a PRBS23 pattern upstream with the specified QAM/QPSK mode, symbol rate, frequency, and power level. Use only in test mode!
write_mbr	[opcode] [numBytes{1..4}] [value]	Writes the multibyte register specified by the 'write' opcode, sending the value and number of bytes specified. You MUST specify a valid write opcode, and the number of bytes must be valid; failure to do this can lead to unpredictable results!
write_posted	[Register] [numBytes{1..4}] [value]	Writes the posted downstream register specified by the Register parameter, sending the value and number of bytes specified. You MUST specify a valid register, and the number of bytes must be valid; failure to do this can lead to unpredictable results!

Docsis Control Home

Command		Description
binarySfid	[true|false]	Use binary SFID encoding in CM initiated DSD REQ.
bpiShow		Prints the BPI State Machine Parameters.
clear_image	[-i number{1..2}]	This causes the specified image (stored in flash memory) to be erased. The -i parameter specifies the image number to be cleared (number of images depends on the platform). WARNING: If you clear all images, then the system won't run!
clearcmcert		Clears the Cable Modem Certificate.
comp_mac_to_phy	[-v] [mac_bytes] [iuc{1..15}]	Runs the UCD-based MAC-to-PHY computation for the specified number of MAC bytes on the specified IUC code. If -v is specified, then verbose debug output will be displayed.
comp_phy_to_mac	[-v] [phy_mslots] [iuc{1..15}]	Runs the UCD-based PHY-to-MAC computation for the specified number of PHY minislots on the specified IUC code. If -v is specified, then verbose debug output will be displayed.
copy_image	[SourceImage{1..2}] [DestinationImage{1..2}]	This causes the specified source image (stored in flash memory) to be copied to the specified destination image. The source image must be valid, and must be small enough to fit in the dest image slot.
dload	[-i Number] [-s] [-l] [-f] [IpAddress] [Filename{127}]	Causes the CM DOCSIS Control thread to download and store the specified image file via TFTP from the specified TFTP Server IP address. When the download is completed, the next reboot will run this image. If you omit the filename and/or IP address parameters, then we will use the ones stored in non-vol settings. The -i parameter specifies the image number to be overwritten (number of images depends on the platform). If omitted then the default image for the platform will be used. If present, the -s causes Secure Download to be used. The -l flag selects image1 as the target and allows a large image to be loaded, if allowed by the flash driver. The -f flag forces

		the image to be loaded even if the signature or compression types are not valid for the platform.
dsdiag		Shows concise information about the downstream state.
dsx_show		Shows the current state of the DSx Helper object.
goto_ds	[Frequency]	Causes the CM to move to the Ds Freq specified. If the CM fails to lock at the specified frequency, then it will continue scanning. When it locks on a valid downstream, it will then range, perform IP initialization, and register. The value can be in units of Hz or MHz (if the value is less than 10,000, then it is assumed to be MHz).
igmpShow		Prints the IGMP Group Statistics.
ip_initialize	[dhcp]	This causes the IP stack to lock in it's canned DHCP settings (IP and router addresses), and enables forwarding of packets to all interfaces. If you use the 'dhcp' parameter, then it will do DHCP to get the address; otherwise, it will use the DHCP settings from non-vol memory.
ip_show		Shows the DHCP settings that are being used by the IP stack.
log_messages	[Bitmask{0xffff}]	Enables/disables logging of DOCSIS MAC Management messages, along with TLV parsing/generation associated with them. You can enable logging of multiple messages by setting their bits to 1. These are the bit definitions: 0x0001 -- UCD 0x0002 -- RNG-REQ 0x0004 -- RNG-RSP 0x0008 -- Config file contents 0x0010 -- REG-REQ/RSP/ACK 0x0020 -- UCC-REQ/RSP, DCC-REQ/RSP/ACK 0x0040 -- DSx-REQ/RSP/ACK 0x0080 -- DCI-REQ/RSP 0x0100 -- UP-DIS 0x0200 -- gathering set of useable UCD's 0x0400 -- TST-REQ 0x0800 -- US phy overhead computations 0x4000 -- Log raw message octets 0x8000 -- Show TLV parsing/generation
modem_caps		Prints the modem capabilities from the REG-RSP.
rate_shaping_enable	[true|false]	This enables/disables DOCSIS 1.0 Class of Service or DOCSIS 1.1 QoS rate shaping. If disabled, then no rate shaping will be performed.
rng_rsp	[true|false]	Enables/disables the one-line RNG-RSP messages that are displayed when a ranging response message is received from the CMTS.
scan_stop		Causes the CM to stop scanning for a downstream channel. You must use goto_ds to start scanning again.
showFlows		Prints the current Dynamic Flow STDs.
state		Shows the current state of the CM DOCSIS Control Thread.
stop_download		If a software download is in progress, this will stop it in its tracks. The storage for the partially downloaded image will be cleared.
ucddiag		Shows concise information about the UCD state.

ucdShow		Prints the current upstream channel description being used.
up_dis	[-t Number]	Causes the DOCSIS state to be reset, deleting all flows, stopping BPI, deregistering from CMTS, stopping ranging, etc. This is equivalent to receiving an UP-DIS message. RFI-N-01049 added the timeout paramer, which you can specify with the -t parameter.
us_phy_oh_show		Prints computed upstream phy overhead settings.
usdiag		Shows concise information about the upstream state.

Docsis Control\Propane Control

Home

Command		Description
debug	[Enable]	Enables/disables internal Propane library debug printing.
discovery	[IpAddress] [PortNumber{0..65535}]	Simulates the CMTS sending a Propane Discovery packet to the CM. You must specify the IP address and TCP/UDP port number that the CMTS would have sent the packet from.
dsx_complete	[true|false]	Simulates the completion of the DSC, with the specified result (success/fail).
oper_caps	[IpAddress] [PortNumber{0..65535}] [PropaneVersion{0..65535}] [PropaneCaps]	Simulates the CMTS sending a Propane Operational Capabilities packet to the CM. You must specify the IP address and TCP/UDP port number that the CMTS would have sent the packet from. See the Propane protocol docs for the version and caps values.
port_number	[Number{0..65535}]	Sets the TCP/UDP port number that we will bind our socket to. This takes effect the next time we get an IP Address Acquired event.
psi_grant	[IpAddress] [PortNumber{0..65535}] [TransactionId SFID] [NumberOfPsis{1..255}]	Simulates the CMTS sending a Propane PSI response packet to the CM. The PSI values are chosen automatically. You must specify the IP address and TCP/UDP port number that the CMTS would have sent the packet from.
release_psis	[TransactionId SFID] [NumberOfPsis{1..255}]	Simulates a request from the Propane Library to release PSIs back to the CMTS. This causes a PSI Release packet to be sent. The PSI values are chosen automatically.
request_psis	[TransactionId SFID] [NumberOfPsis{1..255}]	Simulates a request from the Propane Library to get more PSIs from the CMTS. This causes a PSI Request packet to be sent.
show		Shows the current state of the CM Propane Control Thread.
simulate	exit|ip_acq|ip_lost|cm_oper|not_oper	Sends the specified simulated event to the CM Propane Control Thread.

Ethernet Hal

Home

Command		Description
autoneg	[true|false]	Turns Ethernet AutoNegotiation on or off.
force_link	[true|false]	Enables/disables the link detection logic, forcing the PHY to think that there is a link when there really isn't.
full_duplex	[true|false]	If autoneg is off, sets the Ethernet duplex to full/half.
hal_show		Causes the Ethernet HAL to display its internal state.

read_mii	[PhyAddr] [RegAddr]	Reads the specified ethernet MII register from the PHY specified.
show		Causes the HalIf object to display its state.
speed	[10|100]	If autoneg is off, sets the Ethernet link speed.
transmit	[-s PacketSize{64..1518}] [-t NumSeconds] [-r TimeBetweenPacketsMs] [-p FillPatte]	Transmits packets out the ethernet interface. The packets will have garbage data in them, so you probably don't want to do this on a live network. Packets will be sent as fast as possible unless overridden by the -r flag; you can specify the packet size and/or the number of seconds over which to send packets. If not otherwise specified, it will send 1518 byte packets until the system is power cycled. Flags: -s : The packet size; if not specified, 1518 bytes. -t : Number of seconds you want to transmit; default (0) = infinite. -r : Controls the packet rate. Specify the time (in ms) between each packet. Note that this value will be quantized based on the OS clock tick resolution (usually 10ms), so 1ms, 8ms, and 12ms are all the same as 10ms. A value of 0 means 'as fast as possible', i.e. no delay between packets. -p : Specifies the fill pattern for the buffer. The value specified will be used to fill the buffer. If not specified, then the buffer is filled with increasing values.
write_mii	[PhyAddr] [RegAddr] [Value]	Writes the specified value to the ethernet MII register, using the PHY specified. Note that if you want to mask bits on or off, then you will need to do the math yourself, using read_mii to show the current value.

Event Hal Home

Command		Description
control	[level{0..8}] [reporting{0..255}]	Show or modify the contents of the control table.
flush		Flush the contents of the event log, including stored events.
log_event	eventId{15} [evParm1{127}] [evParm2{127}] [evParm3{127}] [evParm4{127}] [evParm5]	Log an event with the specified event id to the event log. The event may have up to 4 event-specific text parameters; if your parameter has a space, then enclose it in quotes (e.g. "this is parm 1").
read		Read the event log from NV storage and rebuild the table.
show		Dump the contents of the event log to the console.
stress		Start a stress test for the selected event log object.
syslog	[IpAddress]	Set the IP address of the syslog server. Use 0.0.0.0 to inhibit.

Forwarder Home

Command		Description
halif_show	[-s] [-d]	Shows all of the HalIf objects that have been registered. If -s is specified, then it also prints a table of the interfaces, showing who can transmit to whom. Otherwise, it just prints the descriptions. If -d is specified, then it prints the detailed HalIf object contents, including counters, Snoops, etc.

log_packets	[true|false] [from_interfaces] [to_interfaces]	This enables/disables logging for packets received from the specified interfaces and being sent to the specified interfaces. If enabled, then the contents of the packet will be displayed, and the forwarder will show info about the HalIf on which it was received/sent, as well as why the packet was dropped. If the from/to interfaces parameters are missing, then all will be done. The interfaces are a bitmask where 0x01 corresponds to the interface at index 0, 0x04 corresponds to the interface at index 2, etc.
lt_add	[mac_addr] [halif]	Adds an association between the specified MAC address and HalIf.
lt_clear		Clears out the learning table, removing all MAC->HalIf associations.
lt_delete	[mac_addr | index]	Deletes the association between the specified MAC address and its HalIf.
lt_max_entries	[max_entries]	Gets or sets the maximum number of learning table entries that will be allowed. If this is 0, then the number of entries is limited only by memory. Note that the IP stack occupies one entry, so if you want to allow 2 CPE devices, then you must specify a value of 3. Also note that no entries will be removed, even if you specify a value that is smaller than the number of entries that currently exist in the learning table.
lt_show		Displays the contents of the learning table.

IP Hal Home

Command		Description
bootloader	[-f] [IpAddress] [Filename{255}]	Downloads the specified bootloader image from the TFTP server and stores it to the bootloader region. The image must be valid for the platform, and must have a ProgramStore header (but no compression).
clientif_debug	[StackNumber{1..4294967295}] [true|false]	Turns on debugging for the specified DHCP ClientIf object. This will show information related to processing leases, packet generation, packet processing, and timeouts.
dhcpc_debug	[true|false]	Turns on debugging for the DHCP client thread. This will show information about timeouts and packets received from the network (but not the contents of the packets).
dhcpc_show	[StackNumber{1..4294967295}]	Shows the state of the DHCP ClientIf objects. You must specify the stack number of the ClientIf object.
dload	[-i Number] [-l] [-f] [IpAddress] [Filename{255}]	Downloads the specified s/w image from the TFTP server and stores it in the image slot specified. The image must be valid for the platform, and must not contain any security, encryption, or digital signatures. It must be a simple image file with only the normal ProgramStore compression header. Parameters: -i -- Specifies the image slot to store the image to. -l -- Allows a large image to be stored, spanning images 1 and 2, if allowed by the flash

		driver configuration. -f -- Forces the given image to be accepted, as long as the CRCs are valid. Note that you must always specify the TFTP server address and filename; unlike the dload command in the Docsis directory, this command doesn't make use of any Docsis-specific nonvol settings, so it can't remember the last values used.
hal_show		Causes the IP Stack HAL to display its internal state.
ipconfig	[-l Number] [StackNumber{1..4294967295}] [renew|release|static] [IpAddress] [SubnetMask]	Configures the specified IP stack: 'renew' starts DHCP (if not started) or renews the current lease. 'release' causes the current lease to be released, shutting down the IP stack. 'static' configures the stack with the IP address/subnet mask/router specified. When using 'static', you must specify the IP address parameter. The subnet and router are optional, but desirable.
lease_show	[StackNumber{1..4294967295}] [LeaseIndex]	Shows the state of the lease controlled by the DHCP ClientIf object. You must specify the stack number of the ClientIf object, and the 0-based index of the lease. The lease index is shown via dhcpc_show. If you want to show all leases for the ClientIf, leave out the LeaseIndex parameter.
show		Causes the HalIf object to display its state.
test	[all|clientid|settings|lease|other]	Runs tests on the specified component of the DHCP Client system.

Message Log Home

Command		Description
fields	[Bitmask{0x3f}]	Displays or sets the different message fields that are enabled for display. Message field bit definitions: 0x01 -- The severity of the message (INFO, WARNING, ERROR, etc.) 0x02 -- The instance name of the object that generated the message. 0x04 -- The function/method in which the message was generated. 0x08 -- The name of the module/class in which the message was generated. 0x10 -- The system timestamp (millisecond, in hex).
severities	[Bitmask]	Displays or sets the different message severity levels that are enabled for display. Message logging bit definitions: 0x00000001 -- Fatal Errors 0x00000002 -- Errors 0x00000004 -- Warnings 0x00000008 -- Initialization 0x00000010 -- Function entry/exit 0x00000020 -- Informational 0xffffffff -- All messages
show_settings		Displays the current Message Log Settings.

Message Log\remote Access Home

Command		Description
read_default_settings	[telnet]	Causes the Remote Access server to read and use

		the default settings from nonvol. Any existing connections are not changed. This undoes any configuration changes that were made at runtime (e.g. through a MIB, etc).
restart_server	[telnet]	Stops, then starts the specified Remote Access server. Any existing connections will be closed. This is the only way to get a Remote Access server to start using new settings from a Remote Access connection (e.g. change the Telnet settings from a Telnet connection).
start_server	[telnet]	Starts the specified Remote Access server if not already running.
stop_server	[telnet]	Stops the specified Remote Access server if it is running. Any existing connections will be closed.

