



Firmware Release Note

Prestige 652HW-31

Standard version

Release 3.40(IU.4)C0

Date: October 11, 2004
Author: Nedo Lee

ZyXEL Prestige 652HW-31 Standard Version Release 3.40(IU.4)C0 Release Note

Date: October 11, 2004

Supported Platforms:

ZyXEL Prestige 652HW-31

Versions:

ZyNOS F/W Version : V3.40(IU.4) | 10/11/2004 17:39:40

BootBase : V1.14 | 10/27/2003 10:05:54

Notes:

The P652HW-31 is a small-office and home device that will allow a small LAN to access the Internet. By integrating ADSL, WLAN, NAT, P652HW-31 provides the ease of installation and Internet access.

The P652HW-31 provides an PCMCIA wireless card slot for 802.11b Wireless LAN connectivity, four single auto-sensing, auto-detection 10/100BASE-T Ethernet ports for connection to the user's local network, and a single RJ-11 port for connection to ADSL line.

The version of Alcatel modem code is 3.9.122

Known Issues:

1. Upgrading firmware from V3.40(IU.1) to V3.40(IU.2) without loading default ROM file needs to set Menu 1 Bridge to Yes and reboot in order to make communication between WLAN and LAN.
2. Upgrading firmware from V3.40(IU.2) to V3.40(IU.3) need to use firmware upgrade tool to update new firmware. This tool only support change firmware from V3.40(IU.2) to V3.40(IU.3), you can't use this tool to upgrade firmware from others version. [See Appendix 1.](#)
3. The Switch needs 5 minutes to refresh it's bridge table. Therefore, if LAN connection switch to another port will not work for 5 minutes.
4. "SIP passthrough" works failed.
5. In SMT, if we using the WPA in WLAN, the static wep key in menu 3.5 do not support protection mechanical to prevent user start the static wep key. Contrariwise, if we using static wep key in manu3.5, device do no support protection to prevent user start the WPA.
6. If we select the 802.1x dynamic wep key or WPA in SMT manu, the authentication database should be fixed in "RADIUS only"

7. In Web/GUI, Firewall, Rule summary, edit one rule. The Log "log packet detail information" function work failed.(If we turn on the "Alert", then whether we turn on the log feature or not, the log will always work).
8. ATM QoS, when using VBR and setting SCR to zero, the traffic will be blocked.

Features:

Modification in 3.40(IU.4)C0 | 10/11/2004

1. [BUG FIXED]
Change ROM file. In Web/GUI, Firewall page, Rule Summary, select "WAN to WAN Router", configure the source and destination IP address to "Any".
2. Change to FCS version.

Modification in 3.40(IU.4)b2 | 9/24/2004

1. [BUG FIXED]
Symptom: Device will hang when change NAT configuration in SMT menu 4, when performing change from SUA to Full feature if press "Enter" fast
Condition:
2. [BUG FIXED]
Symptom: Edit the customized port in web firewall page, add two rule, then delete the first one and click back, add the rule2 into "select services" and click "Apply" device will show "internal error".
3. [BUG FIXED]
Symptom: The PPPoE will fail when with the continue ping from LAN PC
4. [BUG FIXED]
Symptom: At NAT full feature use many to one or many to many set End IP smaller than start IP save it in SMT menu . Then DUT exception occur.
5. [BUG FIXED]
Symptom: Try to login Prestige by Web GUI. Type in long user name and password. The Prestige will exception.
6. [BUG FIXED]
Symptom: If there are number in the domain name and it is under 255 our device will think it's an IP address instead of domain name and will not try to resolve it with DNS server. This will cause VPN can not be established with remote secure gateway is configured with such domain name
7. [BUG FIXED]
Symptom: When LAN embedded DHCP server is configured and there is another DHCP server on DMZ port. Client when on LAN make DHCP request. It will get IP from the DHCP server on DMZ. Thus the client on the LAN is with IP on DMZ

segment.

8. [BUG FIXED]
Symptom: In Web/GUI, French language page, firewall page do not support customized port setting. And the Germany page's customized port setting show disorder code
9. [BUG FIXED]
Symptom: PPP connection down after enable the bandwidth management on the WAN interface
Condition:
 - (1) Let the PPPoA or PPPoE connection up
 - (2) Setup a upload BM rule, ex. dedicate 12KB for a certain PC upload to any IP(destination=0.0.0.0) and check the 'borrow from parent'.
 - (3) After wait for several seconds, PPP connection goes down.

Modification in 3.40(IU.4)b1 | 07/08/2004

1. [BUG FIXED]
Symptom: UPNP feature can't work on Messenger 4.7
Condition: (1) Enable UPNP feature on Prestige.
(2) Using Messenger 4.7
(3) Video and Audio and whiteboard function do not work
2. [FEATURE ENHANCE]
Symptom: Add CI command "sys upnp reserve [0|1]"(default value is 0) to reserve UPnP NAT rules in flash after system bootup
3. [BUG FIXED]
Symptom: UPNP+SIP can't work fine.
Condition: (1) Enable UPNP feature on Prestige.
(2) Using SIP service on Windows Messenger.
(3) SIP client can't login to SIP server.
4. [BUG FIXED]
Symptom: Dial backup failed.
Condition: (1) Using ISDN TA (or U-336E ZyXEL modem) to trigger dial backup line,
(2) When channel is up, then led of DTR will off,
(3) Then the backup line is failed.
5. [BUG FIXED]
Symptom: The romfile configuration menu does not exist for Franch and German language GUI where it's available on English.
6. [BUG FIXED]
Symptom: Edit custom port in web firewall page doesn't work fine.
7. [BUG FIXED]
Symptom: Default VPI/VCI is 8/35 instead of 0/35.
8. [BUG FIXED]

ZyXEL Confidential

- Symptom: MSN messenger voice function can't work fine.
Condition: Using MSN messenger 6.1
9. [BUG FIXED]
Symptom: Netmeeting can't establish connection.
Condition: Using Netmeeting and establish connection from WAN to LAN.
10. [FEATURE ENHANCEMENT]
Symptom: Turn on firewall triangle route in default romfile.
11. [BUG FIXED]
Symptom: System will reboot
Condition: When we try to login Web GUI using long user name/password.
12. [BUG FIXED]
Symptom: Content filtering doesn't apply after VPN
Condition: Prestige supports a special application:
Prestige(branch)=====VPN=====Prestige(HQ)----->Internet
Internet access from branch office must go out through the VPN tunnel.
Thus HQ can control the traffic from / to the branch office. However,
content filter setting in HQ cannot control the traffic from branch
through the VPN tunnel..
13. [BUG FIXED]
Symptom: Alert Message function didn't work in proper manner
Condition: When we enable the alert message and logs function in firewall rules. Then
some network traffic match the rule(whatever forward or block). The logs
can send to syslog server, but the alert message did not send out..
14. [BUG FIXED]
Symptom: Time and Date display error
Condition: Synchronize system clock with Time Server, then config new
time "12:22:22", click apply button, then the time show "11:22:22".
15. [FEATURE ENHANCE]
Symptom: The maxlength of Password is changed from 31 to 30
16. [BUG FIXED]
Symptom: Sometimes when connect to router by TCP, FTP or HTTP will fail
Condition: (1) One user connects to router by FTP, TELNET or HTTP.
(2) In TCP handshake, client doesn't receive SYN ACK. i.e., router is in
SYN RECEIVE state.
(3) Client timeout and send RESET to router.
(4) Related socket in router is still alive and other users can't login router
until this socket timeout.
17. [BUG FIXED]
Symptom: Modify rom-t file to enable static WEP key and dynamic WEP key then
upload back to device, the PC can not be able to associate to AP by using
either way
Condition: (1) Enable static WEP key on menu 3.5 in rom-t.
(2) Enable dynamic WEP key on menu 23.4 in rom-t.
(3) Using ftp upload rom-t into device.
18. [BUG FIXED]
Symptom: System will reboot

Condition: When setting the NAT address mapping rule and the start IP is greater than the end IP address.

