ZyXEL

Firmware Release Note

Prestige 324

Release 3.61(JA.3)C0

Date: February 26, 2004

Author: Jiffi Xu

Prestige 324 Standard Version
release 3.61(JA.3)C0
Release Note

Date: February 26, 2004

Supported Platforms:

Prestige 324

Versions:

ZyNOS Version : V3.61(JA.3) | 02/26/2004 14:42:28
Bootbase Version : V1.01 | 01/07/2003 14:32:40

Notes:

1. Click here to check CI command lists
2. When switch the AUX/CON slide switcher, the Prestige will reboot to change the Dial/Console Mode.
3. The user cannot config the Dial Backup in SMT menu 2 and eWC in CON mode.
4. The user cannot edit the Dial Backup eWC in CON mode. The Max incomplete TCP session is 20.
5. The user cannot use “aux” CI command set in CON mode.
6. Bypass the Triangle Route as default.
7. Switch the WAN MAC between Factory default and Spoof will cause while disconnect and cause the Lan and Wan LED lighten.
8. The NAT session is 1024.
9. Because the DNS setting mechanism is changed, the CI command “ip dns order” is obsolete and no longer available. Users can set the DNS setting in SMT 3.2 or in web MAIN MENU->LAN->IP page to make the behavior the same as before.
10. In order to switch connections among default WAN, traffic redirect and dial backup smoothly, we recommend user to activate the traffic redirect function and enter a valid IP address in the "Check WAN IP Address" in Web configurator WAN -> Traffic Redirect page.

Known Issues:

1. The Wizard page 3 cannot fetch correct “Remote IP Address” value in PPTP mode.
2. P324 only can use baud rate below 38400 bps to communicate with USR modem. Baud rate that exceeds 38400 bps cannot dial out.
3. Packet filter cannot work.
4. Under dial backup mode, when system switches back to PPPoE or PPTP encapsulation mode, the system cannot acquire DNS information from ISP. User needs to drop the connection and re-dial again in order to obtain the DNS information.

Features:

Modifications in V 3.61(JA.3)C0 | 02/26/2004

1. [FEATURE CHANGED] Formal release.

Modifications in V3.61(JA.3)b1 | 02/11/2004

2. [ENHANCEMENT]
   Add ADM 6996L switch chipset support.

Modifications in V 3.61(JA.1)C0 | 09/10/2003

3. [FEATURE CHANGED] Formal release.
4. [BUG FIX] Symptom: ROM file will be written when system is booted up. Condition: When system boots up, ROM file will be written sometimes.

Modifications in V 3.61(JA.0)C0 | 07/17/2003

5. [FEATURE CHANGED] Formal release.

Modifications in V 3.61(JA.0)b5 | 07/16/2003

6. [BUG FIX]
   Symptom & Condition: In web MAIN MENU->LAN page, the value "**Allow between LAN and WAN**" cannot be saved.
7. [BUG FIX]
   Symptom: Upgrade from 3.60(JA.5)C0 to 3.61(JA.0)b4, the DNS server setting is changed.
   Condition: 1. Setup two DNS servers on version 3.60(JA.5)C0 2. Upgrade firmware o 3.61(JA.0)b4 and keep original setting. 3. LAN PC gets the DNS server from ISP instead of user defined.
8. [BUG FIX]
   Symptom: User cannot set the static route rule in SMT 12.1.
   Condition: 1. Enter SMT 12.1 2. set destination IP address as 1.1.1.1, IP subnet mask as 255.255.0.0, and gateway IP address as 1.2.1.1

Modifications in V 3.61(JA.0)b4 | 07/10/2003

9. [BUG FIX]
   Symptom & Condition: In web MAIN MENU->SYSTEM->General page, the IP addresses of "System DNS Servers" fields are empty when router connects to Internet using dial backup.
10. [BUG FIX]
    Symptom: Cannot get LAN PC's MAC address.
    Condition: Using default rom file and change LAN subnet to 192.168.100.X. When changing WAN MAC address from factory default to LAN PC in web WIZARD page 3.
11. [BUG FIX]
    Symptom & Condition: While in routing mode (NAT = none) and firewall enabled, the WAN PC still can access LAN PC.
12. [BUG FIX]
    Symptom & Condition: Users cannot set the router's LAN IP address in the web MAIN MENU->LAN and in the SMT 3.2.
13. [BUG FIX]
    Symptom & Condition: When changing WAN IP address from static to dynamic, the default route rule does not disable automatically.
14. [ENHANCEMENT]
    Change some wording in the web help pages of MAIN MENU->SYSTEM->General, MAIN MENU->LAN->IP, and WIZARD page 3.
15. [ENHANCEMENT]
    Rearrange the sequence of help content in web MAINTENANCE->Configuration page.

Modifications in V 3.61(JA.0)b3 | 06/27/2003

16. [BUG FIX]
    Symptom & Condition: In web Maintenance->DHCP Table page, the DHCP table is always empty.

17. [BUG FIX]
    Symptom & Condition: In web Time Setting->Help page, the title should be “Time Setting” instead of “Time Zone”
18. [BUG FIX]
    Symptom & Condition: In SMT menu 2->Edit Advanced Setup, when moving cursor in "**Call Control**" fields, system will show some unknown characters.
19. [BUG FIX]
    Symptom & Condition: In SMT 11 (Remote Node Setup)->SMT 11.2 (Remote Node Profile)-> SMT 11.3 (Remote Node Network Layer Options), the IP address assignment is "**Static**".
20. [BUG FIX]
    Symptom & Condition: Integrated DNS GUI is unstable.
21. [BUG FIX]
    Symptom: The test page https://grc.com/x/ne.dll?bh0bkyd2 will show “closed” instead of “stealth” when “**Do not respond to requests for unauthorized services**” in MAIN MENU->REMOTE MGMT->Security is disabled and firewall is enabled.