Ping Helper Home

Command		Description
all_sizes		Configures the settings for sweeping all packet sizes from 64-1518, with waiting and verification enabled. The time between pings is set to 0 ms, the verbosity is set to full, and the reply wait time is set to 1/2 second. The IP address is not changed.
end_size	[size{64..1518}]	Sets or shows the size of the largest ping packet that will be sent (including LLC and IP header overhead). After the packet size is increased by the step amount, if it is larger than this value, then the size is reset to the start size. This must be between start_size..1518 (MTU), inclusive.
hs_nowait		Configures the settings for doing high-speed pings (infinite), without waiting for the reply. The display verbosity is set to 2 (display only a'p'), the time between pings is set to 0, and waiting for replies is disabled. None of the other settings are changed.
hs_wait		Configures the settings for doing high-speed pings (infinite), waiting for the reply. The display verbosity is set to 2 (display only a 'p'), the time between pings is set to 0, and waiting for replies is enabled. None of the other settings are changed.
ip_address	[IpAddress]	Sets or shows the IP address of the device to be pinged.
ip_stack	[Number{0..255}]	Sets the IP stack number that the pings should be sent to. If 0, then the default stack will be used. The stackNum parameter must correspond to a valid IP stack that has been installed and initialized with an IP address.
ip_sweep	[Subnet] [StartingIp]	Pings all IP addresses on the specified subnet, starting with the address specified, reporting success or failure for each one. It changes the ping settings so that only a single ping is sent. This is often used to discover all of the IP addresses on the subnet. The address will be incremented from 1..254, skipping .0 and .255 since these are often used for local broadcast addresses.
number_of_pings	[Number{-1..2147483647}]	Sets or shows the number of pings to be sent. Note that 0 means infinite (you will need to press a

		key or type 'stop' to abort). A value of -1 causes the number of pings to be calculated based on the end size, start size, and step amount, so that it will span the range exactly once; num = (end – start + 1) / step.
ping	[-s] [IpAddress]	Begins pinging the specified IP address, using the current settings. If the IP address is missing, then it uses the one that was previously set. If you specify -s, then pinging will happen int he background until you type stop. Otherwise, it will poll for a keypress.
restore_defaults		Restores all of the options to their default values (excluding the IP address, which is not modified). The default values cause ping to behave like most host-based ping utilities (3 packets, 64 bytes, wait 5 seconds, etc.).
show_settings		Displays the current ping settings.
start_size	[size{64..1518}]	Sets or shows the size of the first ping packet that will be sent (including LLC and IP header overhead). The packet size will be increased by the step amount for each packet. This must be between 64..end_size, inclusive.
stats		Displays the ping statistics summary from the last set of pings. This is the same summary that is displayed at the end of the pings (if verbosity is > 0).
step_amount	[size]	Sets or shows the amount that the packet size will be increased for each packet. This can be any number (including 0, which means to keep the size constant for every packet). Note that if you set it too large, then the packet size will wrap around to the start size every time, since it will never be allowed to be larger than the end_size. You can also specify a negative number which causes the ping size to start with the end size parameter and step down to the start size, then wrap back around to the end size.
stop		Stops the ping that is currently running. This is necessary if you used the -s parameter with ping.
time_between_pings	[MilliSeconds]	Sets or shows the number of milliseconds that the ping helper will wait before sending the next ping. Note that this does not include time spent waiting for the reply or verifying it, or for time spent printing status information. The actual resolution and accuracy of this depends on the system (pSOS generally runs with a 10ms clock tick, so 10ms is the same as 15ms on that system).
verbosity	[Number{0..3}]	Sets the level of information that will be displayed while pinging. A higher number provides more information, but also slows down the rate at which pings can be sent. Most host-based ping utilities provide output equivalent to 3. For high-performance, high packet rate pings, values of 1 or 2 are best.
verify_enable	[true|false]	Enables/disables verification of ping replies. If enabled, and if waiting for replies is enabled, then if a reply is received, it will verify that it matches the ping that was sent, and that all of the data is intact.
wait_enable	[true|false]	Enables/disables waiting for ping replies. If

		enabled, the ping helper will wait a number of milliseconds for the reply, and will process it if received. This is true even if the timeout is 0ms; it will always check for and process the response. If disabled, then no attempt will be made to check for or process a response. This is generally only of interest when you need to send data very quickly, with no variability.
wait_time	[Milliseconds]	Sets or shows the number of milliseconds that the ping helper will wait for a ping response before continuing. This only takes effect if waiting is enabled. The actual resolution and accuracy of this depends on the system (pSOS generally runs with a 10ms clock tick, so 10ms is the same as 15ms on that system).

SNMP Home

Command		Descritption
debug	[level{0..9}]	Set the debug level of the non-portable agent.
delete	[name].[index]	Delete the specified object.
deregister	[name].[index]	De-register the bridge object for the specified MIB object.
direct_set		Test a direct SNMP set, like from the config file.
filters	[state] [hexmask]	Turn SNMP packet filtering on or off. The third argument, if specified, indicates which filters to enable or disable. If not specified, the state will apply to ALL filters. Otherwise... 0x01 -- CPE filters 0x02 -- IP filters 0x04 -- LLC filters 0x08 -- NM filters
get	[name].[index]	Get the specified SNMP object. If no index is specified, assumes '.0'. To query a table entry, use [tablename].[index], not [entryname].[index].
install_group	[vacmGroupName] [dhPublicKey]	Install one of the standard DOCSIS 1.1 groups. Supported groups are: docsisManager docsisOperator docsisMonitor docsisUser vacmGroupName is one of the above names. dhPublicKey is any old text string to use as the public key (no spaces).
log_events		Turn event log messages on or off.
log_filt		Turn SNMP packet filtering messages on or off.
log_nm		Turn SNMP NM access messages on or off.
log_req		Turn SNMP request messages on or off.
n2m	[trapId] [trapVersion] [destIP] [community]	Print the NetToMedia mappings to the console. Note that this is a superset of the ipNetToMediaTable, because it may contain off-net entries as well as on-net ones.
notify_setup		Setup Notify Mibs to enable SNMPv3 Notify. Uses default entries.
set	[name].[index] [type] [value]	Set the specified SNMP object to the specified value.
severities		List SNMP message log app-specific severity bits.
show		Print the SNMP agent's settings to the console.

test		This is a test command.
trap	[trapId] [trapVersion] [destIP] [community]	Send the specified trap of specified version to destIP with specified community string trapId -- 0=COLD_START trapId -- 1=WARM_START trapId -- 2=LINK_DOWN trapId -- 3=LINK_UP trapId -- 4=AUTH_FAILURE trapVersion -- 1=SNMPv1 trap
view_v1v2	[viewname]	Set the view used for SNMPv1/v2c queries for the specified agent.
write_access	[OID] [Access] or done	Test setting of SNMP write access, like from the config file.

USB Hal Home

Command		Description
hal_show		Causes the USB HAL to display its internal state.
show		Causes the HalIf object to display its state.

Release Notes of ZyXEL P-964CR and P-964APR

August 25, 2005

ZyXEL Comm. Inc.

Notes: For simplicity of file maintenance P-964APR and P-964CR share the same file. Please ignore the wireless part when P-964CR is used.

General

Release History

Release Date	Version	Description
2003/11/14	3.60.05r1	This version is sent for Hernden approval
2004/01/20	3.60.05	This is the first FCS version
2004/020/3	3.60.09	Add "monitor" command to show system status per 5 seconds
2004/02/19	3.60.10	Add "fac_reset" command to enable/disable reset password to factory defaults.
2004/02/19	3.60.10	Do not show RIP/TACACS key strings and TELNET password when "show_conf"
2004/02/24	3.60.10	Add wireless AP support
2004/03/09	3.60.10	Support TELNET to WAN-DATA when P964 is in IP Sharing mode.
2004/03/09	3.60.10	Add port forwarding commands: "pfwd_enable", "pfwd_disable", and "pfwd_show".
2004/03/09	3.60.10	Add port filter commands: "pflt_enable", "pflt_disable", and "pflt_show"
2004/03/09	3.60.10	Remove down stream scan plan, but leave all commands without effects.
2004/03/10	3.60.10	Downstream scan set is no more existed.
2004/03/14	3.60.10	Add static IP support for SNMP
2004/03/24	3.60.10	Move web service port to 8080
2004/03/26	3.60.10	Fix LED behavior issue
2004/03/26	3.60.10	Fix Mutex error
2004/05/21	3.60.11	Fix interoperability issue with CISCO PIX router

2004/05/21	3.60.11	Modify “reset button” to reset all to defaults
2004/05/21	3.60.11	Add sending RIP packet in broadcast and multicast mode
2004/05/21	3.60.11	Add “cmd_show” command to show current setting commands
2004/05/21	3.60.11	Add “cmd_tftp” command to backup current setting commands
2004/05/21	3.60.11	Add “man_ip” to configure a static IP for management, e.g. TELNET
2004/05/21	3.60.11	Add “tel_conf” to accept telnet from WAN, LAN or BOTH
2004/05/21	3.60.11	Add “tel_port” to configure TELNET servers’ listening port
2004/05/21	3.60.11	Add “tel_ip” to accept only this IP to connect TELNET server
2004/05/21	3.60.11	Re-involve the “scan” plan functions
2004/05/31	3.60.11	Add one to one NAT function, including commands “nat11”, “nat_add”, “nat_remove” and “nat_show”.
2004/06/04	3.60.11	Add static route function, include a command “route_add”. Obsolete commands “static_ip2” “static_ip3”, but it is no harmless to use them.
2004/06/08	3.60.11	Add “wan_ip” command for some customers who use only one static IP with RIP disabled.
2004/06/09	3.60.11	Fix “ping” now cannot work properly in windows/Linux TELNET client sessions.
2004/06/25	3.60.12	Fix “wan_ip” by adding a third gateway parameter and enable RIP. Although RIP is enabled it is not necessary for CMTS to enable RIP. Besides users can lengthen the RIP report interval up to 65535 seconds to avoid network traffic. “wan_ip” functions the same as P944S’s WAN static mode.
2004/06/25	3.60.12	Add “dhcp_enable” an extra lease time parameter. User can assign a dhcp server lease time for CPEs range from 3600 to 65535

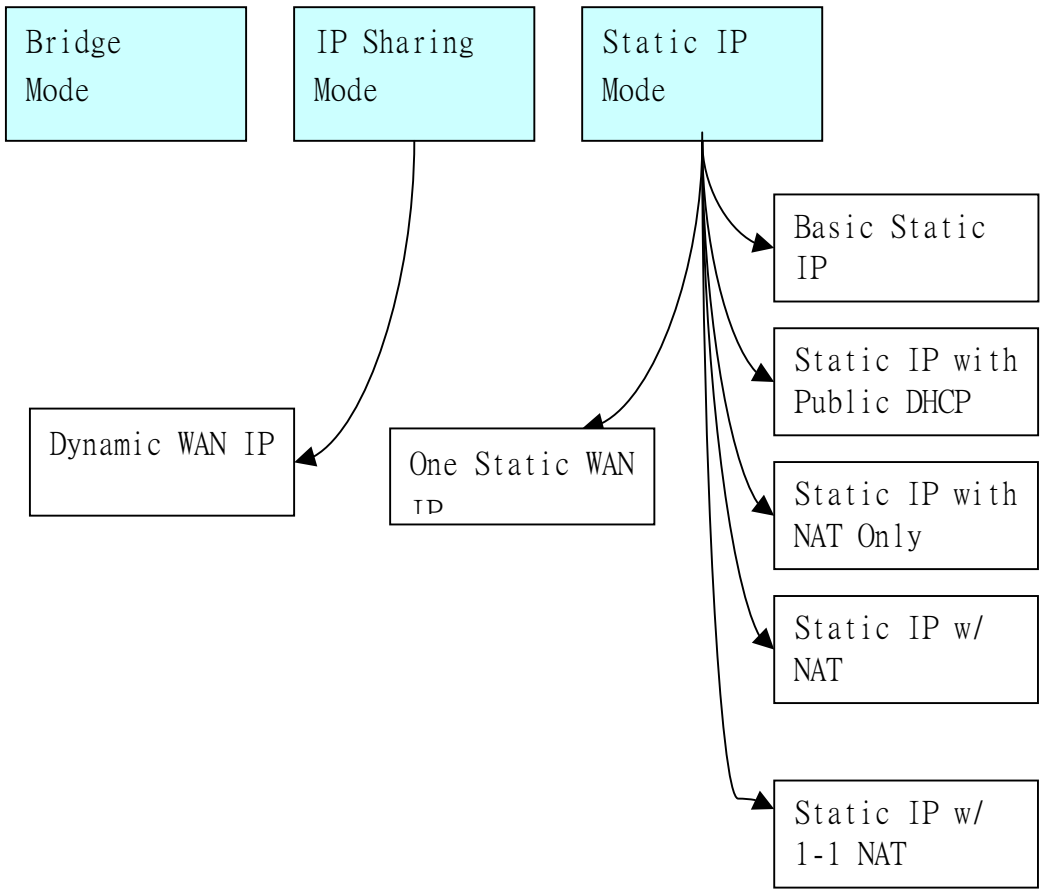
		seconds. For backward compatibility issues this parameter is optional and its default value is 3600 seconds.
2004/06/25	3.60.12	Add "hostname" command to assign P964 a hostname.
2004/09/02	3.60.13	Add CPU usage and Cable/LAN TX/RX information in "monitor" command.
2004/09/02	3.60.13	Add VSIF function.
2004/09/02	3.60.13	Fix ARP packet flooding.
2004/09/02	3.60.13	Add accessing SNMP from trusted IP and correct community string.
2004/09/02	3.60.13	Always enable hardware reset function. Cancel "fac_enable" command.
2004/10/28	3.60.14	Modify the RIP packet broadcast/multicast to WAN port, Cable side, only. This fix prevents RIP packet flooding to LAN port, Ethernet side.
2005/01/26	3.60.15	Add "ipblk_add", "ipblk_clear", and "ipblk_show" commands. "ipblk_add" will block a specific static IP from access Internet. "ipblk_clear" will clear all blocked IPs. And "ipblk_show" will show all blocked Ips
2005/03/01	3.60.16	Modify Telnet messages when users are rejected to connect to. The new message is "Connection Refused..."
2005/0301	3.60.16	Add "trust_add", "trust_clear", and "trust_show" commands. "trust_add" specify a specific IP subnet which a host can TELNET to a P964 in the subnet. "trust_clear" clears all trusted IP subnets. And "trust_show" shows all trusted IP subnets.
2005/03/01	3.60.16	Add "arpFlush" to clear the ARP table.
2005/03/01	3.60.16	Fix Cisco GRE VPN interoperate issue.
2005/05/30	3.60.18b1	Wireless LAN setting
2005/05/30	3.60.18b1	Firewall Web pages (please refer to P964APR firewall web.doc)

2005/08/02	3.60(YD.18)b7 3.60(YC.18)b6	Modify to leverage for both P-964CR and P-964APR
2005/08/18	3.60(YD.18)b8	Modify the CLI command “wl_auth” about 802.1x part of usage.
2005/08/25	3.60(YD.18)C1	Turn into formal version

Hardware Features

Powered by BROADCOM BCM3348 single-chip cable modem
200MHz MIPS32 CPU
Five ports 10/100MHz Ethernet switch with auto sensing
USB1.1 port
DOCSIS 1.0/1.1/2.0 Compliant
CableLabs DOCSIS 2.0 certified in CW#26
802.11b/g

P964 Operation Modes



P964 Cable Router has six major operation modes.

