



**Firmware Release Note**

## **ZyAIR G-2000PLUS**

**Release 3.60(HU.3)C0**

<b>Date:</b>	<b>November 22, 2005</b>
<b>Author:</b>	<b>Watties Lin</b>

## **ZyXEL ZyAIR G-2000PLUS Standard Version release 3.60(HU.3)C0 Release Note**

**Date:** November 22 2005

### **Supported Platforms:**

ZyXEL ZyAIR G-2000PLUS

### **Versions:**

ZyNOS Version: V3.60(HU.3) | 11/22/2005 10:31:00

BootBase : V1.02 | 11/02/2004 15:19:36

### **Notes:**

1. If Wireless Port Control (SMT Menu 23.4) is “Authentication Required”, ZyAIR will enable 802.1x/WPA/WPA-PSK user authentication mechanism, a wireless user must login the ZyAIR successfully before accessing network service. If Wireless Port Control is “No Authentication Required”, ZyAIR will allow all wireless users to access network service. If Wireless Port Control is “No Access Allowed”, ZyAIR will not allow wireless user to access network service.
2. ZyAIR supports external and internal RADIUS server, both of them use the same setting page (SMT Menu 23.2). The internal RADIUS server use EAP-PEAP/MS-CHAP-V2 to authenticate the client. If internal RADIUS server is desired, the server address is “127.0.0.1”, and shared secret is “don’t care”. “Don’t care” means whatever user key in, if server address is “127.0.0.1”, ZyAIR will use default shared secret “1234”. But leave blank is exception.
3. The Local User Database does not support key generation for 802.1x dynamic web key and WPA pairwise/group key.
4. Aegis client doesn't support self-signed certificate yet. If user wants to verify server certificate, please ask third party CA to sign certificate for G2000PLUS.

### **Known Issues:**

1. CNM Wireless LAN configuration is not ready.
2. LAN PC ftp to Linux ftp server will wait about 30 seconds.
3. LAN to WAN and WAN to LAN throughput is about 19Mbps~23Mbps.

### **CI Command List**

## Features:

### Modification in 3.60(HU.3)C0 | 11/22/2005

1. [FEATURE CHANGED]  
Convert to FCS version.

### Modification in 3.60(HU.3)b1 | 11/10/2005

1. [BUG FIXED]  
Symptom: G-2000PLUS will reboot when suffered DoS attack.  
Condition: There is a tool called ZyXELDOS can duplicate this problem.  
(1) STA associate with G-2000PLUS via wireless.  
(2) Run ZyXELDOS.exe in STA, and attack target is G-2000PLUS's management IP address.  
(3) G-2000PLUS exception occurred immediately.
2. [BUG FIXED]  
Symptom: Sony PSP WLAN reconnect problem with G-2000PLUS.  
Condition: Configure PSP to connect to G-2000PLUS w/wo static WEP, then do network test. The result is success at the first time. If PSP do network test again, it will get failed result.
3. [BUG FIXED]  
Symptom: Trigger port second rule can't work.  
Condition: PC1---WAN G-2000PLUS LAN---PC2  
(1) In GUI->SUA/NAT->trigger port, configure two rules.  
Rule 1 incoming port 1000, trigger port 2000.  
Rule 2 incoming port 3000, trigger port 4000.  
(2) Add firewall WAN to LAN relative rules.  
(3) Test rule 1 successful.  
(4) After test rule 1, test rule 2 fail.
4. [FEATURE ENHANCED]  
Check duplication of trust users when rules are active.
5. [BUG FIXED]  
Symptom: When G-2000PLUS enables the WPA-mixed mode. G-405 couldn't connect to AP successfully with WPA authentication.  
Condition: When G-2000PLUS enables the WPA-mixed mode. G-405 couldn't connect to AP successfully with WPA authentication from internal server or extend server.  
SPRID: 050617790
6. [BUG FIXED]  
Symptom: WPA-PSK should not enable mixed mode.  
Condition: In SMT23.4, select key management protocol as WPA-PSK, WPA mixed mode should not be enable.
7. [BUG FIXED]  
Symptom: In the reports of log. the "Direction" and "Amount" showed wrong information.  
Condition: In GUI->LOGS->Reports: The "Direction" and "Amount" showed wrong information.  
SPRID: 050728201
8. [BUG FIXED]  
Symptom: LAN to WAN and WAN to LAN throughput too low.  
Condition: No NAT and No Firewall. G-2000PLUS LAN to WAN and WAN to LAN throughput were about 9 Mbps. It was too low.  
SPRID: 050926377
9. [BUG FIXED]

Symptom: Using WinXP SP1 or SP2 WZC. Client didn't authenticate successfully from G-2000PLUS through G-560 or Linksys WAP54G.