19. [BUG FIXED]

Symptom: Use ROM-d to put default ROM file will get malloc fail

Condition: Use ROM-d to put default ROM file will get malloc fail even available memory size is still large than RAS size.

20. [BUG FIXED]

Symptom: If you set right accounting server, password and enable it, when turn on/off authentication server or accounting server then system possible occurs reset.

21. [BUG FIXED]

Symptom: Output power value is zero

Condition: When issue CI-command "wan adsl linedata near", output power upstream value is zero.

22. [BUG FIXED]

Symptom: The RADIUS server disable would show error message when WPA-PAK is enabled

Condition: (1) Enable WPA-PSK when RADIUS server have been enabled.

(2) Then to disable RADIUS server and it would show error message.

23. [BUG FIXED]

Symptom: It would appear an error message that the RADIUS is not active when setting the WPA-PSK on SMT menu 23.4.

Condition: (1) To set Key Management Protocol is "WPA-PSK" on SMT menu 23.4 and to save it.

(2) It would show error message "Error: RADIUS is not active".

24. [BUG FIXED]

Symptom: 802.1x with dynamic WEP key cannot work when shared secret of accounting server is invalid.

Condition: (1) Enable smt23.2 authentication server and accounting server.

(2) 802.1x supplicant associate to AP with mode 802.1x dynamic wep.

(3) Modify smt23.2 accounting server shared secret with a wrong value.

(4) 802.1x supplicant was prohibited by 802.1x module..

25. [BUG FIXED]

Symptom: In eWC if we ping a address like:"192.168.1.1 a" the device will ping it for a loop and the eWC can't get response and just like been locked.(the same in CI command and we can stop it just "CTRL+C").

26. [BUG FIXED]

Symptom: Sometimes PPPoE/PPPoA can't dial up successfully when power up

Condition: System must finish "eventCmSetup", "eventNetSetup" first and then call "lineEventPolling" to notify upper layer.

27. [BUG FIXED]

Symptom: In SMT menu, system limit the VPI,VCI when VPI is 0 and VCI is 32 or under 32

Condition: remove the limitation.

28. [BUG FIXED]

Symptom: Configure Firewall Anti-probing page as response from DMZ only, but

- DMZ still doesn't response ping
Condition: DMZ should response ping if DMZ is chose.
29. [BUG FIXED]
Symptom: Device will reply wrong packet
Condition: Device will reply wrong packet under ENET ENCAP + IES1000 combination.
30. [BUG FIXED]
Symptom: Wireless WEP key should not treat character as HEX value on eWC
Condition: (1) Into Wireless LAN -> Wireless on eWC and setting WEP Encryption is 64-bit WEP.
(2) To input "0123456789" on key1 then to press apply button.
(3) The eWC can not display any error message.
(4) The 128 and 256 bit WEP have the same bug.
31. [FEATURE ENHANCE]
Symptom: Support one CLI command to enable/disable SIP ALG. This value is saved in the romfile.
(1) "ip nat service sip active 1" is to enable SIP ALG
(2) "ip nat service sip active 0" is to disable SIP ALG
32. [BUG FIXED]
Symptom: content filter sometimes can not work fine when using search engine.
Condition: (1) Setting content filter restricte keyword and enable keyword blocking on eWC.
(2) To setting content filter schedule on eWC
(3) Using seach engine like "google" to search keyword.
(4) Sometimes could link restricted keyword's website.
33. [BUG FIXED]
Symptom: ARP request from 1st remote node(router mode) , replied it from the 2nd remote node (bridge mode). The problem makes the remote VLAN enabled router coufused and the communication will fail
34. [BUG FIXED]
Symptom: Router will disclose portions of memory contents to users
Condition: Ping a zero size packet to router
35. [BUG FIXED]
Symptom: Dial backup can't work fine.
Condition: The host behind the router continuously ping a WAN IP, and using ICMP check mechanism, although ADSL physical status is "UP", router can't fail over from dial backup to ADSL.
36. [BUG FIXED]
Symptom: eWC/Advanced Setup >> NAT Edit Address Mapping Rule, click "Edit Details". information will be saved.
Condition: (1) To eWC/Advance setup/NAT.
(2) Click "Edit Details" but doesn't press "Apply" button
(3) The to other items like "LAN".
(4) Then to "NAT" again that you can see the setting have been save but we don't press "Apply" button.

Modification in 3.40(IU.3)C0 | 03/16/2004

1. Change to FCS version.

Modification in 3.40(IU.3)b4 | 03/10/2004

1. [BUG FIXED]
Symptom: Connecting 2nd IPSec tunnel cause device hang-up.
Condition: While trying to establish 2nd IPSec tunnel will cause device hang-up.
2. [BUG FIXED]
Symptom: Test Bandwidth Management feature cause device exception or traffic is blocked.
Condition: 1). Enable Bandwidth Management at WAN interface. 2). Test Bandwidth Management with AX4000. 3). Device will exception or traffic is blocked.
3. [BUG FIXED]
Symptom: Traffic is blocked.
Condition: WLAN do FTP failed when using B120 with heavy traffic on TX direction.

Modification in 3.40(IU.3)b3 | 02/24/2004

1. [BUG FIXED]
Symptom: SIP pass-through can't work fine.
Condition: Setup a SIP phone call from WAN side to LAN side, then WAN side user can't unhook the call.
2. [BUG FIXED]
Symptom: The link of Wireless LAN-Roaming help page is broken at eWC.

Modification in 3.40(IU.3)b2 | 02/02/2004

1. [BUG FIXED]
Symptom: Firewall can not filter FTP and CuSeeMe Application.
2. [BUG FIXED]
Symptom: In eWC Content Filter-Schedule and Trusted, the settings can't be saved.
3. [BUG FIXED]
Symptom: WLAN hide ESSID can't work fine.
4. [BUG FIXED]
Symptom: Default ROM file setting is not correct.
Condition: 1. Baud rate should be 9600. 2. No default IPSec rule. 3. No default service name for PPPoE connection.
5. [BUG FIXED]
Symptom: In eWC, the check button of "Enable WLAN" doesn't work.
6. [BUG FIXED]
Symptom: In eWC VPN page, there is no NAT Traversal check button.
7. [BUG FIXED]
Symptom: Setting ENET ENCAP mode and SMT Menu 24.10 cause exception happened.
8. [BUG FIXED]
Symptom: Setting IPSec Phase 1 Encryption algorithm = 3DES, then VPN tunnel can't be established.
9. [BUG FIXED]

ZyXEL Confidential

- Symptom: WLAN and LAN can't communicate each other.
10. [BUG FIXED]
Symptom: In eWC Advanced Setup/Firewall/Antiprobng & Threshold click "Apply" button, it didn't jump to previous page.
 11. [BUG FIXED]
Symptom: Firewall log message has ZW string.
 12. [BUG FIXED]
Symptom: WLAN can't ping to DMZ port.
 13. [BUG FIXED]
Symptom: Can't edit firewall rule 0, it will cause system reboot.
 14. [BUG FIXED]
Symptom: Showing firewall/rule summary cause system exception.
 15. [BUG FIXED]
Symptom: LAN can't work after reset default ROM file.
 16. [BUG FIXED]
Symptom: In eWC Firewall/Rule Summary/Edit Rule first time click ADD button will appear error message
 17. [BUG FIXED]
Symptom: Not last firewall rule can move to any rule number. Ex, two rules exist then first rule could change to rule 10.
 18. [ENHANCEMENT]
Symptom: Support WLAN WPA/Dynamic WEP key function for B-120 wireless card.
 19. [ENHANCEMENT]
Symptom: Support Vantage function.
 20. [ENHANCEMENT]
Symptom: Support enhanced wan backup mechanism.
Condition: Nailed-up function of Dial backup node is no longer controlled by ISP node.

