# ZyXEL

**Firmware Release Note**

# Prestige 324

**Release 3.60(JA.5)C0**

**Date:** **Jun 02, 2003**
**Author:** **Gilbert Cheng**

# Prestige 324 Standard Version
# release 3.60(JA.5)C0
# Release Note

**Date: Jun 02, 2003**

## Supported Platforms:

Prestige 324

## Versions:

ZyNOS Version : V3.60(JA.5) | 06/02/2003 16:13:27
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 menu2 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. Bypass the Triangle Route as default.
6. Switch the WAN MAC between Factory default and Spoof will cause while disconnect and cause the Lan and Wan LED lighten.

## Known Issues:

## Features:

**Modifications in V 3.60(JA.5)C0 | 06/02/2003**

1. [NEW FEATURE]
   Support DHCP Relay function.

**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<br>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**

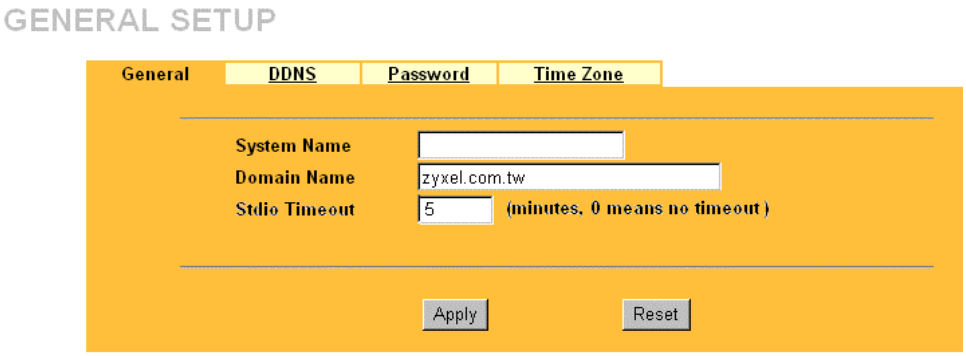
There are three ways to communicate with ZYXEL routers via web based GUI, SMT, or telnet. These interfaces have a common stdio timeout value, i.e., five minutes. Exceeding this value will cause routers to logout. The stdio timeout value can be changed using the CI command “sys stdio <minute>” in the 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).

## Annex A CI Commands

| Command Class List Table | | |
|---|---|---|
| System Related Command | Exit Command | IP Related Command |
| Ethernet Related Command | Firewall 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 |

Exit Command

Home

| Command | | | | Description |
|---|---|---|---|---|
| exit | | | | exit smt menu |

Ethernet Related Command

Home

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

IP Related Command

Home

| Command | | | | Description |
|---|---|---|---|---|
| ip | | | | |
| | address | | [addr] | display host ip address |
| | alias | | <iface> | alias iface |
| | aliasdis | | <0\|1> | disable alias |
| | arp | | | |

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

| | | | | |
|---|---|---|---|---|
| | | | add [string] [trust/untrust/keyword] | add url string |
| | | | delete [string] [trust/untrust/keyword] | delete url string |
| | | | clearAll | clear all information |
| | tredir | | | |
| | | failcount | <count> | set tredir failcount |
| | | partner | <ipaddr> | set tredir partner |
| | | target | <ipaddr> | set tredir target |
| | | timeout | <timeout> | set tredir timeout |
| | | checktime | <period> | set tredir checktime |
| | | active | <on\|off> | set tredir active |
| | | save | | save tredir information |
| | | disp | | display tredir information |
| | | debug | <value> | set tredir debug value |

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 |