Modifications in V 3.61(JA.0)b2 | 06/16/2003

22. [FEATURE CHANGE]
    Change GUI wording “SETUP” to “MAIN MENU”.
23. [BUG FIX]
    Symptom & Condition: In web MAIN MENU->SUA/NAT->Address Mapping page, edit a “Many One-to-One”, but the range does not match, and the status shows “Local Host Lan IP address and Local Host Wan IP address doesnot match”, the “doesnot” should be separated “does not”.
24. [BUG FIX]
    Symptom & Condition: In web MAIN MENU ->LAN->IP Alias page -- If an IP address is entered, the firmware does not compute a subnet mask. The IP Alias web screen and menu 3.2.1 shows the IP address and a subnet mask=0.0.0.0. If an IP is entered in menu 3.2.1, the firmware computes and displays the correct mask.
25. [BUG FIX]
    Symptom & Condition: In web MAIN MENU ->STATIC ROUTE, MAIN MENU ->WAN->WIN IP pages, and MAIN MENU ->WAN->Traffic Redirect page, the "**Metric**" value can over 15 and 0.
26. [BUG FIX]
    Symptom: The DNS server IP address in SMT1 and SMT3.2 is junk. Condition: 1. Choose “**User-Defined**” and enter “168.95.1.1” then save. 2. Choose “**From ISP**” and save. 3. Choose “**User-Defined**”.
27. [BUG FIX]
    Symptom & Condition: Using CI command “ip ping <router LAN or WAN IP>”, the ping reply packet is sometimes lost.
28. [FEATURE ENHANCEMENT]
    Add integrated DNS feature in the wizard page.
29. [BUG FIX]
    Symptom & Condition: LAN clients cannot get DNS server information from router when the WAN encapsulation mode is PPPoE or PPTP.
30. [BUG FIX]
    Symptom & Condition: Using CI commmand "ip ping www.kimo.com.tw" will cause router hang or crash.
31. [BUG FIX]
    Symptom & Condition: In web MAIN MENU ->MAINTENANCE->DHCP Table page, P324 does not need static DHCP feature.
32. [BUG FIX]
    Symptom & Condition: In web MAIN MENU ->LOGS->View Log page, all message fields are blank while ping or trace route.
33. [BUG FIX]
    Symptom & Condition: CI command - Trace commands: "sys trcp brief" and "sys trcp parse" misspell PPPoE *Session* packets. The word is "Session" not "Section".
34. [BUG FIX]

Symptom & Condition: In web MAIN MENU->SYSTEM->Time Setting page, "**Start Date**" is greater than "**End Date**".

35. [BUG FIX]
    Symptom & Condition: In SMT 12.1, the destination IP address and the gateway IP address can be in different subnet.
36. [FEATURE CHANGE]
    Remove "monitoring WAN connectivity" from centralized log.
37. [BUG FIX]
    Symptom & Condition: In Web MAIN MENU->WAN->ROUTE page, user cannot save the setting of traffic redirect priority.
38. [BUG FIX]
    Symptom & Condition: Road Runner can not work when firewall is enabled.
39. [BUG FIX]
    Symptom: CPU utilization is high even when the system is in idle state.
    Condition:
    1. The router stays in **idle** state.
    2. Use the CI command "sys cpu disp".
    3. The usage of the CPU will be about 16%~17%.
40. [BUG FIX]
    Symptom & Condition: All Connections to Internet are disconnected when the LAN clients open more than 20 web pages.

Modifications in V 3.61(JA.0)b1 | 05/06/2003

11. [NEW FEATURE]
    Support Integrated DNS, please refer to the Appendix 7.
12. [BUG FIX]
    [Symptom & Condition] The user cannot play XBox Live via Prestige 324.
13. [BUG FIX]
    Symptom & Condition: Run ping plotter and it will show lots of packet lost errors.
14. [BUG FIX]
    Symptom & Condition: The dial backup line won't be terminated after the failure has been recovered. This will happen when choosing an Internet point as the dial-backup check point.
15. [FEATURE CHANGE]
    Remove the example of the domain name of the Wizard web page 1.
16. [ENHANCEMENT]
    Add an error message when the "**Timeout**" is greater than "**Period**" value in the Traffic Redirect web page.
17. [BUG FIX]
    Symptom: System time is wrong.
    Condition: After Time calibration is complete, the system time will advance 1 hour. The user can check the system in SMT menu 24.10 or TimeZone web page.
18. [ENHANCEMENT]
    Checking the **Metric** value correction in the WAN Route web page. The correct metric value should be 1(Highest) ~ 15(Lowest).
19. [FEATURE CHANGE]
    Change the wording "Use Time Server when Bootup" to "**Time Protocol**", "Time Server IP Address" to "**Time Server Address**"in the SMT menu 24.10, TimeZone Web and help page.
20. [FEATURE CHANGE]
    Change the warning message "Must greater than 4 seconds" to "Must be at least 5 seconds" in the SMT menu 2.1 . This warning message will appear while the user tries to move away from a too small value (e.g. 1).
21. [BUG FIX]
    Symptom: PPPoE client will reconnect automatically.
    Condition: The Prestige 324 will not stay offline when using PPPoE: When manually disconnecting the router through menu 24.1, the P324 will be trigger the PPPoE dial because of the erroneous DNS lookup for "0.0.0.0" shortly afterwards.