Modification in 3.40(IU.3)b1 | 11/19/2003

1. [FEATURE ENHANCE] Add Large ROM-File. Need to update bootbase.
2. [FEATURE ENHANCE] New Firewall Add Port Based VLAN, DMZ and extra Firewall rules.
3. [FEATURE ENHANCE] Add NAT traversal.
4. [BUG FIXED] VPN Can't Pass Through Router with NAT Traversal Truns On.
5. [FEATURE CHANGED] PPPoE will never dis-connect even if the internal host is shut down.
6. [FEATURE ENHANCEMENT] Add CI command "wlan active 1/0".
7. [FEATURE CHANGED] Change France and Singapore WLAN channel range to 1-13.
8. [BUG FIXED] IPSec client behind device can not establish IPSec connection to remote peer.

Modification in 3.40(IU.2)C1 | 10/22/2003

1. [BUG FIX] Set Menu1 Bridge=Yes in default ROM file.

Modification in 3.40(IU.2)b1 | 09/01/2003

1. [BUG FIX] Fix IPSec exception when using PPPoA.
2. [BUG FIX] Fix VPN can't ping after the VPN tunnel created and PFS turned on.

Modification in 3.40(IU.1)b1 | 07/07/2003

1. [BUG FIX] PPPoE pass through can't work when WLAN card is inserted.
2. [BUG FIX] PPPoE connection acts abnormally with Linux PPPoE server.
3. [BUG FIX] Bandwidth management cause PCMCIA hang-up.

Modification in 3.40(IU.0)c0 | 05/27/2003

1. [BUG FIX] PPPoE Client can't work if the first remote node is in bridge mode and smt menu1 routing set to yes.
2. [BUG FIX] smt menu1 select bridge should not affect the submenu 11.2 SUA selection.
3. [FEATURE ENHANCE] Add CI commands by TE request. "sys romreset <1:reboot|2:no reboot>", "sys atsh", "sys atwe <mac address> <country code> <debug flag> <feature bits> < 1:reboot|0:no reboot>", and "sys stdio 0 [seconds]".
4. [FEATURE ENHANCE] Change "sys smt on/off" from internal usage to hide.
5. [FEATURE ENHANCE] Enhance the CI command "sys proc stack" & "sys proc disp" to show the maximum stack usage for THREADX.
6. [BUG FIX] In Web GUI, Port speed select is not consistent with the dial backup advance GUI.
7. [FEATURE CHANGE] Modify WLAN default channel to CH06.

Modification in 3.40(IU.0)b10 | 05/20/2003

1. [FEATURE CHANGE] Modify Boot base product string from "P652HW-31" to "P652H/HW-31".
2. [FEATURE ENHANCE] Add SPTGen for MAC Filter, RADIUS, and IEEE802.1X.
3. [FEATURE ENHANCE] Enlarge FTP allocated buffer.
4. [FEATURE ENHANCE] Add Multi Language Web GUI.
5. [BUG FIX] Web GUI "wan.html" shows error if PPPoE pass through is selected "Yes".

Modification in 3.40(IU.0)b9 | 05/13/2003

1. [BUG FIX] Dial-Backup can't work because the configuration data is saved at wrong place.
2. [FEATURE ENHANCE] Add Telnet client. Use CI command "ip telnet <host>".
3. [FEATURE ENHANCE] Add IP trace route. Use CI command "ip traceroute <host> [ttl] [wait] [queries]".

Modification in 3.40(IU.0)b8 | 05/13/2003

1. [BUG FIX] Dial-Backup can't work if configured through Web GUI or SMT menu.
2. [BUG FIX] VPN Rule 9 and 10 can't be set.
3. [BUG FIX] Web Log page display garbage information.
4. [BUG FIX] Time zone's start date & end date has not consistent with SMT & web.
5. [FEATURE ENHANCE] WLAN will light on under "atgt" debug mode.

Modification in 3.40(IU.0)b7 | 05/02/2003

1. [BUG FIX] LED problem - DSL & ACT led can not turn off right now when system reboot.
2. [BUG FIX] Web problem - Maintenance->Diagnostic Page,ping non-IP format .The result show success.
3. [BUG FIX] SMT problem - If no wireless card plug on, both Web GUI and SMT won't show any information related to WLAN.
4. [BUG FIX] Web problem - Web page wireless mac filter set only 12 set.
5. [BUG FIX] VPN problem - Can not establish 5 VPN at same secure gateway tunnel.
6. [BUG FIX] Web problem - If no change to AUX port,access WAN backup page, sys reboot.
7. [BUG FIX] Web problem - No Time setting page.
8. [BUG FIX] SMT problem - Menu 24.3.3 no context.
9. [BUG FIX] VPN problem - Remote side disconnect the VPN tunnel,VPN still exist.
10. [BUG FIX] Exception problem - System maintenance log enable and drop pppoe connection will caused exception.
11. [FEATURE ENHANCE] VPN tunnel extend to 10 entries.
12. [BUG FIX] In HTP, if the wireless LAN card exist, the WLAN LED will be on.

Modification in 3.40(IU.0)b6 | 04/08/2003

1. [FEATURE ENHANCE] WAN Backup Funtion.
2. [FEATURE CHANGE] Modify HTP process to test UART external before testing WLAN Internal.
3. [BUG FIX] DHCP client doesn't release the IP address.
Symptom: DHCP client doesn't release the IP address when the IP address is expired
Condition: System is configured in "enet encap" (DHCP client), and sometimes DHCP server doesn't response in a period of time, when the lease time is expired system should release WAN IP address.
4. [BUG FIX] IPSec bug.
Symptom: Local and peer content can't change when ID type is IP with CI command.
Condition: "ipsec config lclIdContent" and "ipsec config peerIdcontent" can't change the value when ID type is IP.
5. [BUG FIX] NAT
Symptom: The router tries to search a GRE entry, but sometimes it will find an ESP entry.
Condition:
 1. There is an ESP entry in NAT session table.
 2. There is no other GRE entry in NAT session table.
 3. There is an GRE packet from outside to WAN.
6. [BUG FIX] IPSec Bug
Symptom: Sometimes IPSec rekey procedure failed.
Condition: Under heavy traffic, sometimes IPSec rekey failed.
Symptom: Even the parameter is correct, negotiation for IKE phase 1 may fail.
Condition: There are two types of conditions. 1) When two rules have same secure gateway address, sometimes the second tunnel cannot be established after the first one is built. 2) This situation also happens in rekey. If the initiator did not send DEL

phase 1 information packet first and then start another phase 1 negotiation directly, this negotiation may fail.