Condition: (1) Client=WinXPSP1 or SP2 window zero configuration with G-162 or centrino 11g.

(2) AP= G-560 or Linksys WAP54G.

(3) PEAP server= G-2000PLUS.

(4) WZC client couldn't authenticate successfully from G-2000PLUS through G-560 or Linksys WAP54G.

(5) If you used the odyssey client. It could authenticate successfully.

SPRID: 050525648

**Modification in 3.60(HU.2)C0 | 06/20/2005**

1. [FEATURE CHANGED]  
Convert to FCS version.

**Modification in 3.60(HU.2)b1 | 05/27/2005**

1. [BUG FIXED]  
Symptom: Use system CI command: "IP PING address" cause system exception occurs.  
Condition: Repeat "IP Ping address" + "Ctrl + C" several times quickly, system exception will occur.
2. [BUG FIXED]  
Symptom: Aegis client can't work with G2000PLUS.  
Condition: When choose the wireless security mode as WPA or 802.1X dynamic WEP, and use internal PEAP server. The Aegis client can't authenticate with G2000plus successful.
3. [BUG FIXED]  
Symptom: G405 can't work with G2000PLUS.  
Condition: When choose the wireless security mode as WPA or 802.1X dynamic WEP, and use internal PEAP server. G405 can't authenticate with G2000plus successful.
4. [BUG FIXED]  
Symptom: Enable Intra BSS traffic, two G162 can't ping to each other.  
Condition: When choose the wireless security mode as 802.1X dynamic WEP, and use internal PEAP server. Two G405s can authenticate with G2000plus successful, but can't ping to each other.

**Modification in 3.60(HU.1)C0 | 04/08/2005**

1. [FEATURE CHANGED]  
Convert to FCS version.

**Modification in 3.60(HU.1)b1 | 03/30/2005**

1. [FEATURE CHANGED]  
Add Intra-BSS traffic blocking UI support in WEB GUI->wireless and SMT3.5.

**Modification in 3.60(HU.0)C0 | 02/03/2005**

1. [FEATURE CHANGED]  
Convert to FCS version.

**Modification in 3.60(HU.0)b7 | 01/26/2005**

1. [BUG FIXED]  
Symptom: Fragmentation Threshold should start from 800 bytes.

Condition: S1: In WEB GUI->wireless->wireless: the original boundary of fragmentation threshold is 256 ~ 2432, but the real boundary of wireless chip should be 800 ~ 2432.

S2: In SMT 3.5, the same situation happened.

2. [BUG FIXED]

Symptom: Wireless station can pass the authentication and access network when enable accounting server that didn't exist.

Condition: S1: In WEB GUI->wireless->wireless: choose WPA or 802.1X for security.

S2: Choose external RADIUS server.

S3: Configure authentication server, and setting accounting server if need.

S4: If accounting active is checked, but either the IP address or shared secret of accounting server or both are wrong. The wireless station can still pass the authentication and access network.

3. [FEATURE CHANGED]

In WEB GUI->wireless->wireless: when user select 802.1X+ static WEP or NO WEP, and using internal RADIUS server, the authentication databases can not be changed.

4. [BUG FIXED]

Symptom: After changing the name of automatically generated certificate, G2000PLUS reboot over and over.

Condition: S1: In WEB GUI->certificates->my certificates: choose the automatically generated certificate and press details button.

S2: Rename and press apply button.

S3: Turn off G2000PLUS and then turn it on.

S4: G2000PLUS reboot over and over.

5. [BUG FIXED]

Symptom: Wireless static WEP can not be configured.

Condition: S1: In WEB GUI->wireless->wireless: select static WEP and passphrase is empty then click generate button.

S2: Status will show "Please Input Passphrase".

S3: change security to "No Security" and press apply button.

S4: Status still shows the same message and can not be saved.

6. [BUG FIXED]

Symptom: In SMT, G2000PLUS often reboot with no reason.

Condition: In SMT, G2000PLUS often reboot with no reason.

7. [BUG FIXED]

Symptom: In SMT and telnet, G2000PLUS can key in two duplicate MAC address in MAC filter.

Condition: In SMT3.5.1, G2000PLUS can key in two duplicate MAC address.