22. [BUG FIX]
    Symptom & Condition: The user only can input 20 characters into the "**Time Server Address**" field in the TimeZone web page.
23. [BUG FIX]
    Symptom & Condition: The user can input invalid characters (e.g. test.com) into the "**User Specify IP Addr**" field in the DDNS web page.
24. [ENHANCEMENT]
    Add "**Retype to Confirm**" field in the Dial Backup web page.
25. [BUG FIX]
    Symptom & Condition: The help page of the SUA server web page is missing.
26. [BUG FIX]
    Symptom & Condition: The user can input invalid characters (e.g. test.com) into the "IP Address" and "IP Subnet Mask" field in the IP Alias web page.
27. [ENHANCEMENT]
    Add "**Restart**" button in the Maintenance web page so that the user can restart by the web page.
28. [ENHANCEMENT]
    Add the new romfile upload successfully web page in the Maintenance web page.
29. [ENHANCEMENT]
    Add CI command "sys upnp reserve [0|1]"(default value is 0, enable it will save the UPnP NAT rule to Flash.) to reserve UPnP NAT rules in flash after system bootup.
30. [NEW FEATURE]
    Support DHCP Relay function.
31. [BUG FIX]
    Symptom & Condition: SMT Menu 2 field "Edit Advanced Setup" remains set to "Yes" once it has been toggled in the CON mode. It should return to "No".
32. [BUG FIX]
    Symptom & Condition: Unselect "Remote Management"-->"Security"-->"Do not respond to requests for unauthorized service", the HTTP, TELNET and FTP service on the test web site still shows stealth. Test web site is "http://grc.com/x/ne.dll?bh0bkyd2".
33. [ENHANCEMENT]
    Add CI command "ip dropIcmp [0|1]"(default value is 0) to setup the Prestige 324 to drop ICMP fragment packets.
34. [BUG FIX]
    Symptom & Condition: Email log messages cannot be sent when the log schedule is changed from "HOURLY" to "NONE" and then changed back to "HOURLY" again.

Modifications in V 3.60(JA.4)b1 | 04/15/2003

1. [ENHANCEMENT] Add Prestige 324 product name at page title. The title of the web pages will show "ZyXEL Prestige 324 Broadband Access Router".
2. [BUG FIX]
   Symptom&Condition: When deleting a static route rule which its IP address = 0.0.0.0 and netmask = 0.0.0.0, the routing table's default route will be deleted.
3. [BUG FIX]
   Symptom: Configure the LAN IP on SMT menu 3.2, the system doesn't save the configuration.
   Condition: For example
   1. Set WAN IP to 192.168.2.1.
   2. Set WAN IP to dynamic IP.
   3. Set LAN IP to 192.168.2.1.
   4. The system doesn't save the configuration of step 3.
4. [NEW FEATURE] Support AIM (AOL instant messenger) version 5.1.3036
5. [ENHANCEMENT] In SMT menu 1.1, change words "IP Addr" to "IP Address".
6. [BUG FIX] Symptom & Condition: NAT router will create two session entries when building IPSEC tunnel.
7. [ENHANCEMENT] Add "Delete" button in the "STATIC ROUTE" web page to delete static route entry.
8. [BUG FIX]
   Symptom: "Enable firewall" check box will be automatically checked.

Condition: 1. Disable firewall check box.
2. Disable service blocking.
3. Firewall check box will be automatically selected.

9. [ENHANCEMENT] Add “Bypass Triangle Route” check box in the Firewall Setting web page.
10. [ENHANCEMENT] Add “Blocked Message” field Firewall Filter web page.
11. [ENHANCEMENT] Enlarge the NAT session to be “1024”
12. [BUG FIX]
Symptom: Default gateway will disappear
Condition: When deleting a static route rule which its IP address = 0.0.0.0 and netmask = 0.0.0.0, the routing table's default route will be deleted.
13. [BUG FIX]
Symptom & Condition: In SMT menu 24.10 set "Daylight Savings=Yes”, but in the TimeZone Web page, the "Daylight Savings" checkbox is not checked
14. [BUG FIX]
Symptom: "Enable firewall" check box will be automatically checked.
Condition: 1. Disable firewall check box.
2. Disable service blocking.
3. Firewall check box will be automatically selected.
15. [BUG FIX]
Symptom: "Trusted Computer IP Address" sometimes cannot work.
Condition: 1. Add an IP address in the “Trusted Computer IP Address” field of the Firewall Setting web page.
2. Connect to a Web server in the Internet that contains Java, Cookie or ActiveX.
3. The example that contains those components should not be blocked by router but it still is blocked.
16. [ENHANCEMENT] New login pages.
To prettify the login pages layout and add ZyXEL logo on the pages.
17. [FEATURE CHANGE] Hide "view error log" selection in SMT menu 24.3 "System Maintenance - Log and Trace".
18. [FEATURE CHANGE] Hide error log messages in centralized log.
19. [BUG FIX]
Symptom: PPTP cannot pass-through firewall
Condition: PPTP cannot pass-through firewall from WAN to LAN although port 1723 is forward to PPTP server behind Presrige 324 in SUA mode. When port 1723 is configured in SUA, GRE0 should be automatically allow from WAN to LAN to the same host where port 1723 is foward to.
20.[ENHANCEMENT] Add CI commands to configure UDP port NAT timeout CI command: "ip nat timeout udp [port] <seconds>". For more details, please refer to CI command list.
21.[FEATURE CHANGE] Change the “SYS LED is steady” to “PWR LED is steady” in the firmware upload sucessfully web page.

Modifications in V 3.60(JA.3)C0 | 04/02/2003

1.[BUG FIX]
Symptom: If firewall turns on, traffic redirect can not switch back the original Internet connection.
Condition: This problem only happens when the traffic redirect gateway is not on WAN. If the default Internet connection fails, router will switch routing to traffic redirect gateway. When firewall turns on and the original connection recovers, the routing can not switch back.
2.[NEW FEATURE] Supprt a set of CI command to change the WAN port speed.
ether edit load 2
ether edit speed <auto|10/half|10/full|100/half|100/full>
ether edit save

Modifications in V 3.60(JA.1)C0 | 02/19/2003

1.[FEATURE CHANGE]
Change the “Log Schedule” from “When Log is Full” to be “None” in the Log setting web page.
2.[FEATURE CHANGE]

Set the metric the of Dial Backup to be “15” in the WAN ROUTE web page.