Bridge Mode

In Bridge mode, P964 operates just like a normal cable modem. All operation is compliant to DOCSIS specifications. P964 bridge mode itself is DOCSIS 2.0 certified.

IP Sharing Mode

In IP Sharing mode, the P964 operates as a NAT router. It requires one public IP address from MSO's DHCP pool and provides private IP address space for LAN users. The public IP can be static assigned or dynamically assigned through DHCP.

Static IP Mode

In Static IP mode, P964 provide a routed subnet on its Ethernet interface. A public IP subnet or a single public IP can be assigned at the Ethernet interface such that the end user can have a static assigned subnet. At the same time, the LAN users can also use private IP addresses to get on Internet. Users can also set one-to-one NAT on static IPs. There are six types of configuration which are described in next chapter.

Static IP Mode

There are four types of configuration in static IP mode.

Configuration	Description
Basic Static IP	Customer is assigned a static public IP network using a ZyXEL cable router.
Static IP with Public DHCP	Customer is assigned a static public IP network using a ZyXEL cable router. The customers public IPs, or a portion of, are setup for DHCP delivery to customer devices.
Static IP with NAT only	Customer is assigned a static public IP network using a ZyXEL cable router. The router is also configured to NAT Private IP addresses using a single IP requiring a single Private IP address be configured on the router.
Static IP with NAT and Private	Customer is assigned a static public IP network using a ZyXEL cable router. A private IP network is created for the customer.

DHCP	The IPs are NAT'd and distributed by the router via DHCP.
One Static WAN IP with NAT only	Customer is assigned a static public IP using a ZyXEL cable router. A private IP network is created for the customer. The private IPs are NAT'd to public IPs.
One Static WAN IP with NAT and Router	Customer is assigned a static public IP using a ZyXEL cable router. A private IP network is created for the customer. The private IPs are NAT'd to public IPs. Besides customer could also have static IP networks in his LAN, but CMTS must have routing information for that.
Static Route to Internal Networks	Customer is assigned a static public IP network using a ZyXEL cable router. Customer can also have other static IP network at LAN side.
Static IP with 1-1 NAT	Customer is assigned a static public IP network using a ZyXEL cable router. A private IP network is created for the customer. The private IPs are NAT'd or 1-1 NAT'd to public IPs.

Basic Static IP

Template configuration

```
defaults
ip_sharing false
dhcp_enable false
static_ip <IP Address> <Net Mask>
rip_enable true
rip2_md5  true
rip2_keyid <key_id>
rip2_keystr <RIP Keystring>
tac_enable true
tac_ip 2
tac_md5 true
tac_server <TACACS Server IP> <TACACS Server IP>
tac_key <TACACS Keystring>
bootdelay true
save
reset
```

Static IP with Public DHCP

Template configuration

```
defaults
ip_sharing false
dhcp_enable true
dhcp_server <Public IP Address> <Net Mask>
dhcp_pool <Start IP Address> <Pool Size>
dns_server <DNS Server IP>
static_ip <Public IP Address> <Net Mask>
rip_enable true
rip2_md5  true
rip2_keyid <key_id>
rip2_keystr <RIP Keystring>
tac_enable true
tac_ip 2
tac_md5  true
tac_server <TACACS Server IP> <TACACS Server IP>
tac_key <TACACS Keystring>
bootdelay true
save
reset
```

Static IP with NAT Only

Template configuration

```
defaults
ip_sharing false
dhcp_enable false
dhcp_server <DHCP IP Address> <Net Mask>
dhcp_pool <Start IP Address> <Pool Size>
dns_server <DNS Server IP>
static_ip <Public IP Address> <Net Mask>
rip_enable true
rip2_md5  true
rip2_keyid <key_id>
rip2_keystr <RIP Keystring>
tac_enable true
```

```
tac_ip 2
tac_md5  true
tac_server <TACACS Server IP> <TACACS Server IP>
tac_key <TACACS Keystring>
bootdelay true
save
reset
```

Static IP with NAT and Private DHCP

Template configuration

```
Defaults
ip_sharing false
dhcp_enable true
dhcp_server <DHCP IP Address> <Subnet Mask>
dhcp_pool <Start IP Address> <Pool Size>
dns_server <DNS Server IP>
static_ip <Public IP Address> <Net Mask>
static_ip2 <Public IP Address> <Net Mask>
static_ip3 <Public IP Address> <Net Mask>
rip_enable true
rip2_md5  true
rip2_keyid <key_id>
rip2_keystr <RIP Keystring>
tac_enable true
tac_ip 2
tac_md5  true
tac_server <TACACS Server IP> <TACACS Server IP>
tac_key <TACACS Keystring>
bootdelay true
save
reset
```

One Static WAN IP with NAT Only

Template configuration

```
defaults
```

```
ip_sharing false
dhcp_enable true
dhcp_server <DHCP IP Address> <Net Mask>
dhcp_pool <Start IP Address> <Pool Size>
dns_server <DNS Server IP>
wan_ip <Public IP Address> <Net Mask>
#without the following line we need to use CM IP for management purpose
man_ip <Public IP Address>
rip_enable false
bootdelay true
save
reset
```

One Static WAN IP with NAT and Router

Template configuration

```
defaults
ip_sharing false
dhcp_enable true
dhcp_server <DHCP IP Address> <Net Mask>
dhcp_pool <Start IP Address> <Pool Size>
dns_server <DNS Server IP>
wan_ip <Public IP Address> <Net Mask>
static_ip <Public IP Address> <Net Mask>
#without the following line we need to use CM IP for management purpose
man_ip <Public IP Address>
rip_enable false
bootdelay true
save
reset
```

Static Route to Internal Networks

Template configuration

```
defaults
ip_sharing false
dhcp_enable false
```

```
dns_server <DNS Server IP>
static_ip <Public IP Address> <Net Mask>
route_add 1 <Public IP Address> <Net Mask> <Gateway>
route_add 2 <Public IP Address> <Net Mask> <Gateway>
rip_enable true
rip2_md5  true
rip2_keyid <key_id>
rip2_keystr <RIP Keystring>
bootdelay true
save
reset
```

Static IP with 1-1 NAT

Template configuration

```
defaults
ip_sharing false
dhcp_enable true
dhcp_server <DHCP IP Address> <Net Mask>
dhcp_pool <Start IP Address> <Pool Size>
dns_server <DNS Server IP>
static_ip <Public IP Address> <Net Mask>
nat11 true
nat_add <Private IP Address> <Public IP Address>
# Users can add up to 10 entries
nat_add <Private IP Address> <Public IP Address>
rip_enable true
rip2_md5  true
rip2_keyid <key_id>
rip2_keystr <RIP Keystring>
bootdelay true
save
reset
```

The LAN IP Address is normally assigned as 192.168.1.1 and the Subnet Mask is assigned as 255.255.255.0. The Start IP Address must be at the same subnet as specified by LAN IP Address. For example,

dhcp_pool 192.168.1.33 20

The PC can be configures as DHCP client to retrieve IP address from the DHCP server.
The DNS Server IP assigned will be included in the DHCP reply to PC.

Other Operation Mode

Bridge Mode

Template configuration

```
defaults
router_enable false
save
reset
```

The default command will bring P964 to bridge mode.

IP Sharing Mode

Template configuration

```
defaults
ip_sharing true
dhcp_enable true
dhcp_server <LAN IP Address> <Subnet Mask>
dhcp_pool <Start IP Address> <Pool Size>
save
reset
```

COMMAND References

This section summarize the configuration commands of P964 cable router.

TELNET and WEB Interface

telnet_user [user name]

This command is to set the telnet user name.

Parameters:

[user mane] the user mane length must not exceed 15 characters.

Example:

telnet_user admin

telnet_pass [password]

This command is to set telnet password.

Parameters:

[password] the password, length must not exceed 15 bytes.

Example:

telnet_pass 1234

telnet_pass [password]

This command is to set telnet password.

Parameters:

[password] the password, length must not exceed 15 bytes.

Example:

telnet_pass 1234

tel_conf [Setting]

This command is to set telnet to accept connection request from LAN, WAN, or BOTH.

Parameters:

[Setting] Users can set LAN, WAN, or BOTH.

Example:

tel_conf BOTH

tel_ip [IpAddress]

This command is to set a IP which TELNET server can trust.

Parameters:

[IpAddress] IP address

Example:

tel_ip 10.11.255.254

tel_port [Port]

This command is to set telnet to listen on a specific port.

Parameters:

[Port] 0 to 65535.

Example:

Tel_port 10000

tac_enable [true | false]

This command is used to disable or enable the TACACS authentication service.

Example:

tacacs_enable true

tac_ip [TACACS SourceIpType]

This command is used to set the TACACS source Ip Type value.

Example:

tac_ip 1 → CM IP

tac_ip 2 → Static IP

tac_ip 3 → Wan IP

tac_server [IpAddress] [IpAddress]

This command setup TACACS servers. The primary server is necessary and the secondary is optional.

Example:

tac_server 192.168.80.102 192.168.80.103

tac_md5 [true | false]

This command is used to disable or enable the TACACS authentication service with MD5 encryption.

Example:

tac_md5 true

tac_key [TACACS Keystring]

This command is used to set the TACACS MD5 key string value. Of cause it is only needed when MD5 encryption is used.

Example:

tac_key 1

web_enable [true | false]

This command is used to disable or enable the Web interface. The web service will live on port 8080.

To access it please type http://ip-address:8080/.

Example:

web_admin true

web_admin_id [WebAdminId]

This command is to set the web administrator's login name.

Parameters:

WebAdminId: the WebAdminId length must not exceed 15 bytes.

Example:

web_admin_id admin

web_admin_password [WebAdminPass]

This command is to set web administrator's login password.

Parameters:

WebAdminPass: the WebAdminPass length must not exceed 15 bytes.

Example:

web_admin_password 1234

web_user [WebUserId] [WebUserPass]

This command is to set web administrator's login password.

Parameters:

[WebUserId] the user name for User web, length must not exceed 20 bytes.

[WebUserPass] the password for User web, length must not exceed 20 bytes.
Example:
web_user user 1234

snmp_set [IP] [Community]

This command sets trust SNMP IP and community string which can connect to the P964's SNMP agent. The default values are 0.0.0.0 and "public". The IP 0.0.0.0 represents no limitation.
Example:
snmp_set 210.243.128.9 zygate

remote_manage

This command is used to enable or disable remote access to the Prestige web interface through port 8080.
Example:
remote_manage true

Router Operation command

router_enable [true | false]

Enables/disables the route. If enabled, the CM operates in router mode, otherwise bridge mode.
Example:
router_enable true
router_enable false

ip_sharing [true | false]

Disable/Enable IP sharing mode, Disable this mode CM will not get another IP address
for it WAN port. This value will be true when "router_enable" is setting true. For Time Warner static IP services, this must be set to false.
Example:

```
    ip_sharing true

CM> ip_sharing true
IP sharing support..
Must save and reboot to take effect!
```

static_ip [IpAddress] [NetMask]

Setup the static IP and netmask. It is used for setting a public IP for NAT

Example:

```
static_ip 203.211.2.1 255.255.255.0

CM> static_ip 203.211.2.1 255.255.255.0
Static IP = 203.211.2.1
Netmask = 255.255.255.0
Must save and reboot to take effect
```

static_ip2 [IpAddress] [NetMask]

Setup the static IP and netmask. It is used for setting a public IP for NAT

Example:

```
static_ip2 203.211.3.1 255.255.255.0

CM> static_ip2 203.211.3.1 255.255.255.0
Static IP = 203.211.3.1
Netmask = 255.255.255.0
Must save and reboot to take effect
```

static_ip3 [IpAddress] [NetMask]

Setup the static IP and netmask. It is used for setting a public IP for NAT

Example:

```
static_ip3 203.211.4.1 255.255.255.0

CM> static_ip3 203.211.4.1 255.255.255.0
```

Static IP = 203.211.4.1
Netmask = 255.255.255.0
Must save and reboot to take effect

route_add [Index] [Network] [NetMask] [Gateway]

Add static route to cable router. Sometimes we have subnets in LAN and need a
function to route packets. We limit the number of subnets to 2, Index=1 or Index = 2.
Example:
route_add 1 10.12.20.0 255.255.255.0 10.12.16.20

CM> route_add 1 10.12.20.0 255.255.255.0 10.12.16.20
Must save and reboot to take effect

wan_ip [IpAddress] [NetMask] [Gateway]

Setup the static IP, netmask, and gateway. It is used for setting a static WAN IP for cable router. This setting must follow with RIP enabled and the WAN static IP must be have the same subnet with CMTS then on CMTS RIP is not necessary.
Example:
wan_ip 10.12.0.233 255.255.0.0 10.12.255.254

CM> wan_ip 10.12.0.233 255.255.0.0 10.12.255.254
WAN static IP = 10.12.0.233
Netmask = 255.255.0.0
Gateway = 10.12.255.254
Must save and reboot to take effect

add_passthrough [index] [MAC]

add a MAC address which will not be NATed or Routed but pass through the CM directly.

Example:
add_passthrough 1 00:02:CF:00:00:01

CM> add_passthrough 1 00:02:CF:00:00:01
CM> add_passthrough 2 00:02:CF:00:00:02

Must save and reboot to take effect

del_passthrough [index]

delete an entry which is added in 4.2.5
Example:
del_passthrough 1

CM> del_passthrough 1
Must save and reboot to take effect

nat11 [true | false]

This command is to enable/disable the 1 to 1 NAT
Example:
nat11 true

CM> nat11 true
Must save and reboot to take effect

nat_add [PrivateIP] [PublicIP]

This command sets the 1 to 1 NAT mapping
Example:
Nat_add 192.168.10.101 10.12.16.101

CM> nat_add 192.168.10.101 10.12.16.101
Must save and reboot to take effect

nat_remove

This command removes all 1 to 1 NAT mapping entries.

Example:

nat_remove

CM> nat_remove
Must save and reboot to take effect

nat_show

This command shows all 1 to 1 NAT mapping entries.

Example:

nat_show

CM> nat_show
Must save and reboot to take effect

rip_enable [true | false]

This command is to enable/disable the RIP2 routing protocol.

Example:

rip_enable true

rip2_md5 [true | false]

This command is to enable/disable the RIP2 MD5 feature.

Example:

rip2_md5 true -- Enables RIP2 MD5.

rip2_keyid [key-id]

This command is to set the RIP2 key id. The key-id number can be in range between 0..4294967294.

Example:

rip2_keyid 1

rip2_keystr [key-string]

This command is to set the RIP2 key string. The parameter key-string can not exceed 24 characters.

Example:

rip2_keystr keystr

rip2_debug [true | false]

This command is to set the RIP debug on/off. Console will display RIP broadcast massage every 30 seconds when the flag is enabled..