7. [BUG FIX] IPSec Bug

Symptom: IPSec rekey procedure is not stable.

Condition: 1) There exists an IPSec rule, it's Secure gateway address is domain name. And the phase 2 PFS is on, either DH1 or DH2. 2) Sometimes the IPSec rekey procedure will not work properly. 3) From the log, user will see ZyWALL only receives IKE packets but never responses.

8. [FEATURE CHANGED] IPSec

Symptom: Change the mechanism of initial contact in reboot detection (original: tunnel-based, now: machine-based).

Symptom: In the past, after phase 2 rekey, responder still use old phase 2 SA to transmit packets for a certain period and then started use the new phase 2 SA. Now responder will use new phase 2 SA after rekey immediately.

Symptom: In our previous design, "SA monitor" shows SAs including the old SA. So even the re-negotiated SA will be showed on SA monitor. In this case, after a tunnel re-keyed, there will be two SAs on SA monitor. The new behavior is that SA monitor just shows SA which is "non-negotiated", i.e., SA monitor shows new SA but skips old SA.

9. [FEATURE ENHANCED] IPSec

Symptom: When the remote address range and local address range overlap in a IPSec rule, packets from local to local can skip this rule for checking. For example, a rule: local=> start= 192.168.1.0 mask= 255.255.255.0; remote=> start= 192.168.0.0 mask= 255.255.0.0. Then user can define if a packet from 192.168.1.2 to 192.168.1.3 matches this rule.

Symptom: Add back the inbound idle timer. When a tunnel has no inbound traffic for a certain period, the tunnel will be dropped.

10. [FEATURE ENHANCED] Centralized Log

Symptom: Improve Log performance. Use a macro "NEED_LOG_PACKET" to determine dose the router need log or not.

11. [BUG FIXED] VCHunt

Symptom: (1) The exception is occurred if using "wan atm vchunt remove" to remove non-existed vcHunt table.

(2) The un-configured remoteNode (but active) would be saved the vcHunt result. This might cause system reboot.

12. [BUG FIXED] HWSAR

Symptom: (1) Hwsar atmCfgTable would be full if dropping the ADSL line eight times at ZD2001 platform under PPPoE encap. The would cause no packets would be transmitted or received.

(2) Hwsar atmCfgTable would be full if changing the VPI/VCI setting eight times at ZD2001 platform under PPPoE encap. This would cause no packets transmission or receive.

Modification in 3.40(IU.0)b5 | 04/03/2003

1. [BUG FIX] DHCP client doesn't release the IP address

Symptom: DHCP client doesn't release the IP address when the IP address is expired.

Condition: System is configured in "enet encap" (DHCP client), and sometimes DHCP server doesn't response in a period of time, when the lease time is expired system should release WAN IP address.

2. [BUG FIX] Centralize log Bug

Symptom: The errlog type does not match the centralized log type.

Condition: ERR_INFO will be logged into LOGS_TYPE_ERROR.

Reason: The translated function makes a wrong mapping between errlog & centralized log type.

3. [BUG FIX] IPSec Bug

Symptom: NAT router will create two session entries when building IPSEC tunnel.

Reason&Solution: When creating a new session entry for IPSEC port 500 incoming packets, it will not record the initiator cookie. Next the same packet comes will create a new session entry again. The solution is to record the initiator cookie.

Symptom: Can not save phase 1 ID in smt27.1.1

Condition: In IPSec setup page, when phase 1 ID type is IP and phase 1 ID content is empty, setting can not be saved in smt27.1.1, and the warning message "ID Content Should Be IP Format" shows at the bottom of smt27.1.1.

Symptom: When phase 1 ID check failed, IKE log didn't show the ID content correctly.

Condition: 1) Set Peer ID type = IP and leave Peer ID content as blank.

2) Set different ID content in the peer site.

3) Establish the tunnel. Due to phase 1 ID content is different, the procedure will fail. But in the log, "configured peer ID content" doesn't show correctly.

Reason: in proc_id(), there is no checking mechanism if ID content is blank.

Solution: Add a check. If peer ID content is blank, use secure gateway address as ID content.

Symptom: Two IPSec hosts can establish IPSec connection when one uses main mode and the other chooses aggressive mode.

Condition: When local and peer hosts use different IKE phase1 negotiation mode, they still can establish IPSec connection.

Solution: If the ipsec host is responder, it will check the IKE phase1 negotiation mode is the same or not.

4. [BUG FIX] Web Bug

Symptom: After Web Configurator - Wizard setup, all remote nodes will be changed.

Condition: All remote nodes will change to the same Route/Bridge mode with ISP node.

Solution: Remove call configRNodes() in SaveWizardData().

5. [BUG FIXED] Wireless bug with 802.1x

Symptom: Wireless WEP key in web page have probelm.

Condition: While device support 802.1x, set WEP key in web page can't pass RADIUS authenticate.

6. [BUG FIXED] Wireless bug

Symptom: Display wrong wireless card version.

Condition: Use CI command "wlan version" to display wireless card version, the primary firmware version is always same as secondary version.

ZyXEL Confidential

7. [FEATURE ENHANCED] On line switch multi_language.
8. [BUG FIX] Web Bug
Symptom: From RFC 1483/Bridge to PPPoE/Route, PC can not dial up.
Cause: The configured valued have saved to Device, but fail to correctly switch between Bridge and Routing mode.
9. [BUG FIX] Web Bug
Symptom: The function,spWrite802_1xEntry, been accessed in rpWLan_v.c when 802.1x pages are not needed.
Cause: Compiler flags, IEEE802_1X and RADIUS not add into the related files.
10. [BUG FIX] All LAN traffic is blocked.
Symptom: If product has FILTER_NETBIOS_BLOCK defined on ZD2001 platform, all LAN traffic will be blocked.
Cause: Miss judge NetBIOS packets.
11. [BUG FIX] ROM version increases by 1 every time the router reboot.
Symptom: If product has CYBER_PATROL, or CONTENT_FILTER defined, when every time the router reboot will cause "RomFile Version" and "RomFile Checksum" increased by 1.
Cause: When processing spConv(), the function will always update ROM file.
Solution: Avoid update ROM if Cyber Patrol parameters are already updated.
12. [FEATURE CHANGED] Change AT command "ATLD" to hide while turn off EngDebugFlag.
13. [BUG FIXED] Protected "rom-0" file, when user no login.

Modification in 3.40(IU.0)b4 | 03/12/2003

1. [BUG FIX] HTP test LAN external loop back fail.
2. [FEATURE ENHANCE] Add AUX External Loop Back Test in HTP.
3. [FEATURE ENHANCE] SMT4 will save empty login name and password instead of saving a space.

Modification in 3.40(IU.0)b3 | 03/12/2003

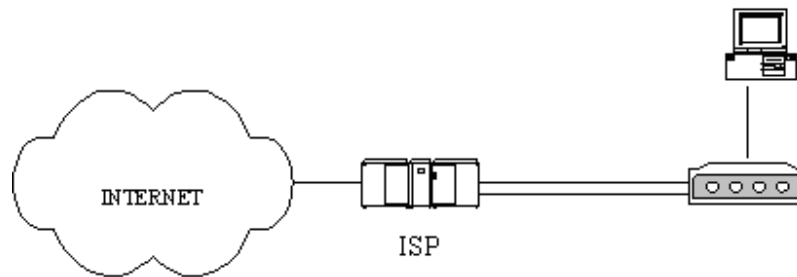
1. [FEATURE ENHANCE] Add DES ASIC in HTP.