3.[FEATURE CHANGE]
Enable the “SUA Only” of the Dial Backup.

4.[FEATURE CHANGE]
Set the default value of the “Rem IP Addr” to be “0.0.0.0” in the SMT menu 11.2.

Modifications in V 3.60(JA.0)C0 | 01/20/2003

1.First release.
2.[NEW FEATURE] Supprt Static Content filter.
3.[NEW FEATURE] Supprt Firewall and related Web pags. For more information, please refer to Appendix6
4. [NEW FEATURE] Supprt Timeout Mechanism, please refer to Appendix 5
5.[NEW FEATURE] Support UPNP. For more information, please refer Appendix 1.
6.[NEW FEATURE] Support Centralize Log, for more infotmation, please refer to Appendix 3.
7.[NEW FEATURE] Support Traffic Redirection and Dial Backup. For more information, please refer to Appendix 4.

Appendix 1 UPnP

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

Appendix 2 SUA Support Table

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

SUA Support Table

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

Appendix 3 Centralize Log

1. Introduction:

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

2. Policy:

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

3. CI commands:

sys logs					
	category				
		access		[0:none/1:log]	record the access control logs
		attack		[0:none/1:log/2:alert/3:both]	record and alert the firewall attack logs
		display			display the category setting
		error		[0:none/1:log/2:alert/3:both]	record and alert the system error logs
		ipsec		[0:none/1:log]	record the access control logs
		javablocked		[0:none/1:log]	record the java etc. blocked logs
		mten		[0:none/1:log]	record the system maintenance logs
		upnp		[0:none/1:log]	record upnp logs
		urlblocked		[0:none/1:log/2:alert/3:both]	record and alert the web blocked logs
		urlforward		[0:none/1:log]	record web forward logs
	clear				clear log
	display				display all logs
	errlog				
		disp			display log error
		clear			clear log error
		online		[on|off]	turn on/off error log online display
	load				load the log setting buffer
	mail				
		alertAddr		[mail address]	send alerts to this mail address
		display			display mail setting
		logAddr		[mail address]	send logs to this mail address
		schedule			
			display		display mail schedule
			hour	[0-23]	hour time to send the logs
			minute	[0-59]	minute time to send the logs
			policy	[0:full/1:hourly/2:daily/3:weekly/4:none]	mail schedule policy
			week	[0:sun/1:mon/2:tue/3:wed/4:thu/5:fri/6:sat]	weekly time to send the logs
		server		[domainName/IP]	mail server to send the logs
		subject		[mail subject]	mail subject
	save				save the log setting buffer

	syslog				
		active		[0:no/1:yes]	active to enable unix syslog
		display			display syslog setting
		facility		[Local ID(1-7)]	log the messages to different files
		server		[domainName/IP]	syslog server to send the logs

Appendix 4 Internet Connectivity Monitor, Traffic Redirect and Dial-Backup

Introduction

These features are used to keep Internet connectivity of the Prestige 324. The Connectivity Monitor is running at interval to detect if the Prestige 324 can reach a desired host/address or the adjacent upstream gateway. Once the Prestige 324 has detected the connectivity is broken, it tries to forward the traffic to another gateway that user has specified.

Menu 11.6 - Traffic Redirect Setup

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

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

(1) Configure "Active" to "YES" if you want this feature work.
(2) "Backup Gateway". When the primary ISP or the check point is unreachable, traffic will be handed over to this backup gateway. [In IP address format]
(3) "Metric". Please reference section "**Metric**"
(4) "Check WAN IP Address". The Connectivity Monitor will probe the connectivity to a check-point. In general case, this check-point is the adjacent upstream gateway, which is typically assigned by ISP. However, if user desires to check a more significant point on the Internet, it can be specified here. A special case should be noticed that, even the ISP is online, this check-point maybe not reachable. The hand-over mechanism will function when the check-point failed. Leave it to 0.0.0.0, and the Prestige 324 will take the upstream gateway as the default check-point.
(5) "Fail Tolerance" is the check failure upper limit. For example, if this value is 2. When Prestige 324 failed to reach the check-point at the 3rd try, Connectivity Monitor will invalidate the corresponding route and promote candidate to be the default route.
(6) "Period". The Connectivity Monitor will examine physical link signal and then probe the check-point at a interval of "period" seconds.
(7) "Timeout". The check-point is expected to response Prestige 324's probe within a reasonable time. After that, Prestige 324 will log a failure. When the fail tolerance is exceeded, traffic will be handed over to the candidate route.
(8) The probing mechanism employs ICMP echo request/reply. Some hosts or routers on Internet may discard such packets.

Menu 2 - Dial-Backup Setup

```
 Menu 2 - WAN Setup  MAC Address: Assigned By= Factory default IP
Address= N/A  Dial-Backup: Active= YES Phone Number= Port Speed=
115200 AT Command String: Init= at&fs0=0 Edit Advanced Setup= No
Press ENTER to Confirm or ESC to Cancel:
```

This menu setup the dial device, which is typically an analog modem or ISDN TA. To activate the dial device, please toggle "Avtive" to "YES".