Example:

rip2_debug true

rip2_broadcast [true | false] [TimeInterval]

This command is to set the RIP sending packet in broadcast when setting "true" or multicast when setting "false". The default value is "false". Meanwhile users can also define the time interval (in seconds) to broadcast or multicast RIP packets.

Example:

rip2_broadcast true 30

pfwd_enable [No] [IP] [Start Port] [End Port] [Protocol]

This command can set virtual hosts at LAN. For example, users have a SMTP server located at LAN. Use the command can forward a SMTP connection from Internet to a SMTP server at LAN.

No: P964 support up to 10 entries from 1 to 10.

IP: An IP address at LAN side.

Protocol: 1 for TCP, 2 for UDP, and 3 for Both

Example:

CM> pfwd_enable 1 192.168.10.2 25 25 1

Must save and reboot to take effect!

pfwd_disable [No]

This command disables the above setting.

Example:

CM> pfwd_disable 1

Must save and reboot to take effect!

pfwd_show

This command shows the port forwarding table.

Example:

CM> pfwd_show

pflt_enable [No] [Start Port] [End Port] [Protocol]

This command set specified ports that can not be access from LAN CPEs.
For example, the administrator does not want CPEs users telnet to Internet.
The port 23 for TCP can be filtered.
No: P964 support up to 10 entries from 1 to 10.
Port: 0 to 65535
Protocol: 1 for TCP, 2 for UDP, and 3 for Both

Example:

CM> pflt_enable 1 23 23 1

Must save and reboot to take effect!

pflt_disable [No]

This command disables the above setting.

Example:

CM> pflt_disable 1

Must save and reboot to take effect!

pflt_show

This command shows the port filtering table.

Example:

CM> pflt_show

LAN and DHCP Setting

dhcp_enable [true | false] [LeaseTime]

This command is to enable or disable the LAN DHCP service and DHCP lease time in seconds, from 3600 to 65535, for CPEs. The LeaseTime parameter is optional and its default value is 3600 seconds.

Example:

dhcp_enable true 36000 -- Enable LAN DHCP server and set its lease time to 36000 seconds.

CM> dhcp_enable true 36000
Enable DHCP server.
      Lease Time = 36000 Sec.
Must save and reboot to take effect!

dhcp_server [DhcpServer] [NetMask]

Set LAN DHCP server IP address and its net mask. It is also the LAN IP address. It can be set even when DHCP server is disabled.

Example:

dhcp_server 192.168.0.1 255.255.255.0

CM> dhcp_server 192.168.0.1 255.255.255.0
Must save and reboot to take effect!

dhcp_pool [DhcpStartAddress] [IpSize]

Set LAN DHCP IP range starting from [DhcpStartAddress]. The pool size is

[IpSize]
IpSize: IpSize number, range between 1..65535.
Example:
dhcp_size 192.168.1.2 10

CM> dhcp_size 192.168.1.2 10
new lan pool strat is 192.168.1.2
new lan pool size is 10
Must save and reboot to take effect!

dns_server [DnsServer1] [DnsServer2] [DnsServer3]

This command is to setup the DNS server IP addresses. The IP address will be included in the DHCP reply to PC.
Example:
CM> dns_server 10.24.4.5 10.24.4.6 4.2.2.2
Set DNS Server 1.
Set DNS Server 2.
Set DNS Server 3.
Must save and reboot to take effect!

Wireless LAN Commands (ARP only)

wl_ssid [ssid]

This command is to set wireless LAN SSID. The maximum length of SSID is 32 bytes.
Example:
wl_ssid ZyXEL -- Set the wireless LAN SSID.

CM> wl_ssid ZyXEL
Set SSID = ZyXEL
Must save and reboot to take effect!

wl_type [open|closed]

Set P964APR to a closed network true, if you do not want to send SSID on air.

Example:

wl_type closed

CM> wl_type closed
Must save and reboot to take effect!

wl_country [country] [Channel]

Set Country code and it associated channel. The following is the wireless LAN channel defined by countries

Country	Channels
Worldwide	1 ~ 13
Thailand	1 ~ 14
Israel	5 ~ 7
Jordan	10 ~ 13
China	1 ~ 13
Japan	1 ~ 14
USA	1 ~ 11
Europe	1 ~ 13
All channels	1 ~ 14

Example:

wl_country USA 1

CM> wl_country USA 1
Must save and reboot to take effect!

wl_enable [true|false]

Enable wireless LAN interface or not.

Example:

wl_enable true

```
CM> wl_enable true
Must save and reboot to take effect!
```

wl_auth [[[disable] [WEP_OFF|WEP64|WEP128] [optional|shared_key][Pass Phrase|Key Index(1..4)] [Key1 Key2 Key3 Key4]] | [[802.1x] [Radius Server IP] [Port(0..65535)] [Key]] | [[WPA] [Radius Server IP] [Port] [Key] [Re-Key Interval(0..65535)] [AES|TKIP]] | [[WPA-PSK] [WPA Pre-Shared Key] [Re-Key Interval] [AES|TKIP]]]

Enable wireless LAN authentication.

Example:

```
CM> wl_auth disable WEP_OFF optional
```

The above command set network authentication disabled, shared key and WEP key are not necessary.

```
CM> wl_auth disable WEP128 optional 1 k1 k2 k3 k4
```

The above command set network authentication disabled and 128 bit WEP key with manual key input and shared key authentication mode is optional. For WEP64 the keys are input as follows: 0102030405 hex digit characters or 5 character string.
For WEP128 the keys are input as follows: 01020304050607080910111213 hex digit characters or 13 character string.

```
CM> wl_auth disable WEP128 optional pass_phrase
```

The above command set network authentication disabled and 128 bit WEP key with auto-key generation using pass phrase. The pass phrase is a maximum 26 byte character string.

CM> wl_auth 802.1x 4.2.2.2 1812 radius_key
The above command set 802.1x network authentication mode and Radius server IP, port, and key. It data encryption uses 128 bit WEP keys with auto-key generation. A radius key is a maximum 255 byte character string. P-964 only supports the above mode without setting WEP options and pass phrase.

CM> wl_auth WPA TKIP 4.2.2.2 1812 radius_key 0
The above command set WPA network authentication mode and Radius server IP, port, and key. It data encryption uses TKIP or AES. And 0 means that a periodical key change is not necessary.

CM> wl_auth WPA-PSK AES WPA_pre_shared_key 0
The above command set WPA network authentication mode and a WPA key. It data encryption uses TKIP or AES. And 0 means that a periodical key change is not necessary. The WPA pre-shared key is an 8 to 63 byte character string or a 64-digit hex number.

wl _restrict [Disable|Allow|Deny]

The command set a MAC address filtering policy. There are three policies. Allow policy means only the listed MACs are allowed to access Internet through P-964. Deny policy means only the listed MACs are NOT allowed to access Internet through P-964. Disable policy means no restricts.
Example:
CM> wl_restrict Allow
Must save and reboot to take effect

wl _mac [index] [MAC]

The command filters a MAC address which will be allowed/deny to access Internet. The max numbers of MAC addresses are 16.
Example:
CM> wl_mac 1 00:02:CF:00:00:01
Must save and reboot to take effect
To delete an entry:
CM> wl_mac 1 00:00:00:00:00:00
Must save and reboot to take effect

wl _mode [compatibility|gonly|performance]

The command set wireless LAN card to auto, 802.11g, or maximize performance mode.
Max Compatibility - supports 802.11b/g clients
g Only - supports only 802.11g clients
Max performance - supports only 802.11g clients and uses a proprietary method of improving performance. This mode may not work with all 802.11g clients.

Example:
CM> wl_mode compatibility
Must save and reboot to take effect

wl _protect [off|auto]

The command set wireless LAN card to automatic protection mode or not. Wireless Protection is a mechanism that is created for using RTS/CTS to maximize the throughput in mixed 802.11b/g networks. When set to 'Auto', it will use this method to maximize throughput. If the network only contains 802.11g clients, set this to off to maximize 11g performance. Mixed networks have an issue where an 11b client is not able to determine that an 11g client is transmitting so it will transmit anyway and squash the g transmission. The wireless protection will keep 11b clients from using too much bandwidth by determining when they can transmit so not to interfere with 11g clients.
Example:
CM> wl_protect auto
Must save and reboot to take effect

wl _rate [(0..54000)]

The command set wireless LAN card data rate speed. Set to 0 means auto. 54,000 means 54Mbps. The following are the valid values: 1000, 2000, 5500, 6000, 9000, 11000, 12000, 18000, 24000, 36000, 48000, 54000.
Example:
CM> wl_rate 0

Must save and reboot to take effect

wl _power [(25..100)]

The command set wireless LAN card's output power. The following are the valid values: 25, 50, 75,100.

Example:

CM> wl_power 25

Must save and reboot to take effect

wl _beacon [(0..65535)]

The command set wireless LAN card's beacon interval in mini-second. Set 0 means no beacon be sent.

Example:

CM> wl_beacon 100

Must save and reboot to take effect

wl _dtim [(1..255)]

The command set wireless LAN card's DTIM interval to number of beacon interval.

DTIM - Delivery Traffic Indication Message.

A DTIM is a signal sent as part of a beacon by an access point to a client device in sleep mode, alerting the device to a packet awaiting delivery.

DTIM interval - A DTIM interval, also known as a Data Beacon Rate, is the frequency at which an access point's beacon will include a DTIM. This frequency is usually measured in milliseconds (ms).

Example:

CM> wl_dtim 3

Must save and reboot to take effect

wl _frag [(256..2346)]

This command set the threshold, in bytes, at which wireless packets will be fragmented. This can be used to improve throughput when RF interference

is causing poor throughput.

Example:

CM> wl_frag 2000

Must save and reboot to take effect

wl _rts [(0..3000)]

RTS - Request To Send. An RTS is a message sent by a networked device to its access point, seeking permission to send a data packet.

RTS threshold - Request To Send threshold. The RTS threshold specifies the packet size, in bytes, of an RTS transmission. This helps control traffic flow through an access point, especially one with many clients.

Example:

CM> wl_rts 2000

Must save and reboot to take effect

wl _show

This command shows the wireless LAN configuration.

Example:

CM> wl_show

Firewall Commands

fw_enable [true|false]

This command is to enable the firewall features.

Example:

fw_enable true -- Set the firewall feature enable

CM> fw_enable true

Other Commands

defaults

This command is to reset the configuration to default. The P964CR must be rebooted to make it effective. The
default setting is as below:
- router_enable true
- ip_sharing true
- rip_enable false
- tac_enable false

Example:
defaults
Warning:
If you Telnet from MSO to the P964CR, please don't enter this command when the current operation mode is
Static IP mode or IP Sharing mode. Otherwise the connection will be lost.

save

This command is to write the configuration into flash ROM.
Example:
save

reset

This command is to resets the system (warm boot). The hardware reset line is triggered, causing the application to be reloaded from scratch. On host-based app simulators, this will cause the application to exit.
Example:
reset

arpShow

Displays current arp table information.
Example:

```
CM> arpShow
LINK LEVEL ARP TABLE
destination     gateway          flags  Refcnt   Use    Interface
-------------------------------------------------------------------------------------------
10.11.255.254    00:50:54:68:a8:38    405    0      0     bcm0
```

```
192.168.100.254  00:10:18:ff:ff:ff     c05    0      0     bcm1
-------------------------------------------------------------------------------------------------
```

.

ifShow

Displays current interface information.

Example:

ifShow

show_conf

This command is to show the current configuration.

Example:

show_conf

load_config [IpAddress] [Filename]

This command is to load a text based configuration from a TFTP server. After loaded, the commands inside the file will be executed line by line. This can be used for easy configuration.

Example:

load_config 192.168.100.5 config.txt

config.txt:

```
default
router_enable true
ip_sharing false
rip_enable true
static_ip 24.85.2.1 255.255.255.0
rip2_keyid 2
rip2_keystr try
save
reset
```

logout

For Telnet clients, this lets the user log out cleanly.

Example:

logout

version

Display the current firmware version

bootdelay

In some environment the head end can not sense that CM is rebooting. Use this command to let head end has much more time to know that CM is rebooting.

Example:

bootdelay true

man_ip

Some users want a specific IP, other than IP for NAT, for management, e.g. snmp, tftp, TACACS, ICMP and TELNET, when access. Set man_ip to 0.0.0.0 means use NAT IP for managemant.

cable router.

Example:

man_ip 10.12.16.2

hostname

Set a hostname for P964. It is only for management to identify who own this box. Its maximum length is up to 254 bytes.

Example:

hostname ZyGATE

dload –s [IP address] [firmware_file]

This command is located in directory, “CM/docsis_ctl”. Users need to use “cd CM/docsis_ctl” command to use them then “cd /” back to use other commands.

This command is used to upgrade the firmware of Prestige cable router from

the LAN side. The
"firmware_file" is the parameter of firmware name. The filename is usually the model name with a *.img
extension, e.g., P964CR.img. To upgrade firmware for Prestige, follow the steps:
1. Configure PC's IP address as 192.168.100.2
2. Run TFTP server on the PC and put "P964CR.img" into the outbound directory where the
"P964CR.img" is the firmware name.
3. Telnet the Prestige cable router using user name and password.
4. Enter "cd docsis_ctl" to get into docsis_ctl directory
5. Use "scan_stop" command to bypass the downstream scanning procedure if without headend CMTS.
6. Use "dload -s 192.168.100.2 P964CR.img" to start upgrade.

monitor

This command shows system status per 3 seconds for diagnostic use. Enter "exit" command to exit the monitor. If users do not exit it, the screen will be repeatedly displayed for about 30 minutes. Then it will automatically stop.

Example:

```
monitor
```

exit

This command stops displaying system status screen.

Example:

```
exit
```

cmd_show

This command shows all current setting commands.

Example:

```
cmd_show
```

cmd_tftp [TftpServerIp] [File]

This command backs up all current setting commands to a tftp server.

Example:

cmd_tftp 192.168.80.151 cmd_back.txt

ipblk_add [No] [IP address]

This command will block a specific static IP from access Internet.

Example:

ipblk_add 1 192.168.100.5

ipblk_clear

This command will clear all blocked IPs.

Example:

ipblk_clear

ipblk_show

This command will show all blocked IPs

Example:

Ipblk_show

trust_add [No] [IP address]

This command will specify a specific IP subnet which a host can TELNET to a P964 in the subnet.

Example:

trust_add 1 192.168.100.5

trust_clear

This command will clear all trusted IP subnets.

Example:

trust_clear

trust_show

This command will show all trusted IP subnets

Example:

trust_show

arpFlush

This command will clear the ARP table.