8. [BUG FIXED]

Symptom: After STA re-authenticates more times, G2000PLUS reboot and hang up.

Condition: S1: In WEB GUI->wireless: configure security mode as WPA or 802.1x + dynamic 64/128 WEP, and change default re-authentication timer 1800 second to 10 second, then press apply.

S2: In WEB GUI->auth server->trusted user: add two new active user's accounts.

S3: Configure two wireless stations to connect to G2000PLUS.

S4: After two stations re-authenticate a period of times with G2000PLUS, G2000PLUS reboot and hang up.

**Modification in 3.60(HU.0)b6 | 12/22/2004**

1. [BUG FIXED]

Symptom: G2000PLUS does not send saved SSID.

Condition: S1: Reset default configuration.

S2: In WEB GUI->wireless: change the SSID from "ZyXEL" to "PQA-3274 G2000 PLUS" and apply.  
S3: STA rescan the available AP and can't find the SSID "PQA-3274 G2000 Plus" of G2000PLUS.  
S4: Use AiroPeek to capture the wireless packets. In the beacon, the SSID of G2000PLUS still shows "ZyXEL".  
S5: After restarted G2000PLUS. STA rescan available AP and find "PQA-3274 G2000 Plus".

2. [BUG FIXED]

Symptom: Four PCs run Chariot endpoint. After a long time, G2000PLUS's WLAN is down.  
Condition: S1: One PC runs as Chariot console, and four PCs run as Chariot endpoints.  
S2: Two of the four PCs run the script "Filesndl" to send packets to the console PC.  
S3: The other two of the four PCs run the script "Filesndl" to receive packets from the console PC.  
S4: After a long time, G2000PLUS's WLAN is down.

3. [BUG FIXED]

Symptom: In WEB GUI, update the ras code, G2000PLUS hang up and can't work again.  
Condition: S1: In WEB GUI->wireless: change security mode to WEP or 802.1X or WPA.  
S2: In WEB GUI->maintenance: select the location of firmware and press apply.  
S3: G2000PLUS hang up and can't work again.

4. [BUG FIXED]

Symptom: After STA re-authenticates more times, G2000PLUS reboot and hang up.  
Condition: S1: In WEB GUI->wireless: configure security mode as WPA or 802.1x + dynamic 64/128 WEP, and change default re-authentication timer 1800 second to 10 second, then press apply.  
S2: In WEB GUI->auth server->trusted user: add two new active user's accounts.  
S3: Configure two wireless stations to connect to G2000PLUS.  
S4: After two stations re-authenticate a period of times with G2000PLUS, G2000PLUS reboot and hang up.

5. [FEATURE ENHANCED]

Add "Note: When you are saving your certificate, use ".cer" or ".crt" as the file name extension" in certificates help page to note user.

**Modification in 3.60(HU.0)b5 | 11/30/2004**

1. [FEATURE ENHANCED]

Support LAN port link up/down status detection.

2. [FEATURE CHANGED]

Change wireless default ESSID from "wireless" to "ZyXEL".

3. [BUG FIXED]

Symptom: System shows Management FreeQ related error message.  
Condition: In WEB GUI->maintenance->configuration: select ROM files to restore, error message occurs and restore configuration fail.

4. [BUG FIXED]

Symptom: System shows WPA/WPA-PSK related error message.  
Condition: In SMT23.4, select key management protocol as WPA or WPA-PSK, error message "Set attachment fail" occurs when system reboot.

5. [FEATURE CHANGED]

Change browser title to "ZyXEL G-2000PLUS".

6. [BUG FIXED]

Symptom: When type invalid Mac data, G2000PLUS show error message "invalid Mac address #1"  
Condition: In WEB GUI->wireless->MAC filter: When type invalid Mac data, DUT show error message "invalid Mac address #1".

7. [BUG FIXED]

Symptom: Legal trusted user name can't be authenticated successful.

Condition: In Web GUI->auth server->trusted user: can save user name like: [test@aaa.bbb](mailto:test@aaa.bbb), but this user name can't be authenticated successful.

8. [FEATURE ENHANCED]

Support WZC (windows wireless zero configure) domain name input, but the response is don't care. It's meaning system will treat user1/domain1, user1/domain2 as the same one.

9. [BUG FIXED]

Symptom: User can key in illegal character.

Condition: In WEB GUI->auth server->trusted user: system will not check if user key in illegal character.

10. [BUG FIXED]

Symptom: System hangs on in WPA or WPA-PSK mode.