Menu 11.1 - Backup ISP Setup

```
 Menu 11.1 - Remote Node Profile (Backup ISP)  Rem Node Name=
Backup route  Edit PPP Options= No Active= Yes                Rem
IP Addr= 0.0.0.0                          Edit IP= YES Outgoing:
Edit Script Options= No  My Login=  My Password= ********     Telco
Option:   Authen= CHAP/PAP              Allocated Budget(min)=
0   Pri Phone #= ?                 Period(hr)= 0   Sec Phone #=
Nailed-Up Connection= No                                 Session
Options:                                 Edit Filter Sets= No
Idle Timeout(sec)= 100  Press ENTER to Confirm or ESC to Cancel:
```

A valid pair of login username and password is required. And the phone number of ISP is required. Leave "Rem IP Addr" to 0.0.0.0 makes Prestige 324 try to get its IP address from ISP.

```
 Menu 11.3 - Remote Node Network Layer Options Rem IP Addr= 0.0.0.0
Rem Subnet Mask= 0.0.0.0 My WAN Addr= 0.0.0.0  Network Address
Translation= SUA Only Metric= 2 Private= No RIP Direction= Both
Version= RIP-2B Multicast= None  Enter here to CONFIRM or ESC to
CANCEL:
```

Typically, "Network Address Translation" should be "SUA Only".

Metric

Once the traffic redirect and dial-backup mechanism were activated, Prestige 324 will have 3 default routes to Internet. The first one is the normal route that designated by ISP or the static route mechanism; the second one is the traffic-redirect route (i.e. the backup gateway); the third one is the dial-backup route.

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

Normal route > Traffic-redirect route > Dial-backup route

For another example, if user want Prestige 324 to use dial-backup route prior than traffic-redirect route or even the normal route, all need to do is to make metric of dial-backup route to be "1" and the others to be equal to "2" (or greater).

C/I commands

A set of C/I commands are provided.

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

Note

(1) Turn off "RIP" in SMT3.2 is recommended.
(2) When traffic redirect is turned on, and encapsulation type is PPPOE or PPTP, "Nail-UP"

function in SMT11.1 will be enabled

(3) A useful WINDOWS commands "tracert" can be used to verify the packet routing.

(4) Connectivity Monitor can not be disabled. However, traffic redirect and dial-backup mechanism can be enabled/disabled independently.

(5) Because the primary ISP and the backup ISP may assign different WAN IP address to Prestige 324. When traffic have handed over from one ISP to the other, all exist connections may be forced to reconnect.

(6) The Prestige 324 support Console/Aux Dual mode which means the P324 can change 9-pin console port to be dial backup mode and console mode. To use this feature, please switch the slide switcher to be "AUX" and adopt a 9-pin DUV connector between the 9 pin console and RS-232.

Appendix 5 Web/Telnet/RS232 Timeout Mechanism

Introduction

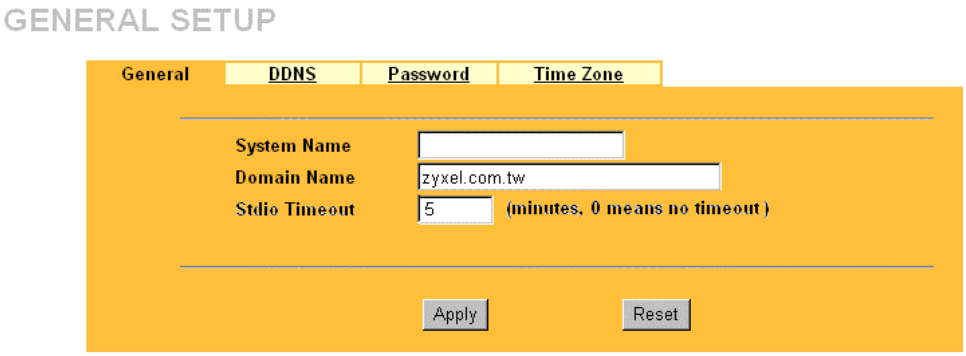
There are three ways to communicate with ZYXEL routers via web based GUI, SMT, or telnet. These interfaces have a common stdio timeout value, i.e., five minutes. Exceeding this value will cause routers to logout. The stdio timeout value can be changed using the CI command “sys stdio <minute>” in the period of runtime. This CI command changes the stdio timeout value in minutes. When one user enters “sys stdio 0”, it means that this user wants no stdio timeout with web-based, SMT, or telnet environment. Some users want to permanently change the value to a user-specified value even if the system is rebooted, so this stdio timeout value needs to be stored in the ROM.

CI command

Ex 1: “sys stdio” with no parameter will display the current stdio timeout value, i.e., 5 minutes.

Ex 2: “sys stdio 168” will change the stdio timeout value to 168 minutes for SMT, GUI, or telnet and save this value to ROM..

Web



Appendix 6 Firewall

Introduction

The Firewall policy of the Prestige 324 support change automatically.

1. **LAN-to-WAN** rules are local network to Internet firewall rules. The default is to forward all traffic from your local network to the Internet. You may choose to block certain **LAN-to-WAN** traffic in the **Services** screen (click the **Services** tab after you click the **Firewall** link). All services displayed in the **Blocked Services** list box are blocked **LAN-to-WAN** rules.

2. **WAN-to-LAN** rules are Internet to your local network firewall rules. The default is to block all traffic from your the Internet to your local network. You may allow traffic originating from the WAN to be forwarded to the LAN by configuring port forwarding rules in the **SUA Server** screen from the **SUA/NAT** link and in the **Address Mapping** screen from the same link when you configure **One-to-One** and **Many-One-to-One** mapping rules. Configure the Prestige 324 as forward the **NetBios** form Wan to Lan, the firewall automatically allows NetBIOS traffic through to LAN computers.