Example:

arpFlush

VSIF

VSIF specification			
2b NN 08 03 00 02 cf 80 nn ---------- 81 nn ---------- a b c d e f g h i j k			
Block	Bytes	Value	Description
a	1	2b	VSIF declaration tag
b	1	integer	Length of “c+d+e+f+g+h+i+j+k” (bytes)
c	1	08	MAC address declaration tag
d	1	03	The first 3 bytes of MAC address
e	3	00 02 cf	MAC header of ZyXEL
f	1	80	File name declaration tag
g	1	Integer	Lemgth of block “h” in bytes
h	<=16	Character	File name
i	1	81	File location declaration tag
j	1	Integer	Lemgth of block “k” in bytes
k	<=15	Character	File location in IP address
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- ---------- 2b 20 08 03 00 02 cf 80 0e 32 30 30 34 30 37 31 + ...?.?.2004071 35 30 32 2e 54 58 54 81 09 31 30 2e 31 30 2e 30 502.txt? 10.10.0 2e 31 .1			

IP Connectivity

Bridge Mode

Before P964 gets on line, CPE can not get an IP address from Ethernet

After P964 gets on line, CPE can be assigned with a public IP and browse Internet

PC can Ping to 192.168.100.1

PC can Telnet to 192.168.100.1

PC can Web to 192.168.100.1

PC can use SNMP to access 192.168.100.1 and browse MIB

PC can Ping to CMIP

PC can Telnet to CMIP

From Head-end, the MSO can Ping to CMIP

From Head-end, the MSO can Telnet to CMIP

From Head-end, the MSO can use SNMP to browse CMIP

IP Sharing Mode

No matter P964 gets on line or not, the CPE can get private IP address.
CPE can Ping, Telnet and SNMP to 192.168.100.1
CPE can Ping, Telnet and SNMP to the LAN IP (DHCP Server IP) of P964
PC can Ping to 192.168.100.1
PC can Telnet to 192.168.100.1
PC can Telnet to WAN-DATA IP
PC can Web to LAN IP (DHCP Server IP) of P964
From Head-end, the MSO can Web to WAN-DATA IP of P964

Static IP Mode

No matter P964 gets on line or not, when P964 enables DHCP server the CPE can get private IP address.
After P964 gets on line, CPE can be assigned with a public IP and browse Internet
PC can Ping to 192.168.100.1
PC can Telnet to 192.168.100.1
PC can Web to 192.168.100.1
PC can use SNMP to access 192.168.100.1 and browse MIB
PC can Ping to CMIP
From Head-end, the MSO can Ping to CMIP
From Head-end, the MSO can Ping to Static IP
PC can Telnet to CMIP
PC can Telnet to Static IP
From Head-end, the MSO can Telnet to CMIP
From Head-end, the MSO can Telnet to Static IP
From Head-end, the MSO can use SNMP to browse CMIP
From Head-end, the MSO can use SNMP to browse Static IP

WEB ES of ZyXEL
P-964CR and P-964APR

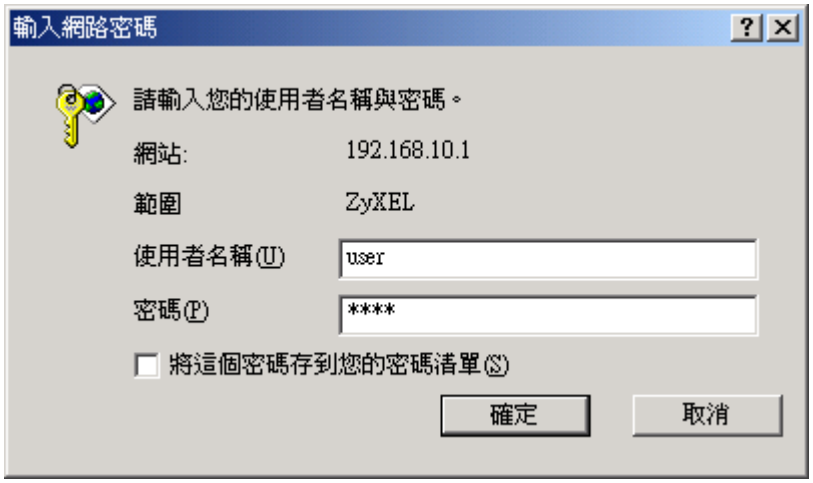
August 25, 2005

ZyXEL Comm. Inc.

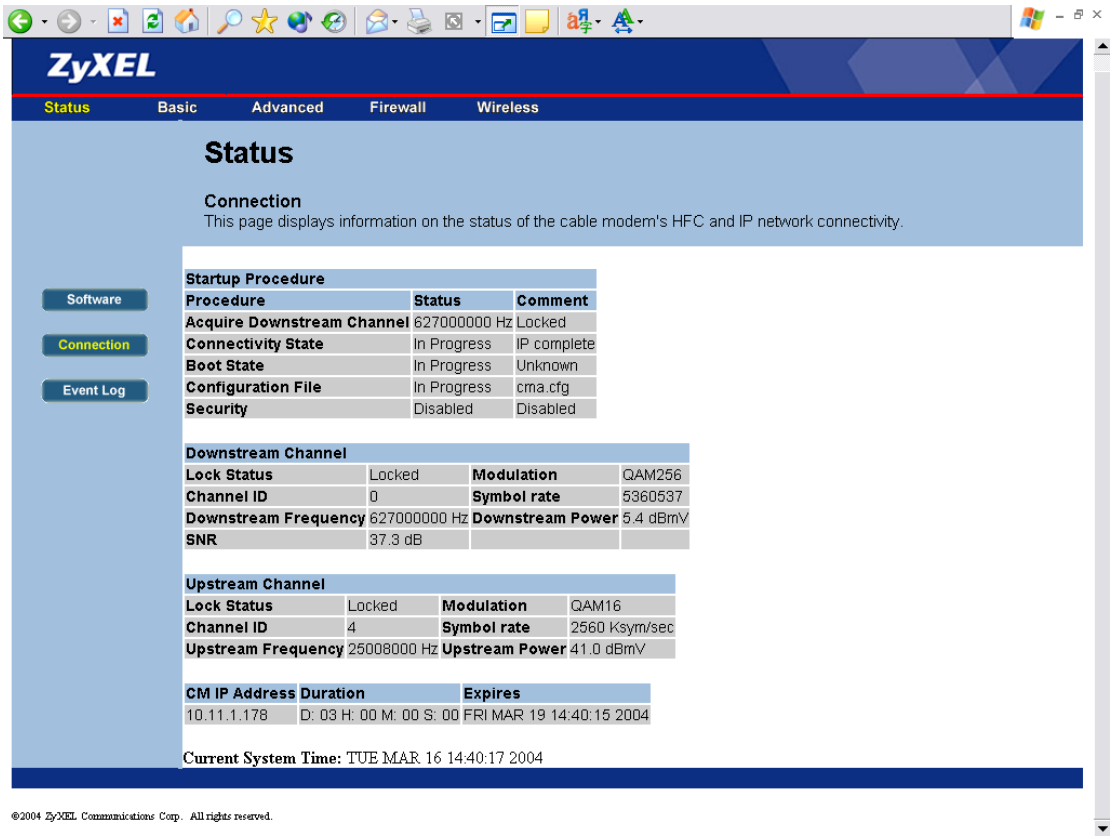
Notes: For simplicity of file maintenance P-964APR and P-964CR share the same file. Please ignore the wireless part when P-964CR is used.

Release Date	Version	Description
2004/02/24	3.60.10	File created
2005/05/30	3.60.18b1	Add firewall web pages
2005/08/09	3.60.18b7	Modify WLAN setting pages
2005/08/19	3.60.18b8	Modify WLAN setting pages
2005/08/25	3.60.18C1	Turn into formal version

ZyXEL Prestige 964 cable router provides users to configure their own LAN setting; including DHCP server IP, netmask, DHCP clients' start IP address and the number of CPEs. To configure the LAN setting, users use a PC to browse the LAN IP of the cable router. The web functions only open to the LAN, no access from HFC cable is allowed. When browsing stared, the cable router prompts the following windows for user to login.

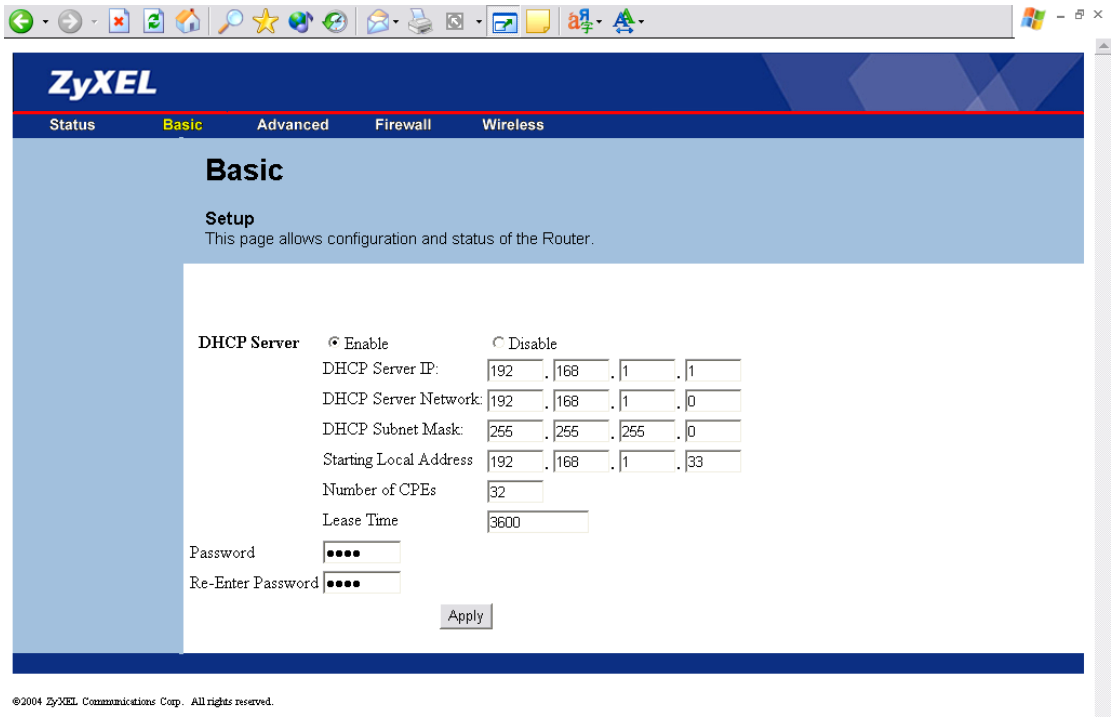


After input username/password, users can click "確定" and the following window will be displayed.

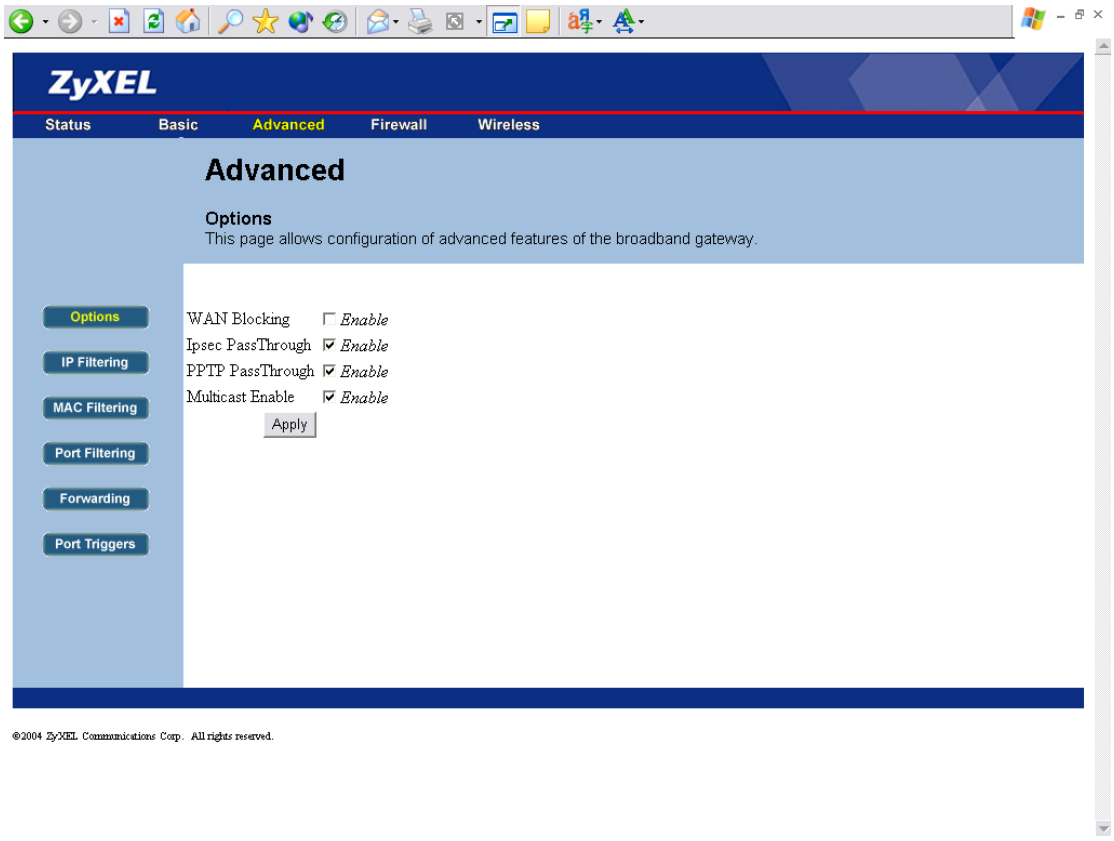


The above shows the connection status of the cable router. Users also click the
"software" icon to show the software information of the box. Besides users can also
click the icons above to set the LAN:

1. "status"
   Show the above screen.
2. "Basic"
   Click it, users can set his own DHCP server IP, netmask and etc.
3. "Advanced"
   This function especially for users who want more control of their LAN. For example, users can block some CPE, packet to access internet. Users can also open some well known ports or some special port for accessing from Internet.
4. "Wireless"
   Users can set the wireless access point.



The "Basic" windows is as above. It is quite straight and forward. From it users can set the DHCP srever IP for their LAN, as well as the network, netmask, DHCP's starting IP and the number of CPEs. User even can set lease time for the CPEs. But to update these above settings may prevent users from accessing Internet. Do not update it unless you can handle it.



The "Advanced" is a more powerful tool to set more advanced features for the Prestige 964 cable router:

WAN Blocking: Do not response to some ICMP's probing packets, e.g. ping, traceroute and etc.