Condition: Configure as WPA or WPA-PSK mode. When user disables Wireless, system hangs on then exception when reach the WPA Broadcast/Multicast Key Update Timer.

**Modification in 3.60(HU.0)b4 | 11/16/2004**

1. [FEATURE ENHANCED]

Add preamble configuration and ON/OFF wireless blue LED in WEB GUI and SMT3.5. Add edit roaming configuration in SMT3.5.

2. [FEATURE CHANGED]

Enlarge firewall buffer to 20K or maximum 300 rules.

3. [FEATURE ENHANCED]

Add default NTP server support (time.nist.gov--192.43.244.18).

4. [FEATURE CHANGED]

In wizard setup steps 2, add description of basic and extend security.

5. [FEATURE CHANGED]

Change wireless default roaming port from 16290 to 3517.

6. [FEATURE ENHANCED]

Add new help web page of Auth. Server and Certificates, and correct wrong help web page of Wireless and firewall.

7. [BUG FIXED]

Symptom: In WEB GUI, the DNS setting can set any IP address. And some issue in others interface.

Condition: In WEB GUI->LAN->IP: the DNS setting can accept any IP address include illegal IP address unless 0.0.0.0.

8. [BUG FIXED]

Symptom: SUA/NAT Trigger Port function has a saving problem

Condition: In Web GUI->SUA/NAT->Trigger Port: Edit Rule 1, then click"Apply", it will always show an error message"Valid port range: 1~65535"g.

9. [BUG FIXED]

Symptom: Using FTP client connected to G2000PLUS, system exception will occur.

Condition: S1: Using TFTP client put wrong ROM file to DUT through LAN.

S2: Update ROM file can't successfully.

S3: Using FTP client connected to G2000PLUS through LAN.

S4: System exception occurs.

10. [BUG FIXED]

Symptom: G2000PLUS assigns the WAN IP address to my LAN computer when it reboots.

Condition: When system reboot, LAN side PCs will get IP addresses assigned by WAN side DHCP server.

11. [BUG FIXED]

Symptom: G2000PLUS doesn't support pass phrase function. But it was show on the static WEP of WEB UI.

Condition: In WEB GUI->wireless->security: choose static WEP or 802.1x+static WEP, pass phrase button will appear.

12. [BUG FIXED]

Symptom: Wireless Station can't authenticate successfully after the first time setting of G2000PLUS.

Condition: S1: Reset the G2000 PLUS.

S2: Configure the trusted user in AUTH.SERVER functions from the G2000 PLUS.

S3: To configures the internal RADIUS Server in wireless function.

S4: To configures clients with 802.1x-PEAP authentication.

S5: The clients associate to G2000 PLUS with PEAP authentication.

S6: The clients can't authenticate with G2000 PLUS successfully.

S7: You must restart the G2000 Plus, client can authenticate with G2000 Plus successfully.

13. [BUG FIXED]

Symptom: In WEB GUI, when you key in wrong DHCP pool value. G2000PLUS shows wrong information.

Condition: In WEB GUI, when you key 99999 on DHCP pool function. G2000PLUS show "An error was detected on the this page. y<- HTML item value: 99999" wrong information.

14. [BUG FIXED]

Symptom: Interoperability of 802.1X with G-560 fail.

Condition: Connecting G-560 WAN port to G2000PLUS LAN port and using G2000PLUS as authentication server. Wireless stations connect to G-560, and authenticate fail.

15. [FEATURE ENHANCED]

Add wireless 64/128 bits static WEP pass phrase support in WEB GUI.

16. [FEATURE ENHANCED]

Add EAP/PEAP validate server certificate support.

17. [BUG FIXED]

Symptom: Low wireless throughput.

Condition: G-2000+ has low throughput about TX/RX=13/13 Mbps.

18. [BUG FIXED]

Symptom: System exception and reboot occur when system name is up to 30 characters long and enable 802.1X.

Condition: S1: Set SMT 1 System Name more than 16 characters.

S2: Enable 802.1X or WPA.

S3: User association.

S4: System exception occurs.

19. [BUG FIXED]

Symptom: SIP pass through cannot work well with P2002 when using P2P

Condition: S1: Build the topology like this:

phone1—P2002\_1—G2000PLUS\_1—G2000PLUS\_2—P2002\_2—phone2.

S2: Create P2P phone book at phone1 and phone2.

S3: Dial from phone1 to phone2 will fail.