3. WAN-to-WAN/Prestige rules are Internet to the Prestige WAN interface firewall rules. The default is to block all such traffic unless you allow web, FTP, Telnet, SNMP, DNS or ICMP traffic by selecting WAN or LAN & WAN in the **Remote Management** screens. When you decide what **WAN-to-LAN** packets to log, you are in fact deciding what **WAN-to-LAN** and WAN-to-WAN/Prestige packets to log.

Web

Enable Firewall

Make sure this check box is selected to have the firewall protect your LAN from Denial of Service (DoS) attacks.

1. **LAN to WAN**
   All traffic originating from the LAN is forwarded unless you block certain services in the Services screen. All blocked LAN-to-WAN packets are considered alerts.
   Packets to Log: [No Log, Log Blocked, Log All]

2. **WAN to LAN**
   All traffic originating from the WAN is blocked unless you configure port forwarding rules, One-to-One mapping rules, Many-One-to-One mapping rules and/or allow remote management. Forwarded WAN-to-LAN packets are not considered alerts.
   Packets to Log: [No Log, Log Forwarded, Log All]

Note:

1. Only the log of the **Blocked** Services selected in the Firewall Serivce will be alert type(Red color).

2. Log of the Lan to Wan:

- **No Log**
- **Log Blocked** (log available services selected in the **Services** screen that appear in the **Blocked Services** textbox with **Enable Services Blocking** selected)
- **Log All** (log all **LAN to WAN** packets)

3. Log of the Wan to Lan: (include Wan to Wan/P324)

- **No Log**

- **Log Forwarded** (see how to forward WAN to LAN traffic above)
- **Log All** (log all **WAN to LAN** packets).

Appendix 7 Integrated DNS

Introduction

Domain name server is used to resolve domain name to an IP address or resolve IP address to domain name. The DNS server setting on the router has two parts.

One is the system DNS server on WAN for NTP, VPN, and DDNS to resolve domain names, and this system DNS server is for router use only. It may come from a DHCP message that is got from the Internet Service Provider. If the WAN is not a DHCP client, it cannot get any DNS server information from the Internet and there is no other way for WAN to set a DNS server for system use. So the default DNS is generated in this situation. The default DNS server is set to the ZyXEL DNS server and was hidden to users. When the WAN is set to DHCP none, the router can't get DNS server and the default DNS server is worked.

Another is the DNS servers which the router assigns to LAN hosts. When the hosts in the LAN are DHCP clients and the router is DHCP server, the router will pass the DNS server information to the LAN hosts. The hosts can use these DNS server information to resolve the domain names they need. The router will assign the following DNS servers to LAN host: (1). SMT menu 3.2 user configuration. (2). DNS server that is got from ISP. (3). LAN IP as DNS proxy.

Current DNS design has two problems. One is user can't set the default DNS configuration when the default DNS can't work. The default DNS server is hidden for users, and is set to ZyXEL DNS server IP. If the default DNS server IP has changed, users that using default DNS server IP maybe fail to access Internet. The best solution is to replace the default DNS server with user defined DNS server in SMT menu 1. When users choose DHCP none on the WAN setting, the router will show a warning message to users. It informs users to enter some user defined system DNS server IPs for router use. If users don't enter the DNS server information, some Internet accesses will not work. Another problem is what the DNS query order for router or LAN hosts used to query the domain name or IP. It does not have a brief setting to tell users what the DNS query order is and how to change the DNS query order. We will provide the DNS query order setting in the SMT, and GUI and make the DNS server setting friendly to users. The following is the method to improve the DNS architecture.

External Specification

【DNS Server】

There are three kinds of DNS servers on WAN:

1) DNS server that is got from ISP.
2) User configured DNS in SMT menu 1 or system->general (GUI).
3) None

There are four kinds of DNS servers on LAN:

1) DNS server that is got from ISP.
2) User configured DNS in SMT menu 3-2 or LAN->IP (GUI).
3) LAN IP as DNS server (Proxy mode).
4) None