Appendix 1: ZyXEL F/W Upgrade Tool

Network Environment:

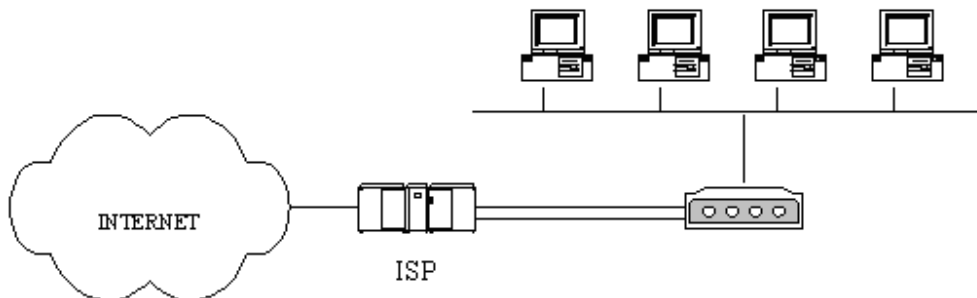
1. Prestige Modem Series

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



2. Prestige Router Series

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



Firmware Upgrade Procedure

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

Annex A CI Command List

Command Class List Table		
System Related Command	Exit Command	Ethernet Related Command
WAN Related Command	WLAN Related Command	IP Related Command
IPSec Related Command	PPP Related Command	Bridge Related Command
Radius Related Command	8021x Related Command	Firewall Related Command
Vantage Related Command		

System Related Command

[Home](#)

Command				Description
sys				
	adjtime			retrive date and time from Internet
	cbuf			
		display	[a f u]	display cbuf a: all f: free u: used
		cnt		cbuf static
			display	display cbuf static
			clear	clear cbuf static
	baud		<1..5>	change console speed
	callhist			
		display		display call history
		remove	<index>	remove entry from call history
	clear			clear the counters in GUI status menu
	countrycode		[countrycode]	set country code
	date		[year month date]	set/display date
	domainname			display domain name
	edit		<filename>	edit a text file
	enhanced			return OK if commands are supported for PWC purposes
	errctl		[level]	set the error control level 0:crash no save,not in debug mode (default) 1:crash no save,in debug mode 2:crash save,not in debug mode 3:crash save,in debug mode
	event			
		display		display tag flags information
		trace		display system event information
			display	display trace event
			clear <num>	clear trace event
	extraphnum			maintain extra phone numbers for outcalls
		add	<set 1-3> <1st phone num> [2nd phone num]	add extra phone numbers
		display		display extra phone numbers
		node	<num>	set all extend phone number to remote node <num>
		remove	<set 1-3>	remove extra phone numbers
		reset		reset flag and mask
	feature			display feature bit
	fid			
		display		display function id list
	firmware			display ISDN firmware type
	hostname		[hostname]	display system hostname
	iface			

ZyXEL Confidential

		disp	[#]	display iface list
	isr		[all used free]	display interrupt service routine
	interrupt			display interrupt status
	log			
		category		
			access [0:none/1:log]	record the access control logs
			attack [0:none/1:log/2:alert/3:both]	record and alert the firewall attack logs
			display	display the category setting
			error [0:none/1:log/2:alert/3:both]	record and alert the system error logs
			ipsec [0:none/1:log]	record the access control logs
			mten [0:none/1:log]	record the system maintenance logs
			upnp [0:none/1:log]	record upnp logs
			urlblocked [0:none/1:log/2:alert/3:both]	record and alert the web blocked logs
			urlforward [0:none/1:log]	record web forward logs
		clear		clear log
		display		display all logs
		errlog		
			clear	display log error
			disp	clear log error
			online	turn on/off error log online display
		load		load the log setting buffer
		mail		
			alertAddr [mail address]	send alerts to this mail address
			display	display mail setting
			logAddr [mail address]	send logs to this mail address
			schedule display	display mail schedule
			schedule hour [0-23]	hour time to send the logs
			schedule minute [0-59]	minute time to send the logs
			schedule policy [0:full/1:hourly/2:daily/3:weekly/4:none]	mail schedule policy
			schedule week [0:sun/1:mon/2:tue/3:wed/4:thu/5:fri/6:sat]	weekly time to send the logs
			server [domainName/IP]	mail server to send the logs
			subject [mail subject]	mail subject
		save		save the log setting buffer
		syslog		
			active [0:no/1:yes]	active to enable unix syslog
			display	display syslog setting
			facility [Local ID(1-7)]	log the messages to different files
			server [domainName/IP]	syslog server to send the logs
	mbuf			
		cnt		
			disp	display system mbuf count
			clear	clear system mbuf count
		link	link	list system mbuf link
		pool	<id> [type]	list system mbuf pool
		status		display system mbuf status
		disp	<address>	display mbuf status
		debug	[on off]	
	memory		<address> <length>	display memory content

ZyXEL Confidential

	memwrite		<address> <len> [data list ...]	write some data to memory at <address>
	memwl		<address>	write long word to memory at <address>
	memrl		<address>	read long word at <address>
	memutil			
		usage		display memory allocate and heap status
		mqueue	<address> <len>	display memory queues
		mcell	mid [f u]	display memory cells by given ID
		msecs	[a f u]	display memory sections
		mtstart	<n-mcell>	start memory test
		mtstop		stop memory test
		mtalloc	<size> [n-mcell]	allocate memory for testing
		mtfree	<start-idx> [end-idx]	free the test memory
	model			display server model name
	proc			
		display		display all process information
		stack	[tag]	display process's stack by a give TAG
		pstatus		display process's status by a give TAG
	queue			
		display	[a f u] [start#] [end#]	display queue by given status and range numbers
		ndisp	[qid]	display a queue by a given number
	quit			quit CI command mode
	reboot		[code]	reboot system code = 0 cold boot, = 1 immediately boot = 2 bootModule debug mode
	reslog			
		disp		display resources trace
		clear		clear resources trace
	stdio		[second]	change terminal timeout value
	time		[hour [min [sec]]]	display/set system time
	timer			
		disp		display timer cell
		trace	[on off]	set/display timer information online
		start	[tmValue]	start a timer
		stop	<ID>	stop a timer
	trcdisp			monitor packets
	trclog			
		switch	[on off]	set system trace log
		online	[on off]	set on/off trace log online
		level	[level]	set trace level of trace log #:1-10
		type	<bitmap>	set trace type of trace log
		disp		display trace log
		clear		clear trace
		call		display call event
		encapmask	[mask]	set/display tracelog encapsulation mask
	trcpacket			
		create	<entry> <size>	create packet trace buffer
		destroy		packet trace related commands
		channel	<name> [none incoming outgoing bothway]	<channel name>=enet0,sdsl00, fr0 set packet trace direction for a given channel
		string		enable smt trace log
		switch	[on off]	turn on/off the packet trace
		disp		display packet trace