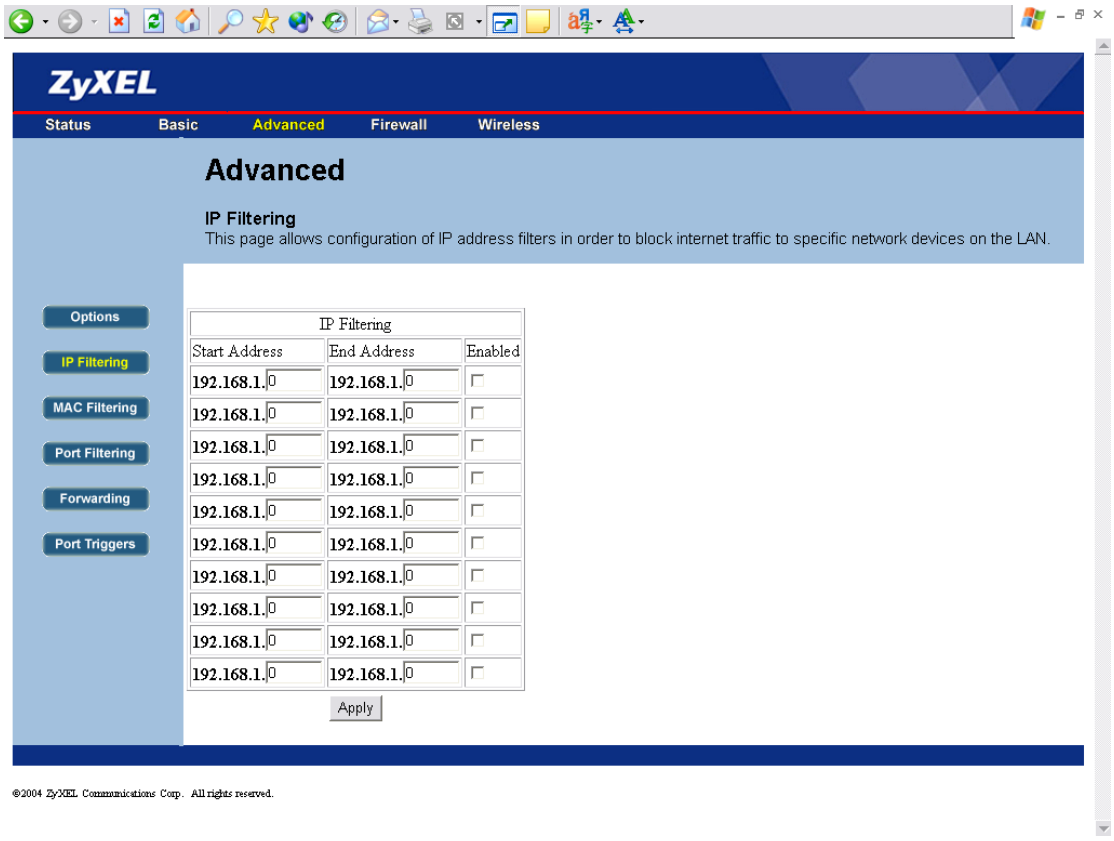
Ipsec PassThrough: for users use VPN

L2TP PassThrough: for users use VPN

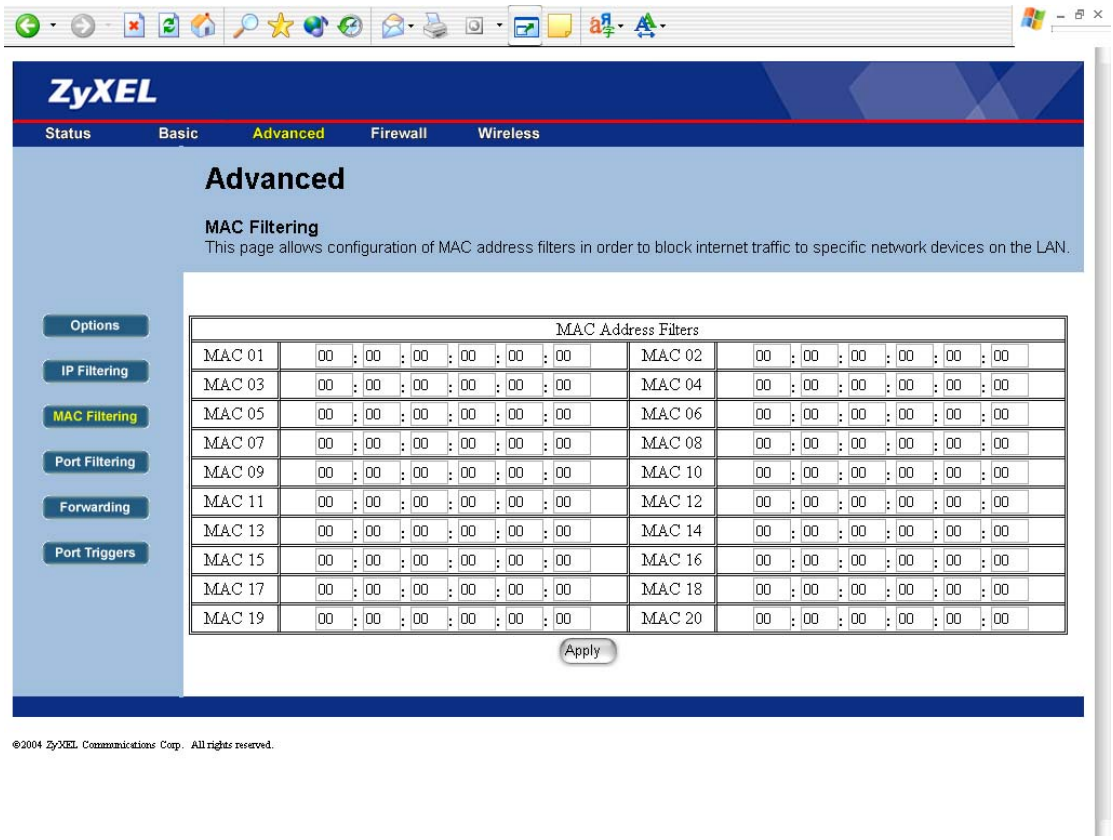
Remode Config Management: TBD

Multicast Enable:TBD

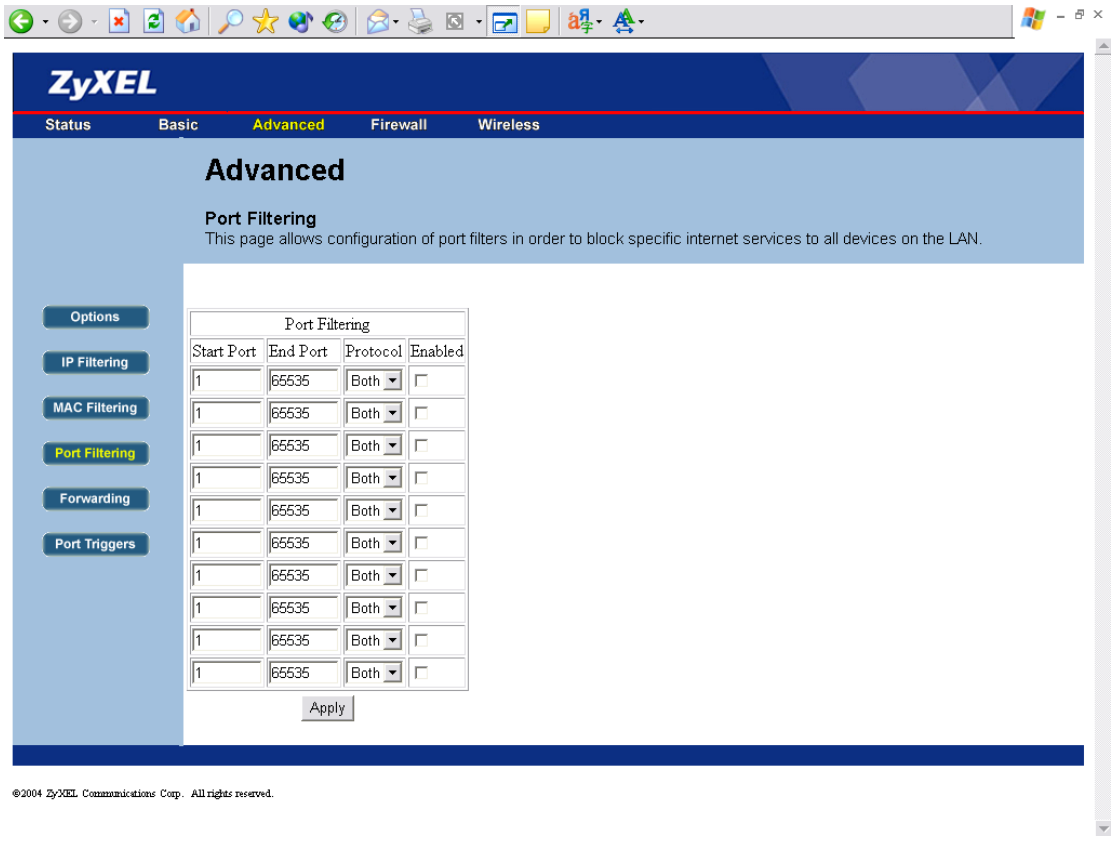
Besides these more functions are described as follows:



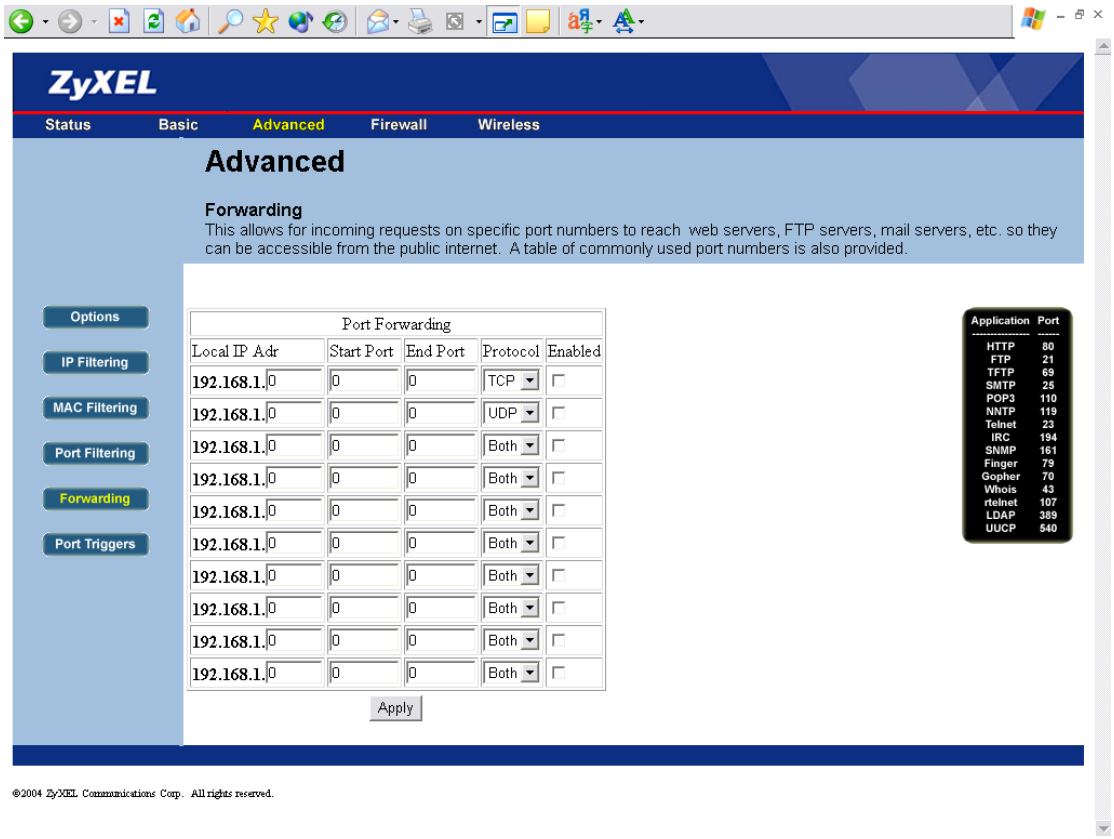
Click "IP Filtering" icon the above screen is displayed. Users can block specific CPEs to access the Internet. For example, there is a CPE whose IP is 192.168.10.20, users can set it in the above screen and click "apply". The CPE will no more can access the Internet.



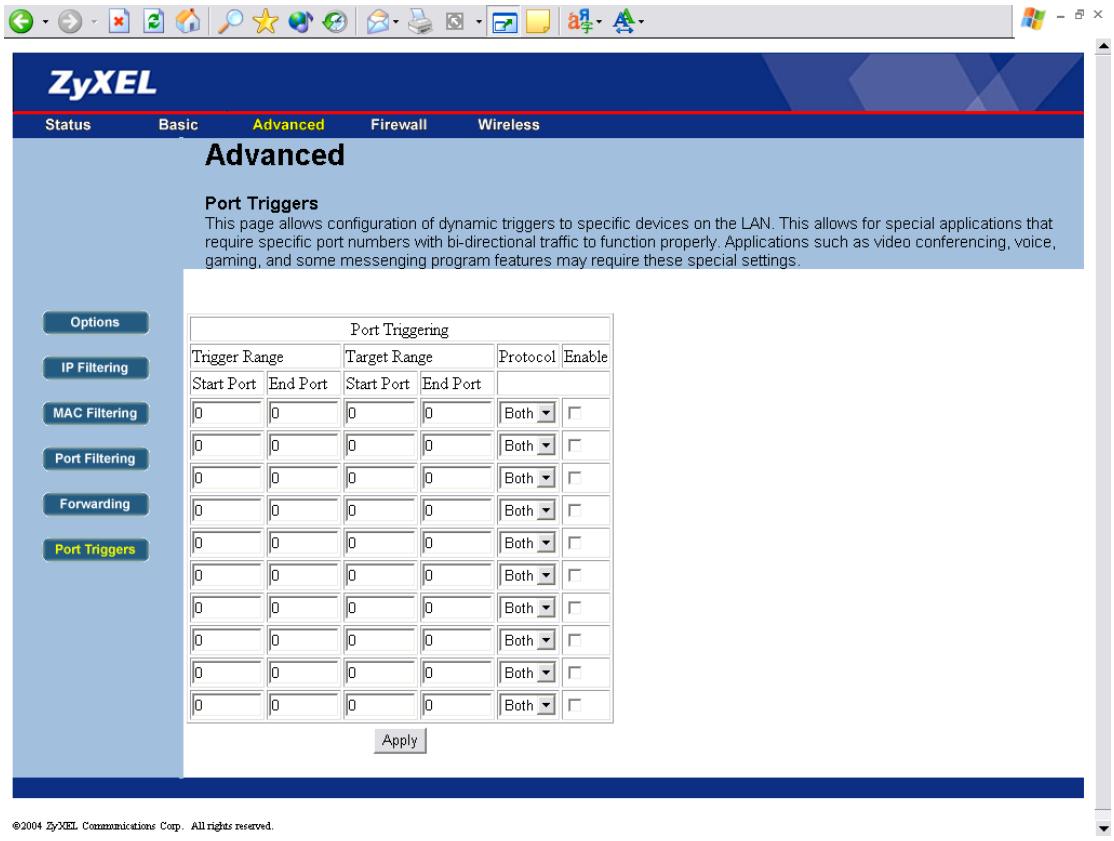
Click "MAC Filtering" icon the above screen is displayed. Users can block specific CPEs to access the Internet. It has the same effect as "IP Filtering" except this function use MAC address instead of IP address.