【SMT menu 1】

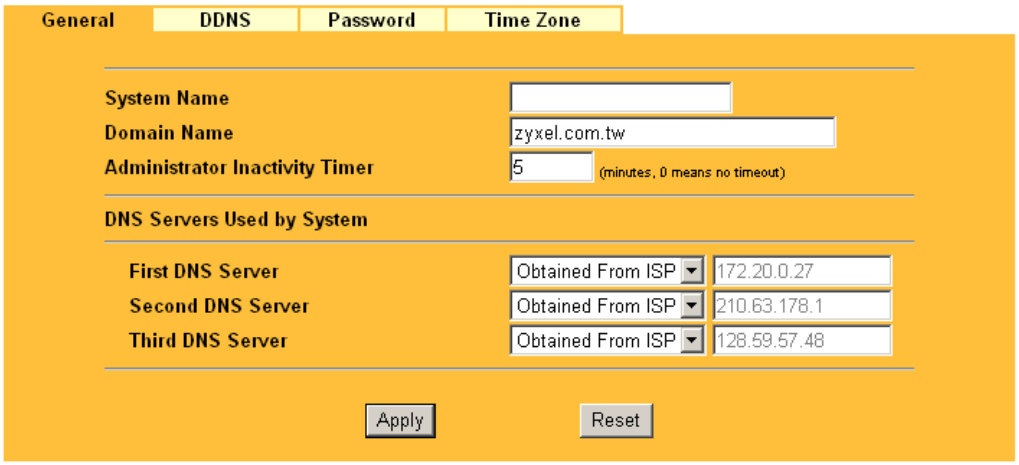
```
                Menu 1 - General Setup

        System Name= ?
        Domain Name=
        First System DNS Server= From ISP
          IP Address= N/A
        Second System DNS Server= From ISP
          IP Address= N/A
        Third System DNS Server= From ISP
          IP Address= N/A
        Edit Dynamic DNS= No









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

【SMT menu 3.2】

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


   DHCP= Server                    TCP/IP Setup:
   Client IP Pool:
     Starting Address= 192.168.1.33      IP Address= 192.168.1.1
     Size of Client IP Pool= 32        IP Subnet Mask= 255.255.255.0
   First DNS Server= From ISP          RIP Direction= Both
     IP Address= N/A                 Version= RIP-1
   Second DNS Server= From ISP           Multicast= None
     IP Address= N/A                 Edit IP Alias= No
   Third DNS Server= From ISP
     IP Address= N/A
   DHCP Server Address= N/A









                Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

【WEB ➔ Main Menu ➔ System ➔ General】

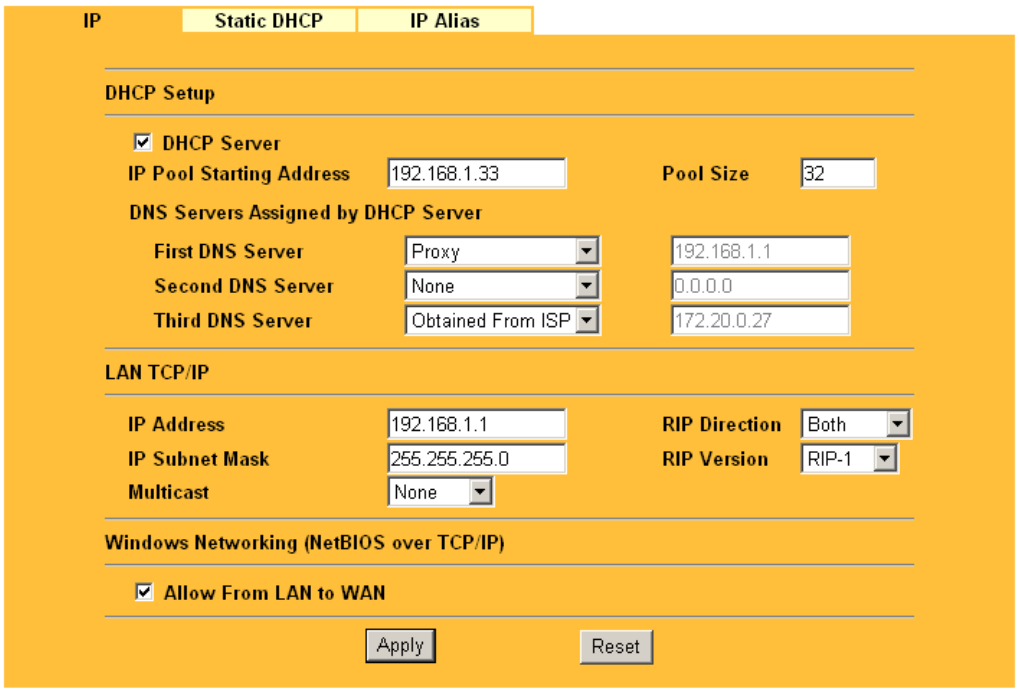
SYSTEM



Note：If WAN setting is DHCP none and users does not enter the IP address in the First DNS server field, the router will show a warning message to inform users that some connections maybe fail due to lack of DNS setting.

【WEB ➔ Main Menu ➔ LAN ➔ IP】

LAN



Annex A CI Commands

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

System Related Command
Home

Command				Description
Sys				
	adjtime			retrive date and time from Internet
			Display	display cbuf static
	callhist			
		display		display call history
		remove	<index>	remove entry from call history
	country code		[countrycode]	set country code
	date		[year month date]	set/display date
	domain name			display domain name
	edit		<filename>	edit a text file
	extraph num			maintain extra phone numbers for outcalls
		add	<set 1-3> <1st phone num> [2nd phone num]	add extra phone numbers
		display		display extra phone numbers
		node	<num>	set all extend phone number to remote node <num>
		remove	<set 1-3>	remove extra phone numbers
		reset		reset flag and mask
	feature			display feature bit
	hostna me		[hostname]	display system hostname
	logs			
		category		
			access [0:none/1:log]	record the access control logs
			display	display the category setting
			error [0:none/1:log/2:alert/3:both]	record and alert the system error logs
			javablocked [0:none/1:log]	record the java etc. blocked logs
			mten [0:none/1:log]	record the system maintenance logs
			upnp [0:none/1:log]	record upnp logs
			urlblocked [0:none/1:log/2:alert/3:both]	record and alert the web blocked logs
			urlforward [0:none/1:log]	record web forward logs
		clear		clear log
		display		display all logs
		dispSvrIP		Display the IP address of email log server and syslog server
		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
		updateSvrIP	<minute>	If there is one parameter <minute>, it will change the dns timer task timeout value. Otherwise, do dns resolve to find email log server and syslog server IP.
	pwderrtm		[minute]	Set or display the password error blocking timeout value.
	rn			
		load	<entry no.>	load remote node information
		disp	<entry no.>(0:working buffer)	display remote node information
		nat	<none|sua|full_feature>	config remote node nat
		nailup	<no|yes>	config remote node nailup
		save	[entry no.]	save remote node information
	stdio		[second]	change terminal timeout value
	time		[hour [min [sec]]]	display/set system time
	trcdisp			monitor packets
	trclog			
	trcpacket			
	version			display RAS code and driver version
	view		<filename>	view a text file
	wdog			
		switch	[on|off]	set on/off wdog
		cnt	[value]	display watchdog counts value: 0-34463
	romreset			restore default romfile

	socket			display system socket information
	filter			
		netbios		
			disp	display netbios filter status
			config <0:LAN to WAN, 1:WAN to LAN, 2:LAN to DMZ, 6:IPSec passthrough, 7:Trigger Dial> <on|off>	config netbios filter
	roadrunner			
		debug	<level>	enable/disable roadrunner service 0: diable <default> 1: enable
		display	<iface name>	display roadrunner information iface-name: enif0, wanif0
		restart	<iface name>	restart roadrunner
	ddns			
		debug	<level>	enable/disable ddns service
		display	<iface name>	display ddns information
		restart	<iface name>	restart ddns
		logout	<iface name>	logout ddns
	cpu			
		display		display CPU utilization
	upnp			
		active	[0:no/1:yes]	Activate or deactivate the saved upnp settings
		config	[0:deny/1:permit]	Allow users to make configuration changes. through UPnP
		display		display upnp information
		firewall	[0:deny/1:pass]	Allow UPnP to pass through Firewall.
		load		save upnp information
		reserve	[0:deny/1:permit]	Reserve UPnP NAT rules in flash after system bootup or not