20. [BUG FIXED]

Symptom: After STA re-authenticates more times from DUT. DUT doesn't work

Condition: S1: G500: Setting 802.1x authentication and 10 seconds todo re-authentication on time.

S2: STA: STA connect to G500 with 802.1x-PEAP authentication from G2000Plus.

S3: STA can authenticate successfully and it can get dynamic IP from G2000Plus. STA can ping G2000Plus.

S4: After STA re-authenticate more times from G2000Plus through the G500. STA can't ping G2000PlusServer. G2000Plus was exception.

S5: SMT hang on when DUT reboot.

S6: G2000Plus must cold restart and work again.

### **Modification in 3.60(HU.0)b3 | 09/29/2004**

1. [BUG FIXED]  
Symptom: In WEB GUI, when key in wrong RTS/CTS, Fragmentation values, system shows a wrong message.  
Condition: In WEB GUI->wireless: When key 9999 on RTS/CTS, Fragmentation text box. System shows "An error was detected on this page. y<- HTML item value: 9999". It should be "RTS/CTS Threshold value error" and "Fragmentation Threshold value error".
2. [BUG FIXED]  
Symptom: SMT24.6. Restore configuration out of function.  
Condition: In SMT24.6, system can't restore configuration file and hang up.
3. [BUG FIXED]  
Symptom: In WEB GUI and SMT11. System can't save the Remote IP address and Remote IP subnet mask on PPTP function.  
Condition: In SMT11->encapsulation=PPTP, edit IP=yes->IP address assignment=static:  
And in WEB GUI->WAN->ISP->encapsulation=PPTP, WEB GUI->WAN->IP: system can't save the Remote IP address and Remote IP subnet mask.
4. [BUG FIXED]  
Symptom: System exception occurs and can be duplicated while we set SUA server function from WEB GUI.  
Condition: In Web GUI-> SUA/NAT-> SUA server: Issue a default server, then press applies twice, system exception occurs.
5. [BUG FIXED]  
Symptom: It has two" Press Enter to Confirm or ESC to cancel:" message in Menu 4.  
Condition: Some items of SMT4 show redundant message" Press Enter to Confirm or ESC to Cancel:"
6. [BUG FIXED]  
Symptom: The SUA server function can not work and can't ping to WAN IP from WAN side while SUA server set.  
Condition: In Web GUI-> SUA/NAT-> SUA server: Issue a default server, the related WAN to LAN firewall rule is incorrect, so default server is out of function.
7. [BUG FIXED]  
Symptom: LAN to LAN/ZyAIR firewall function can't work in default action and ACL rule.  
Condition: In WEB GUI->firewall->default rule->(W)LAN to (W)LAN/ZyAIR: change default action from forward to block is not work. And In eWC->firewall->rule summary-> (W) LAN to (W) LAN/ZyAIR: Configure a rule to block packets from LAN side but fail.
8. [BUG FIXED]  
Symptom: The system displays" within 3 .....seconds" while system power on.  
Condition: The system displays" Press any key to enter debug mode within 3 .....seconds" while system power on, but it should be "Press any key to enter debug mode within 3 seconds."
9. [BUG FIXED]  
Symptom: Connection-specific DNS suffix not work.  
Condition: In WINDOWS->start->run->cmd->ipconfig-> Connection-specific DNS suffix: can't display related DNS suffix, while all of the environment and setting are correct.

10. [BUG FIXED]

Symptom: System shows a message “request too large”, when configure trusted user.

Condition: In WEB GUI->AUTH SERVER->TRUSTED User, key in 32 pairs of user name and password with maximum length, system will show a error message “request too large”.

11. [BUG FIXED]

Symptom: Firewall doesn't save rule anymore, while its storage space is still not full.

Condition: In WEB GUI->firewall->rule summary->any packet direction: Storage space about 76%, create a new rule in any direction, but system doesn't save it.

12. [FEATURE ENHANCED]

Add WLAN Quick Bridge to enhance the performance of LAN<->WLAN.

**Modification in 3.60(HU.0)b2 | 08/19/2004**

1. [BUG FIXED]

Symptom: HTP test “LAN external loop back” has no response.

Condition: Enter debug mode, ATGT will run some internal and external loop back test. When testing goes on “LAN external loop back”, system will hang on.

2. [BUG FIXED]

Symptom: Console shows unreadable symbols.

Condition: Enter debug mode, under baud rate 9600, using ATWE to change MAC address. If successful, system will print “OK”, but show unreadable symbols.

3. [BUG FIXED]

Symptom: 802.1 x clients have been authenticated fail.