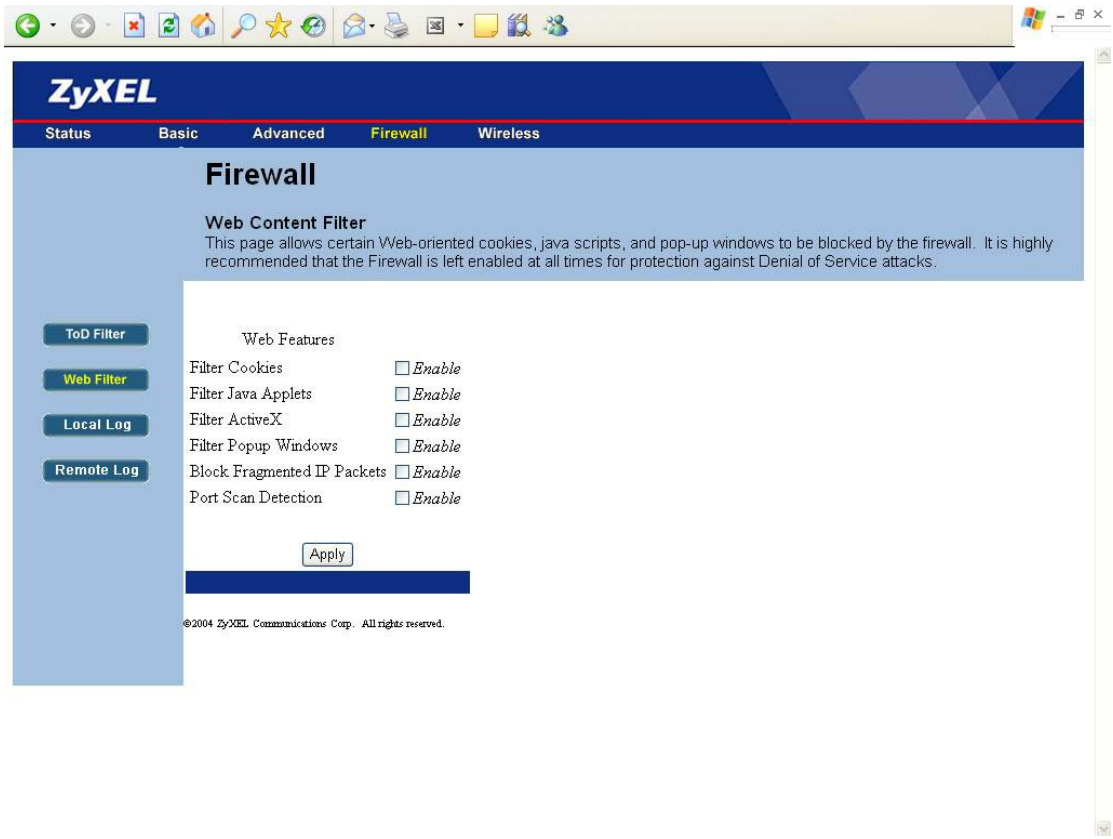
The "Port Filtering" control CPEs not to access the Internet to get the services which is provided through the ports.



The "Forwarding" function allows for incoming requests on specific port numbers to reach web servers, FTP servers, mail servers, etc. so they can be accessible from the public Internet. A table of commonly used port numbers is also provided.

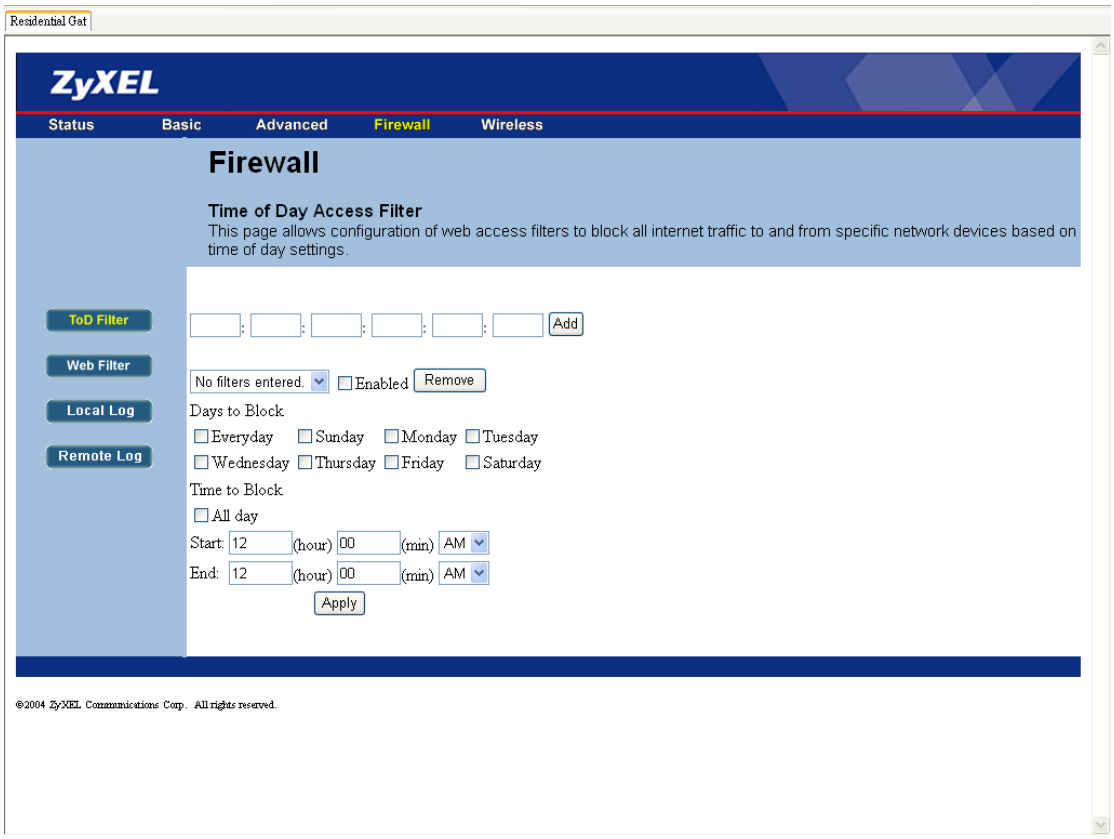


This "Port Triggers" function allows configuration of dynamic triggers to specific devices on the LAN. This allows for special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messaging program features may require these special settings.



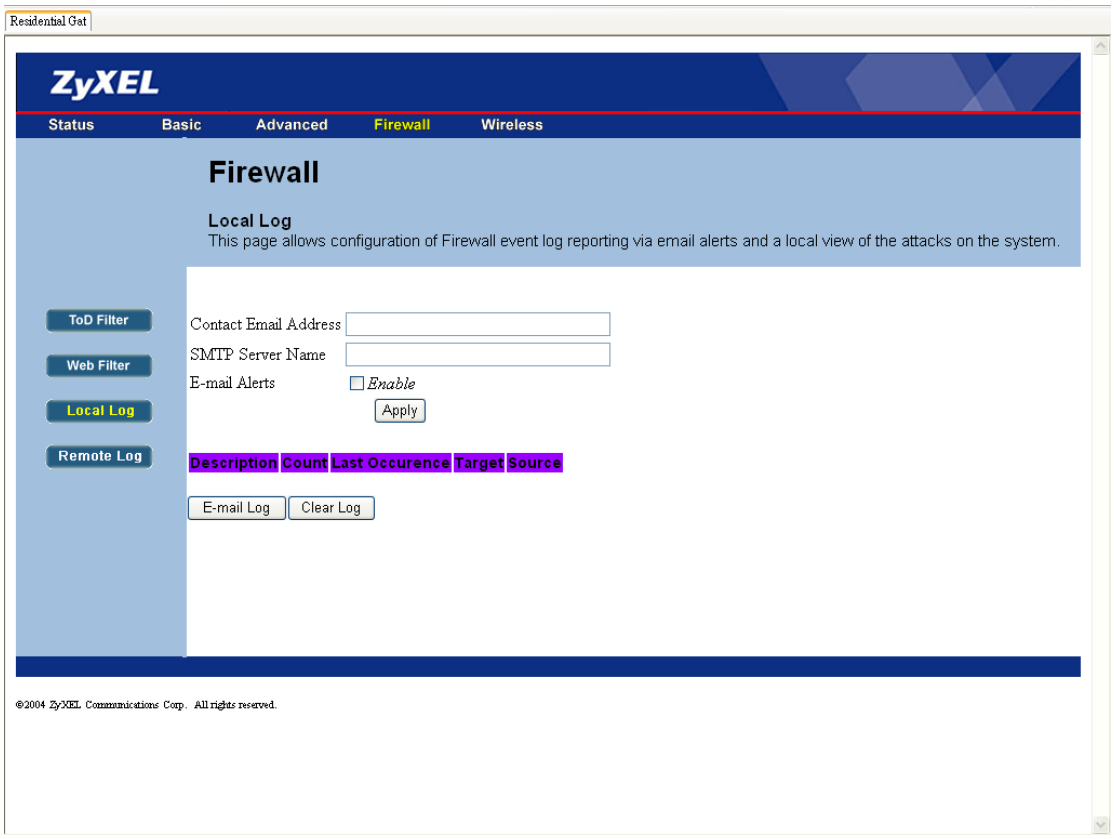
The "Web Content Filter" allows certain Web-oriented cookies, java scripts, and pop-up windows to be blocked by the firewall. Specific Firewall features can also be enabled. It is highly recommended that the Firewall is left enabled at all times for protection against Denial of Service attacks.

Users can check 'Enable' boxes to enable filtering the above web features. Besides, these users can also 'Enable' 'Block Fragmented IP Packets', 'Port Scan Detections' to prevent hackers' attack.



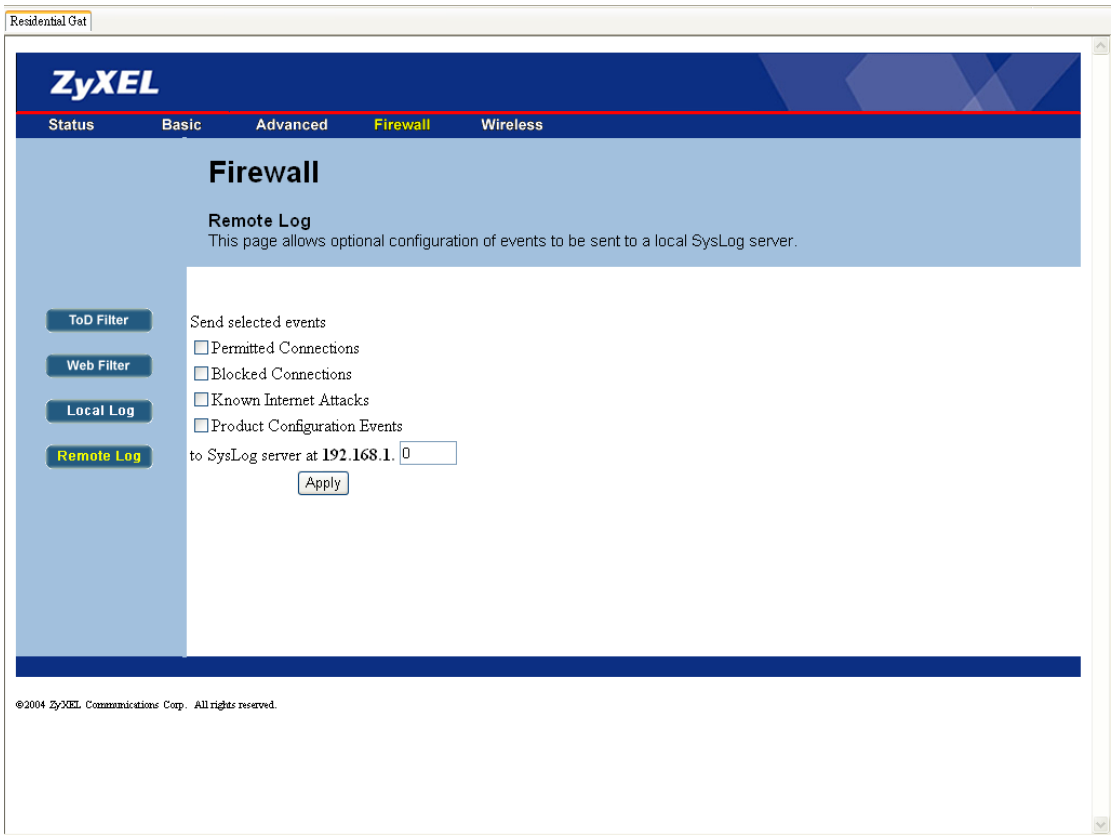
The "Time of Day Access Filter" allows configuration of web access filters to block all internet traffic to and from specific network devices based on time of day settings.

Users can add, remove CPEs' MAC address to the above Internet access filter list. For example, users can set a CPE's MAC address then 'enable' it to be limited accessing internet by enter the 'Days to Block' and 'Time to Block'. Then the CPE could access the internet resource except the blocking days and time.



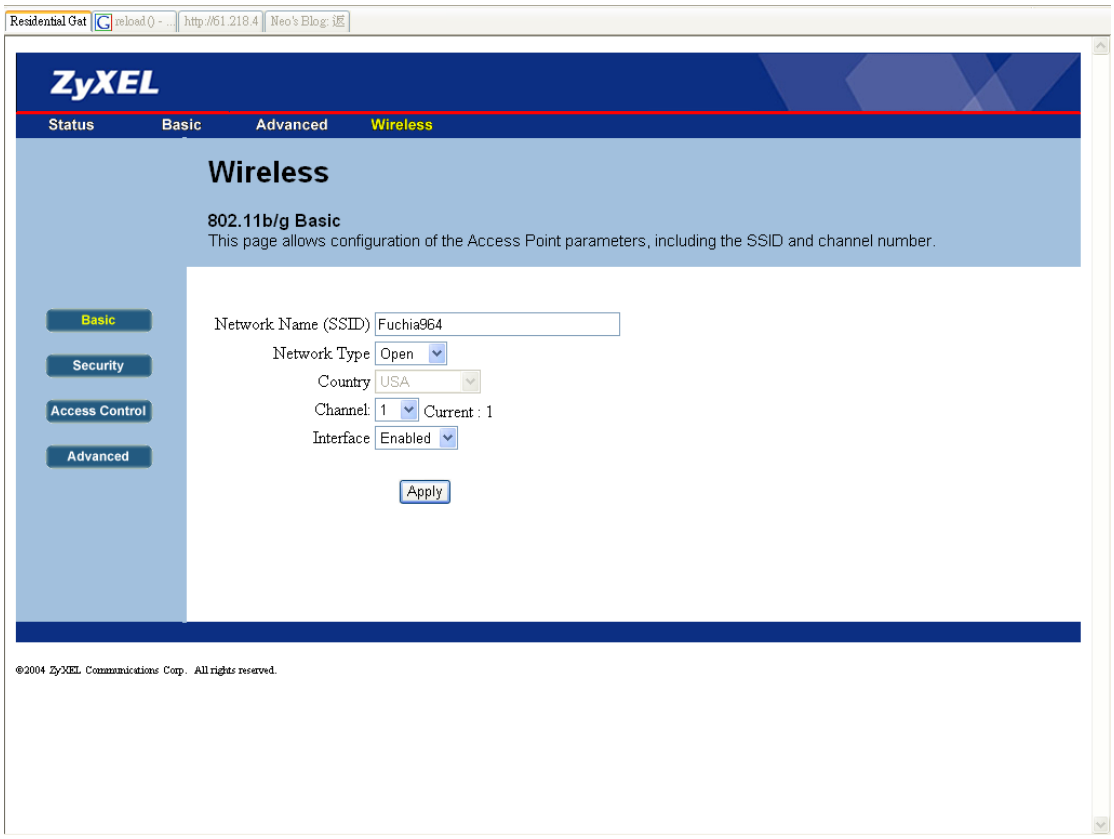
The "Local Log" allows configuration of Firewall event log reporting via email alerts and a local view of the attacks on the system.