		save		save upnp information

Exit Command

Home

Command				Description
Exit				exit smt menu

Ethernet Related Command

Home

Command				Description
Ether				
	config			display LAN configuration information
	driver			
		cnt		
			disp <name>	display ether driver counters
		ioctl	<ch_name>	Useless in this stage.
		status	<ch_name>	see LAN status
	version			see ethernet device type
	edit			

		load	<ether no.>	load ether data from spt
		speed	<auto|10/half|10/full|100/half|100/full>	set ether data speed
		save		save ether data to spt

IP Related Command

Home

Command				Description
Ip				
	address		[addr]	display host ip address
	alias		<iface>	alias iface
	aliasdis		<0|1>	disable alias
	arp			
		status	<iface>	display ip arp status
	dhcp		<iface>	
		client		
			release	release DHCP client IP
			renew	renew DHCP client IP
		status		show dhcp status
	dns			
		query		
		server	<primary> [secondary] [third]	set dns server
		stats		
	httpd			
	icmp			
		status		display icmp statistic counter
		discovery	<iface> [on|off]	set icmp router discovery flag
	ifconfig		[iface] [ipaddr] [broadcast <addr> |mtu <value>|dynamic]	configure network interface
	ping		<hostid>	ping remote host
	route			
		status	[if]	display routing table
		add	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add route
		addiface	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add an entry to the routing table to iface
		addprivate	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add private route
		drop	<host addr> [/<bits>]	drop a route
	smtp			
	status			display ip statistic counters
	udp			
		status		display udp status
	rip			
	tcp			
		status	[tcb] [<interval>]	display TCP statistic counters
	tftp			
	xparent			
		join	<iface1> [<iface2>]	join iface2 to iface1 group

		break	<iface>	break iface to leave ipxparent group
	urlfilter			
		exemptZone		
			display	display exemptzone information
			actionFlags [type(1-3)][enable/disable]	set action flags
			add [ip1] [ip2]	add exempt range
			delete [ip1] [ip2]	delete exempt range
			clearAll	clear exemptzone information
		customize		
			display	display customize action flags
			actionFlags [act(1-6)][enable/disable]	set action flags
			logFlags [type(1-3)][enable/disable]	set log flags
			add [string] [trust/untrust/keyword]	add url string
			delete [string] [trust/untrust/keyword]	delete url string
			clearAll	clear all information
	tredir			
		failcount	<count>	set tredir failcount
		partner	<ipaddr>	set tredir partner
		target	<ipaddr>	set tredir target
		timeout	<timeout>	set tredir timeout
		checktime	<period>	set tredir checktime
		active	<on|off>	set tredir active
		save		save tredir information
		disp		display tredir information
		debug	<value>	set tredir debug value
	nat		udp [port] <value>	set nat udp timeout value of specific port
	dropIcmp		[0|1]	Setup the device to drop ICMP fragment packets

Firewall Related Command

Home

Command				Description
sys	Firewall			
		acl		
			disp	Display specific ACL set # rule #, or all ACLs.
			delete	Delete specific ACL set # rule #.
		active	<yes|no>	Active firewall or deactivate firewall
		clear		Clear firewall log
		cnt		
			disp	Display firewall log type and count.
			clear	Clear firewall log count.
		debug		Set firewall debug level.
		disp		Display firewall log
		init		### nothing. ###
		mailsubject		
			disp	Display mail setting which is used to mail alert.
			edit	Edit mail setting.
		online		Set firewall log online.
		pktdump		Dump the 64 bytes of dropped packet by firewall
		tos		

			delete	Delete specific TOS session.
			display	Display TOS sessions.
			status	Display TOS sessions' status.
			dump	Dump TOS.
		tosctrl		
			destination	Display TOS destination hash
			incomplete	Display TOS incomplete List.
		update		Update firewall
		dynamicrule		
			display	Display firewall dynamic rules
		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		
			block_code3	Set ICMP block code3 on/off
			display	Display ICMP block code3 setting.
		dos		
			smtp	Set SMTP DoS defender on/off
			display	Display SMTP DoS defender setting.
			ignore	Set if firewall ignore DoS in lan/wan/dmz/wlan
		ignore		
			dos	Set if firewall ignore DoS in lan/wan/dmz/wlan
			triangle	Set if firewall ignore triangle route in lan/wan/dmz/wlan

AUX Related Command

Home

Command				Description
aux				
	atring		<device name>	Command the AT command to the device.
	cnt			
		disp	<device name>	display aux counter information
		clear	<device name>	clear aux counter information
	drop		<device name>	disconnect
	dump		<start#> <display#>	dump aux debug information
	init		<device name>	initialize aux channel
	mstatus		<device name>	display modem last call status
	mtype		<device name>	display modem type
	netstat		<device name>	prints upper layer packet information
	rate		<device name>	show tx rx rate
	redirect		<device name>	invalid
	signal		<device name>	show aux signal