Condition: In 802.1x mode, authentication server selects a large size certificate will cause client been authenticated fail and timeout.

**Modification in 3.60(HU.0)b1 | 08/10/2004**

1. First firmware release

**CI Command List**

Command Class List Table		
<a href="#">System Related Command</a>	<a href="#">Exit Command</a>	<a href="#">Ethernet Related Command</a>
<a href="#">Wireless LAN Related Command</a>	<a href="#">IP Related Command</a>	<a href="#">Bridge Related Command</a>
<a href="#">Radius Related Command</a>	<a href="#">802.1x Related Command</a>	<a href="#">Certificates</a>
<a href="#">Radserv</a>		

System Related Command

[Home](#)

Command				Description
sys				
	Adjtime			retrive date and time from Internet
	Callhist			
		display		display call history
		remove	<index>	remove entry from call history
	countrycode		[countrycode]	set country code
	Date		[year month date]	set/display date
	domainname			display domain name
	Edit		<filename>	edit a text file
	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
	Hostname		[hostname]	display system hostname
	Log			
		clear		clear log error
		disp		display log error
		online	[on/off]	turn on/off error log online display
	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
	systemname		[system name]	Change system name
	time		[hour [min [sec]]]	display/set system time
	Trcdisp	parse, brief, disp		monitor packets
	Trclog			
	Trcpacket			
	Syslog			
		server	[destIP]	set syslog server IP address
		facility	<FacilityNo>	set syslog facility
		type	[type]	set/display syslog type flag
		mode	[on/off]	set syslog mode
	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		
	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
	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

## 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
		save		save ether data to spt

## Wireless LAN Related Command

[Home](#)

Command				Description
wlan				
	active		[on off]	set on/off wlan
	association			display association list
	chid		[channel id]	set channel
	diagnose			self-diagnostics
	essid		[ess id]	set ESS ID
	scan			scan wireless channels
	version			display WLAN version information

## 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	[option]	show dhcp status
	dns			
		query		
		server	<primary> [secondary] [third]	set dns server
		stats		
		default		set default DNS server
	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
	status			display ip statistic counters
	udp			
		status		display udp status
	rip			
	tcp			
		status	[tcb] [<interval>	display TCP statistic counters
	telnet		<host> [port]	execute telnet client command

	tftp			
	tracert		<host> [ttl] [wait] [queries]	send probes to trace route of a remote host
	xparent			
		join	<iface1> [<iface2>]	join iface2 to iface1 group
		break	<iface>	break iface to leave ipxparent group
	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

## Bridge Related Command

[Home](#)

Command				Description
Bridge				
	cnt			related to bridge routing statistic table
		Disp		display bridge route counter
		Clear		clear bridge route counter
	stat			related to bridge packet statistic table
		Disp		display bridge route packet counter
		Clear		clear bridge route packet counter

## Radius Related Command

[Home](#)

Command				Description
Radius				
	auth			show current radius authentication server configuration
	acct			show current radius accounting server configuration

## 802.1x 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

## Certificates Related Command

[Home](#)

Command				Description
certific ates				
	my_cert	create	Self-signed	
			request	
			Scep_enroll	
			Cmp_enroll	
		import		Import certificate.

		export	<name>	Export certificate.
		view	<name>	View certificate content.
		verify	<name> [timeout]	Verify certificate path.
		delete	<name>	Delete the specific certificate.
		list		List all my certificate.
		rename	<old name> <new name>	Rename the certificate.
		def_self_signed		Show the default self signed certificate name.
		replace_factory		Replace certificate to factory default.
	ca-trusted	Import	<name>	Import trust CA certificate.
		Export	<name>	Export trust CA certificate
		view	<name>	View trust CA certificate content
		Verify	<name> [timeout]	Verify trust CA certificate path.
		Delete	<name>	Delete the specific trust CA certificate.
		List		List all trust CA certificate.
		Rename	<old name> <new name>	Rename the trust CA certificate.
		Crl issuer	<name> [on/off]	Check the crl of trust CA.
	Cert_manager	Reinit		Reinitialize the certificate manager.
	Debug_tools	Cm_reset		Reset the certificate manager.

## Radserv Related Command

[Home](#)

Command				Description
radserv				
	Time_out		<value(ms)>	Set radius server authenticate time out.
	authenticator	Set	<entry_no active [ip secret]>	Set trust AP.
		remove	<entry_no>	Remove trust AP.
		list		List trust AP.