Users can enter 'Contact Email Address', e.g. james@zyxel.com, and the mail server, e.g. ourmailserver.zyxel.com. Then check the 'Enable' box to enable it.



The "Remote Log" allows optional configuration of events to be sent to a local SysLog server.

Users can set up a SysLog server on customers' internal network, then check the above event boxes. Then enter the SysLog server's IP address. After 'apply' P964 will log the checked events to the SysLog server.



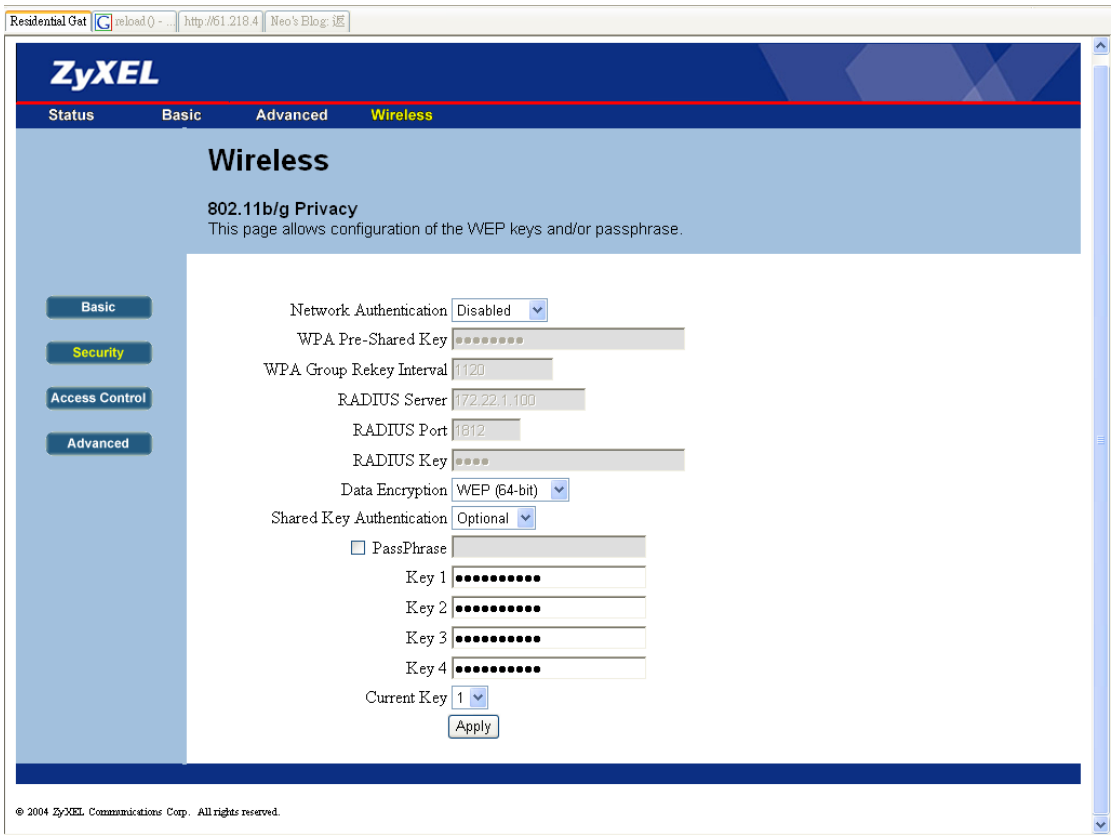
The "802.11b/g Basic" allows configuration of the Access Point parameters, including the SSID and channel number.

- Network Name (SSID):
  "SSID" is an ASCII string up to 32 characters. 802.11b/ g client adapters must have the same ID to connect to Prestige 964 wireless AP.
- Network Type :
  Select **"Open"**(default) will broadcast SSID, wireless mobile users can see the Prestige 964 wireless AP and join. In order to prevent this situation, choose **"close"** to disable broadcast SSID.

- **Country:**
  Prestige 964 wireless AP support the following channel for each country The default value is **"USA"**.

Worldwide	1 ~ 13	Jordan	10 ~ 13	USA	1 ~ 11
Thailand	1 ~ 14	China	1 ~ 13	Europe	1 ~ 13
Israel	5 ~ 7	Japan	1 ~ 14	All channels	1 ~ 14

- **Channel:** After setting country, user can assign channel for each country. Its default value is **"1"**.
- **Interface:** Enabled/Disabled the wireless interface card. The default value is **"Enable"**.
- **Apply**: Save the above change.



The “802.11b/g Privacy” allows configuration of the WEP keys and/or pass phrase.

- Network Authentication:

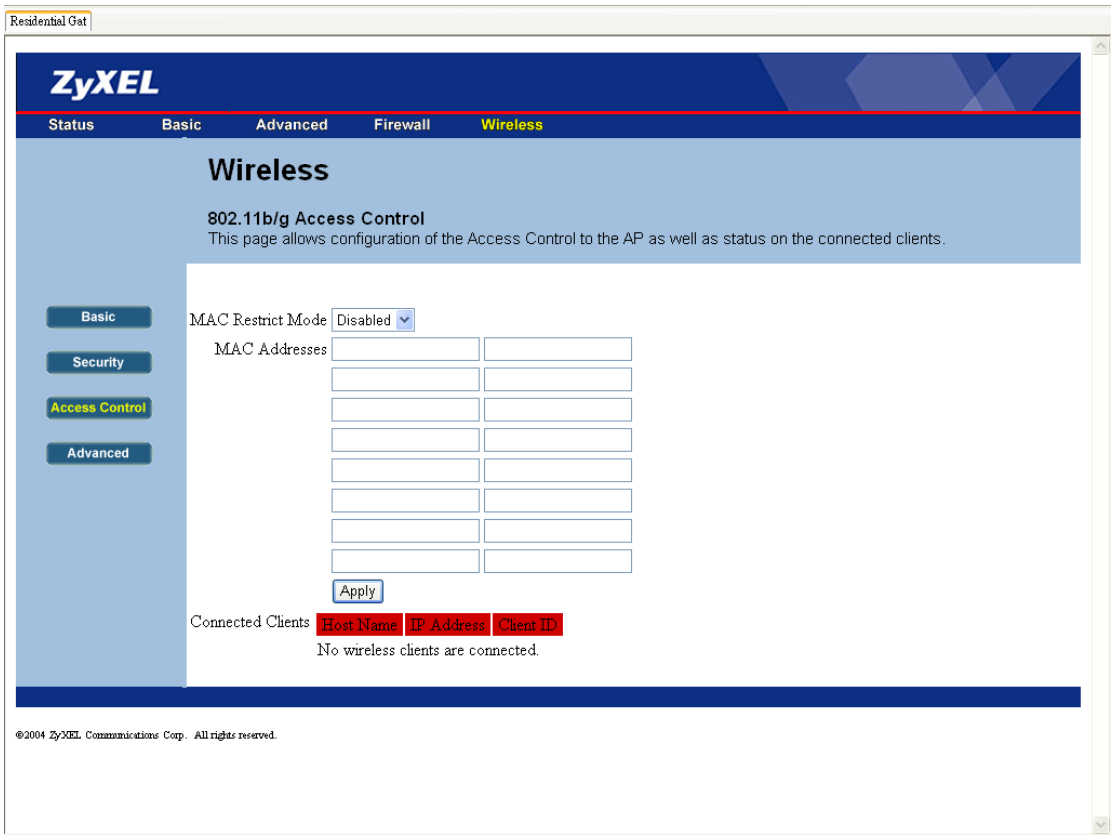
  The Prestige 964 wireless AP supoorts the following authentications.
  "Disabled": This is the default value. When "Disabled" is choose, users can set "Data Encryption" as 'Off', 'WEP(64-bit)' or '(WEP)128-bit'. The check box used to differentiate how the WEP key generated, from PassPhrase or enter direct. Use "Generate WEP Keys" to eliminate set "Network Key". The 802.11b/ g client adapters must have the same settings to connect to Prestige 964 wireless AP.

  "802.1x": There must be a RADIUS server when use this setting. 802.11b/g client adapters must have a relative setting to this option and enter the correct "PassPhrase", set on RADIUS server, when connecting.

  "WPA": This option has the same requirement to set the RADIUS server. 802.11b/g client adapters must support WPA option to connect.

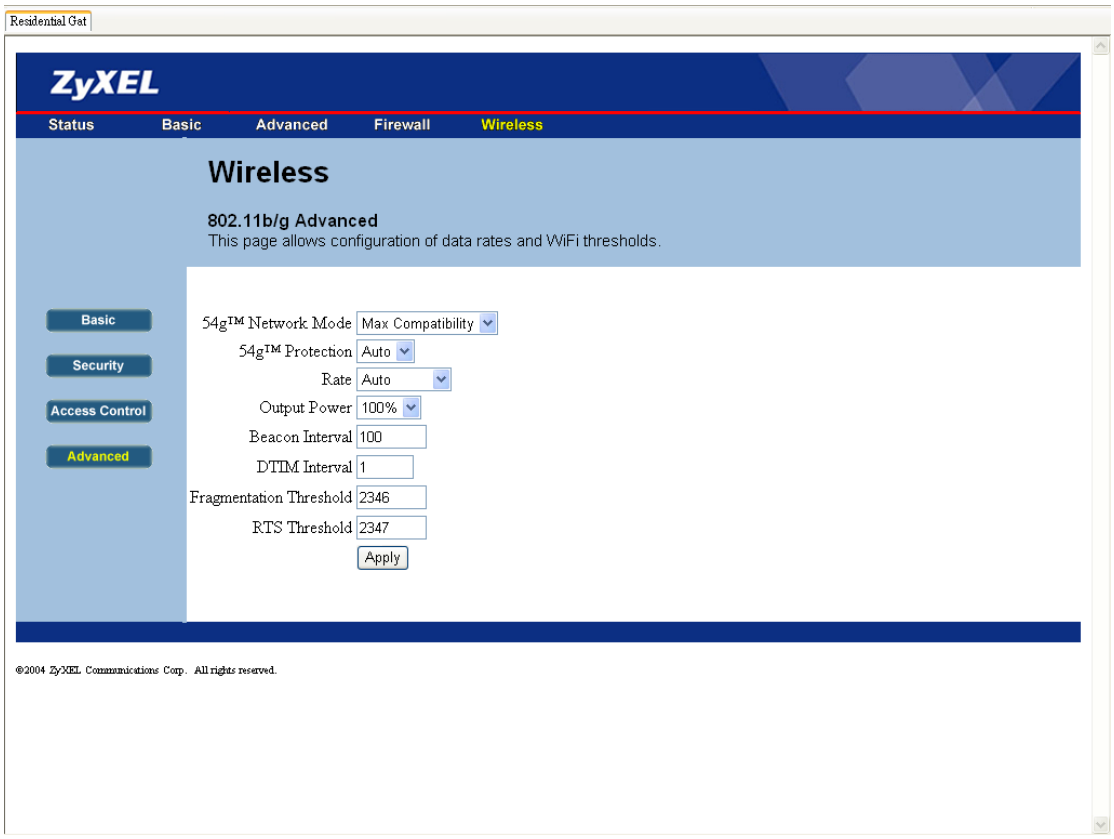
  "WPA-PSK": The RADIUS server is not required, but the "WPA Pre-Shared Key" must be set. 802.11b/g client adapters must support WPA option to connect. The Prestige 964 wireless AP also has a "WPA Group Rekey Interval", in seconds, option to set the change WPA key periodically by the interval setting.

- [Apply]: Save all change.



The "802.11b/g Access Control" allows configuration of the Access Control to the AP as well as status on the connected clients.

- **"MAC Restrict Mode":** The restrict mode can 'Allow', 'Deny' to allow or deny the following MAC address CPEs to connect the Prestige wireless AP. Choose 'Disabled' without any restrictions.
- **"MAC Addresses":** MAC Addresses to 'Deny' or 'Allow'
- **[Apply]:** Save all change.
- **"Connected Clients":** Show the current connecting CPEs.



The "802.11b/g Advanced" allows configuration of data rates and WiFi thresholds.

- **"54g Network Mode":**
  Max Compatibility - supports 802.11b/g clients
  54g Only - supports only 802.11g clients
  Max performance - supports only 802.11g clients and uses a proprietary method of improving performance. This mode may not work with all 802.11g clients.
- **"54g Protection":** 54g Protection is a mechanism that is created for using RTS/CTS to maximize the throughput in mixed 802.11b/g networks. When
  set to 'Auto', it will use this method to maximize throughput. If the network only contains 802.11g clients, set this to off to maximize 11g
  performance. Mixed networks have an issue where a 11b client is not able to
  determine that a 11g client is transmitting so it will transmit anyway

and
squash the g transmission. The 54g protection will keep 11b clients from using
too much bandwidth by determining when they can transmit so not to interfere
with 11g clients.

- **"Rate":**
  Auto / 1.0 Mbps / 2.0 Mbps / 5.5 Mbps / 6.0 Mbps / 9.0 Mbps / 11.0 Mbps / 12.0 Mbps / 18.0 Mbps / 24.0 Mbps / 36.0 Mbps / 48.0 Mbps / 54.0 Mbps

- **"Output Power"**: 25% / 50% / 75% / 100%

- **"Beacon Interval":**
- **"DTIM Interval":**
- **"Fragmentation Threshold":**
- **"RTS Threshold":**
  These normally don't need to be changed, but here's a description of what each one does:

  DTIM - Delivery Traffic Indication Message. A DTIM is a signal sent as part of a beacon by an access point to a client device in sleep mode, alerting the device to a packet awaiting delivery.

  DTIM interval - A DTIM interval, also known as a Data Beacon Rate, is the frequency at which an access point's beacon will include a DTIM. This frequency is usually measured in milliseconds (ms).

  Fragmentation Threshold - This set the threshold at which wireless packets
  will be fragmented. This can be used to improve throughput when RF interference is causing poor throughput.

  RTS - Request To Send. An RTS is a message sent by a networked device to its
  access point, seeking permission to send a data packet.

  RTS threshold - Request To Send threshold. The RTS threshold specifies the

packet size of an RTS transmission. This helps control traffic flow through
an access point, especially one with many clients.

- **[Apply]:** Save all change.