ZyXEL Confidential

		udp		send packet trace to other system
			switch [on off]	set tracepacket upd switch
			addr <addr>	send trace packet to remote udp address
			port <port>	set tracepacket udp port
		parse	[[start_idx], end_idx]	parse packet content
		brief		display packet content briefly
	version			display RAS code and driver version
	view		<filename>	view a text file
	wdog			
		switch	[on off]	set on/off wdog
		cnt	[value]	display watchdog counts value: 0-34463
	romreset			restore default romfile
	server			
		access	<telnet ftp web icmp snmp dns> <value>	set server access type
		load		load server information
		disp		display server information
		port	<telnet ftp web snmp> <port>	set server port
		save		save server information
		secureip	<telnet ftp web icmp snmp dns> <ip>	set server secure ip addr
	spt			
		dump		dump spt raw data
			root	dump spt root data
			rn	dump spt remote node data
			user	dump spt user data
			slot	dump spt slot data
		save		save spt data
		size		display spt record size
		clear		clear spt data
	cmgr			
		trace		
			disp <ch-name>	show the connection trace of this channel
			clear <ch-name>	clear the connection trace of this channel
		cnt	<ch-name>	show channel connection related counter
	socket			display system socket information
	filter			
		clear		clear filter statistic counter
		disp		display filter statistic counters
		sw	[on off]	set filter status switch
		set	<set>	display filter rule
		netbios		
			disp	display netbios filter status
			config <0:LAN to WAN, 1:WAN to LAN, 2:LAN to DMZ, 3:IPSec passthrough, 4:Trigger Dial> <on off>	config netbios filter
	ddns			
		debug	<level>	enable/disable ddns service
		display	<iface name>	display ddns information
		restart	<iface name>	restart ddns
		logout	<iface name>	logout ddns
	cpu			
		display		display CPU utilization

Exit Command

[Home](#)

Command				Description
exit				exit smt menu

Ethernet Related Command

[Home](#)

Command				Description
ether				
	config			display LAN configuration information
	driver			
		cnt		
			disp <name>	display ether driver counters
			clear <name>	clear ether driver counters
		iface	<ch_name> <num>	send driver iface
		ioctl	<ch_name>	Useless in this stage.
		mac	<ch_name> <mac_addr>	Set LAN Mac address
		reg	<ch_name>	display LAN hardware related registers
		rxmod	<ch_name> <mode>	set LAN receive mode. mode: 1: turn off receiving 2: receive only packets of this interface 3: mode 2+ broadcast 5: mode 2 + multicast 6: all packets
		status	<ch_name>	see LAN status
		init	<ch_name>	initialize LAN
	version			see ethernet device type
	pkttest			
		disp		
			packet <level>	set ether test packet display level
			event <ch> [on/off]	turn on/off ether test event display
		sap	[ch_name]	send sap packet
		arp	<ch_name> <ip-addr>	send arp packet to ip-addr
		mem	<addr> <data> [type]	write memory data in address
	test		<ch_id> <test_id> [arg3] [arg4]	do LAN test
	pncconfig		<ch_name>	do pnc config
	mac		<src_ch> <dest_ch> <ipaddr>	fake mac address

WAN Related Command

[Home](#)

Command				Description
wan	adsl	bert		ADSL ber
		chandata		ADSL channel data, line rate
		close		Close ADSL line
		coding		ADSL standard current
		ctrleint		ADSL CTRL response command
		defbitmap		ADSL defect bitmap status
		dyinggasp		Send ADSL dyinggasp
		fwav		Test the ADSL F/W available ping
		fwdl		Download modem code, but must reset first
		linedata		
			near	Show ADSL near end noise margin
			far	Show ADSL far end noise margin

ZyXEL Confidential

		open		Open ADSL line
		opencmd		Open ADSL line with specific standard
		opmode		Show the operational mode
		perfdata		Show performance information,CRC,FEC, error seconds..
		rdata	[start] [length]	Read DSP CTRL registers 512 bytes
		reset		Reset ADSL modem, and must reload the modem code again
		selftest		
			long	ADSL long loop test
			short	ADSL short loop test
		status		ADSL status (ex: up, down or wait for init)
		version		ADSL version information
		vendorid		ADSL vendor information
		utopia		Show ADSL utopia information
		cellcnt		Show ADSL cell counter
		display		
			shutdown	Show the counter of rate adaptive mechanism happening
			rateup	Show real status that rate adaptive mechanism happened
		rateadap	[on off]	Turn on/off rate adaptive mechanism
		dumpcondition	[on off]	Turn on/off online debug information of rate adaptive mechanism
		sampletime	[mins]	Tune the sample time of rate adaptive mechanism
		noisegt	[dB]	if noise margin is 3db greater than before, and rate is worse than before, then system will do “L1 shutdown RA3”, default is 3db
		noisemargin	[dB]	if noise margin is greater than this value, and rate is worse than before, then system will do “L1 shutdown RA3”, default is 8db
		persisttime	[time]	when the adaptive condition is matched system will continue to monitor the time period “persisttime” before doing “L1 shutdown RA3”, default is 30 seconds
		timeinterval	[mins]	when “L1 shutdown RA3” is done twice, and still can’t reach the max rate which system recorded, it will delay a time period that the period base time is “timeinterval” before starting again. The time-based default is 2 hrs
		defectcheck	[on off]	Turn on/off detect table checking, default is on
		txgain	[value]	Set the CTRL register (0xc3), the value is from 0xfa to 0x06
		targetnoise	[value]	Set the CTRL register (0xc4), the value is from 0xfa to 0x06
		maxtonelimit	[value]	Set the CTRL register (0xc5), the value is from 0xfa to 0x06
		rxgain	[value]	Set the CTRL register (0xc6), the value is from 0xfa to 0x06
		txoutputpwr	[value]	Set the CTRL register (0xc7), the value is from 0xfa to 0x06
		rxoutputpwr	[value]	Set the CTRL register (0xc8), the value is from 0xfa to 0x06
		maxoutputpwr	[value]	Set the CTRL register (0xc9), the value is from

ZyXEL Confidential

				0xfa to 0x06
		errorsecond		
			sendes	Send current error second information immediately
		dygasprecover		
		dygasprecover	level [value]	By default is 100, after receiving 100 dying gasp system will reboot
		dygasprecover	active [on/off]	Turn on/off this mechanism
		rsploss	[1 0]	Turn on means to response signal loss of CTRL-E immediately, default is off
	atm	test	[fix rand period oam loopback]	Generate ATM traffic
	hwsar	disp		Display hwsar packets incoming/outgoing information
		clear		Clear hwsar packets information

WLAN Related Command

[Home](#)

Command				Description
wlan				
	version			Show WLAN AP F/W version

IP Related Command

[Home](#)

Command				Description
ip				
	address		[addr]	display host ip address
	loopbackaddr		<IP1> [IP2]	Set loopback address.
	alias		<iface>	alias iface
	aliasdis		<0 1>	disable alias
	arp			
		status	<iface>	display ip arp status
		add	<hostid> ether <ether addr>	add arp information
		resolve	<hostid>	resolve ip-addr
		drop	<hostid> [hardware]	drop arp
		flush		flush arp table
		publish		add proxy arp
	dhcp		<iface>	
		client		
			release	release DHCP client IP
			renew	renew DHCP client IP
		mode	<server relay none client>	set dhcp mode
		relay	server <serverIP>	set dhcp relay server ip-addr
		reset		reset dhcp table
		server		
			probecount <num>	set dhcp probe count
			dnsserver <IP1> [IP2] [IP3]	set dns server ip-addr
			winsserver <winsIP1> [<winsIP2>]	set wins server ip-addr
			gateway <gatewayIP>	set gateway
			hostname <hostname>	set hostname
			initialize	fills in DHCP parameters and initializes (for PWC purposes)
			leasetime <period>	set dhcp leasetime
			netmask <netmask>	set dhcp netmask
			pool <startIP> <numIP>	set dhcp ip pool

ZyXEL Confidential

			renewaltime <period>	set dhcp renew time
			rebindtime <period>	set dhcp rebind time
			reset	reset dhcp table
			server <serverIP>	set dhcp server ip for relay
			dnsorder [router isp]	set dhcp dns order
		status	[option]	show dhcp status
		static		
			delete <num> all	delete static dhcp mac table
			display	display static dhcp mac table
			update <num> <mac> <ip>	update static dhcp mac table
	dns			
		query		
			address <ipaddr> [timeout]	resolve ip-addr to name
			debug <num>	enable dns debug value
			name <hostname> [timeout]	resolve name to ip-addr
			status	display dns query status
			table	display dns query table
		server	<primary> [secondary] [third]	set dns server
		stats		
			clear	clear dns statistics
			disp	display dns statistics
		table		display dns table
	httpd			
		debug	[on off]	set http debug flag
	icmp			
		echo	[on off]	set icmp echo response flag
		data	<option>	select general data type
		status		display icmp statistic counter
		trace	[on off]	turn on/off trace for debugging
		discovery	<iface> [on off]	set icmp router discovery flag
	ifconfig		[iface] [ipaddr] [broadcast <addr> [mtu <value> dynamic]	configure network interface
	ifdrop		<iface>	chaek if iface is available.
	ping		<hostid>	ping remote host
	pong		<hostid> [<size> <time-interval>]	pong remote host
	route			
		status	[if]	display routing table
		add	<dest_addr default>[/<bits>] <gateway> [<metric>]	add route
		addiface	<dest_addr default>[/<bits>] <gateway> [<metric>]	add an entry to the routing table to iface
		addprivate	<dest_addr default>[/<bits>] <gateway> [<metric>]	add private route
		drop	<host addr> [/<bits>]	drop a route
		flush		flush route table
		lookup	<addr>	find a route to the destination
		errent		
			disp	display routing statistic counters
			clear	clear routing statistic counters
	status			display ip statistic counters
	adjTcp		<iface> [<mss>]	adjust the TCP mss of iface
	udp			
		status		display udp status
	rip			

ZyXEL Confidential

		accept	<gateway>	drop an entry from the RIP refuse list
		activate		enable rip
		merge	[on off]	set RIP merge flag
		refuse	<gateway>	add an entry to the rip refuse list
		request	<addr> [port]	send rip request to some address and port
		reverse	[on off]	RIP Poisoned Reverse
		status		display rip statistic counters
		trace		enable debug rip trace
		mode		
			<iface> in [mode]	set rip in mode
			<iface> out [mode]	set rip out mode
		dialin_user	[show in out both none]	show dialin user rip direction
	tcp			
		ceiling	[value]	TCP maximum round trip time
		floor	[value]	TCP minimum rtt
		irtt	[value]	TCP default init rtt
		kick	<tcb>	kick tcb
		limit	[value]	set tcp output window limit
		max-incomplete	[number]	Set the maximum number of TCP incomplete connection.
		mss	[value]	TCP input MSS
		reset	<tcb>	reset tcb
		rtt	<tcb> <value>	set round trip time for tcb
		status	[tcb] [<interval>]	display TCP statistic counters
		syndata	[on off]	TCP syndata piggyback
		trace	[on off]	turn on/off trace for debugging
		window	[tcb]	TCP input window size
	samenet		<iface1> [<iface2>]	display the ifaces that in the same net
	uninet		<iface>	set the iface to uninet
	tftp			
		support		prtn if tftp is support
		stats		display tftp status
	xparent			
		join	<iface1> [<iface2>]	join iface2 to iface1 group
		break	<iface>	break iface to leave ipxparent group
	antiprobe		<0 1> 1:yes 0:no	set ip anti-probe flag
	igmp			
		debug	[level]	set igmp debug level
		forwardall	[on off]	turn on/off igmp forward to all interfaces flag
		querier	[on off]	turn on/off igmp stop query flag
		iface		
			<iface> grouptm <timeout>	set igmp group timeout
			<iface> interval <interval>	set igmp query interval
			<iface> join <group>	join a group on iface
			<iface> leave <group>	leave a group on iface
			<iface> query	send query on iface
			<iface> rsptime [time]	set igmp response time
			<iface> start	turn on of igmp on iface
			<iface> stop	turn off of igmp on iface
			<iface> ttl <threshold>	set ttl threshold
			<iface> v1compat [on off]	turn on/off v1compat on iface
		robustness	<num>	set igmp robustness variable
		status		dump igmp status
	pr			

ZyXEL Confidential

		clear		clear ip pr table counter information
		disp		dump ip pr table counter information
		switch		turn on/off ip pr table counter flag
	nat			
		timeout		
			gre [timeout]	set nat gre timeout value
			iamt [timeout]	set nat iamt timeout value
			generic [timeout]	set nat generic timeout value
			reset [timeout]	set nat reset timeout value
			tcp [timeout]	set nat tcp timeout value
			tcpother [timeout]	set nat tcp other timeout value
		update		create nat system information from spSysParam
		iamt		display nat iamt information
		iface	<iface>	show nat status of an interface
		lookup	<rule set>	display nat lookup rule
		new-lookup	<rule set>	display new nat lookup rule
		loopback	[on/off]	turn on/off nat loopback flag
		reset	<iface>	reset nat table of an iface
		server		
			disp	display nat server table
			load <set id>	load nat server information from ROM
			save	save nat server information to ROM
			clear <set id>	clear nat server information
			edit active <yes/no>	set nat server edit active flag
			edit svrport <start port> [end port]	set nat server server port
			edit intport <start port> [end port]	set nat server forward port
			edit remotehost <start ip> [end ip]	set nat server remote host ip
			edit leasetime [time]	set nat server lease time
			edit rulename [name]	set nat server rule name
			edit forwardip [ip]	set nat server server ip
			edit protocol [protocol id]	set nat server protocol
		service		
			irc [on/off]	turn on/off irc flag
		resetport		reset all nat server table entries
		incikeport	[on/off]	turn on/off increase ike port flag

IPSec Related Command

[Home](#)

Command				Description
ipsec				
	debug	<1 0>		turn on/off trace for IPsec debug information
	route	lan	<on/off>	After a packet is IPsec processed and will be sent to LAN side, this switch is to control if this packet can be applied IPsec again.
				Remark: Command available since 3.50(WA.3)
		wan	<on/off>	After a packet is IPsec processed and will be sent to WAN side, this switch is to control if this packet can be applied IPsec again.
				Remark: Command available since 3.50(WA.3)
	show_runtime	sa		display runtime phase 1 and phase 2 SA information
		spd		When a dynamic rule accepts a request and a tunnel is established, a runtime SPD is created according to peer local IP address. This

ZyXEL Confidential

				command is to show these runtime SPD.
	switch	<on/off>		As long as there exists one active IPSec rule, all packets will run into IPSec process to check SPD. This switch is to control if a packet should do this. If it is turned on, even there exists active IPSec rules, packets will not run IPSec process.
	timer	chk_my_ip	<1~3600>	- Adjust timer to check if WAN IP in menu is changed
				- Interval is in seconds
				- Default is 10 seconds
				- 0 is not a valid value
		chk_conn.	<0~255>	- Adjust auto-timer to check if any IPSec connection has no traffic for certain period. If yes, system will disconnect it.
				- Interval is in minutes
				- Default is 2 minuets
				- 0 means never timeout
		update_peer	<0~255>	- Adjust auto-timer to update IPSec rules which use domain name as the secure gateway IP.
				- Interval is in minutes
				- Default is 30 minutes
				- 0 means never update
				Remark: Command available since 3.50(WA.3)
	updatePeerIp			Force system to update IPSec rules which use domain name as the secure gateway IP right away.
				Remark: Command available since 3.50(WA.3)
	dial	<rule #>		Initiate IPSec rule <#> from ZyWALL box
				Remark: Command available since 3.50(WA.3)
	display	<rule #>		Display IPSec rule #
	config	netbios	active <on/off>	Set netbios active flag
			group <group index1, group index2...>	Set netbios group
		name	<string>	Set rule name
		active	<Yes No>	Set active or not
		keyAlive	<Yes No>	Set keep alive or not
		lcIdType	<0:IP 1:DNS 2:Email>	Set local ID type
		lcIdContent	<string>	Set local ID content
		myIpAddr	<IP address>	Set my IP address
		peerIdType	<0:IP 1:DNS 2:Email>	Set peer ID type
		peerIdContent	<string>	Set peer ID content
		secureGwAddr	<IP address Domain name>	Set secure gateway address or domain name
		protocol	<1:ICMP 6:TCP 17:UDP>	Set protocol
		lcAddrType	<0:single 1:range 2:subnet>	Set local address type
		lcAddrStart	<IP>	Set local start address
		lcAddrEndMask	<IP>	Set local end address or mask
		lcPortStart	<port>	Set local start port
		lcPortEnd	<port>	Set local end port
		rmAddrType	<0:single 1:range 2:subnet>	Set remote address type
		rmAddrStart	<IP>	Set remote start address
		rmAddrEndMask	<IP>	Set remote end address or mask
		rmPortStart	<port>	Set remote start port
		rmPortEnd	<port>	Set remote end port

		antiReplay	<Yes No>	Set anitreplay or not
		keyManage	<0:IKE 1:Manual>	Set key manage
		ike	negotiationMode <0:Main 1:Aggressive>	Set negotiation mode in phase 1 in IKE
			preShareKey <string>	Set pre shared key in phase 1 in IKE
			p1EncryAlgo <0:DES 1:3DES>	Set encryption algorithm in phase 1 in IKE
			p1AuthAlgo <0:MD5 1:SHA1>	Set authentication algorithm in phase 1 in IKE
			p1SaLifeTime <seconds>	Set sa life time in phase 1 in IKE
			p1KeyGroup <0:DH1 1:DH2>	Set key group in phase 1 in IKE
			activeProtocol <0:AH 1:ESP>	Set active protocol in phase 2 in IKE
			p2EncryAlgo <0:Null 1:DES 2:3DES>	Set encryption algorithm in phase 2 in IKE
			p2AuthAlgo <0:MD5 1:SHA1>	Set authentication algorithm in phase 2 in IKE
			p2SaLifeTime <seconds>	Set sa life time in phase 2 in IKE
			encap <0:Tunnel 1:Transport>	set encapsulation in phase 2 in IKE
			pfs <0:None 1:DH1 2:DH2>	set pfs in phase 2 in IKE
		manual	activeProtocol <0:AH 1:ESP>	Set active protocol in manual
		manual ah	encap <0:Tunnel 1:Transport>	Set encapsulation in ah in manual
			spi <decimal>	Set spi in ah in manual
			authAlgo <0:MD5 1:SHA1>	Set authentication algorithm in ah in manual
			authKey <string>	Set authentication key in ah in manual
		manual esp	encap <0:Tunnel 1:Transport>	Set encapsulation in esp in manual
			spi <decimal>	Set spi in esp in manual
			encryAlgo <0:Null 1:DES 2:3DES>	Set encryption algorithm in esp in manual
			encryKey <string>	Set encryption key in esp in manual
			authAlgo <0:MD5 1:SHA1>	Set authentication algorithm in esp in manual
			authKey < string>	Set authentication key in esp in manual

PPP Related Command

[Home](#)

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

Bridge Related Command

[Home](#)

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

ZyXEL Confidential

		clear		clear bridge route counter
	stat			related to bridge packet statistic table
		disp		display bridge route packet counter
		clear		clear bridge route packet counter
	disp			display bridge source table

Radius Related Command

[Home](#)

Command				Description
radius				
	auth			show current radius authentication server configuration
	acco			show current radius accounting server configuration

8021x Related Command

[Home](#)

Command				Description
8021x				
	debug	level	[debug level]	set ieee802.1x debug message level
		trace		show all supplications in the supplication table
		user	[username]	show the specified user status in the supplicant table

Firewall Related Command

[Home](#)

Command				Description
sys				
	firewall			
		acl		
			disp	Display specific ACL set # rule #, or all ACLs.
		active	<yes no>	Active firewall or deactivate firewall
		ent		
			disp	Display firewall log type and count.
			clear	Clear firewall log count.
		pktdump		Dump the 64 bytes of dropped packet by firewall
		update		Update firewall
		dynamicrule		
		tcprst		
			rst	Set TCP reset sending on/off.
			rst113	Set TCP reset sending for port 113 on/off.
			display	Display TCP reset sending setting.
		icmp		
		dos		
			smtp	Set SMTP DoS defender on/off
			display	Display SMTP DoS defender setting.
			ignore	Set if firewall ignore DoS in lan/wan/dmz/wlan
		ignore		
			triangle	Set if firewall ignore triangle route in lan/wan/dmz/wlan

Vantage Related Command

[Home](#)

Command				Description
---------	--	--	--	-------------

ZyXEL Confidential

cnm	active	[0/1/2]		Display or set the CNM features to enable or disable . 0: disable 1: enable CNM features and communicate through WAN interface. 2: enable CNM features and communicate through WAN/LAN interfaces.
	sgid			Display sgid which is the unique ID of the device in Vantage.
	managerIP	[addr]		Display or set the IP of Vantage server/COMServer which manage this device. [addr] specifies the IP of the Vantage serve/COMServer.
	debug	[0/1/2/3<addr>/4<addr>]		Display or set the way of outputting CNM debug messages. 0: disable debug messages. 1: output the debug messages to console and can accept SGMP inquire message only after the device is registered to Vantage server. 2: output the debug message to console and accept SGMP inquire message even if the device is not registered to Vantage server. 3: output the debug messages to console and a remote server to log debug messages. 4: output the debug messages to a remote log server only and no console output.
	reset			Reset the state machine of SGMP and return to the state of SGMP_STATE_UNKNOWN. Device will re-register to Vantage server if CNM is active.
	encrykey	[string]		Display or set encryption key. [string] specifies the encryption key. to be set. Key length can not less than 8 alphanumeric characters long, if ecrymode is DES. Key length can not less than 24 alphanumeric characters long, if ecrymode is 3DES.
	encrymode	[0/1/2]		Display or set the encryption mode for SGMP messages. [0:NONE /1:DES/2:3DES] specifies the encryption mode to be set.