



**Firmware Release Note**

**ZyAIR G-2000PLUS v2**

**Release 3.60(AAF.1)C0**

**Date:** June 15, 2006  
**Author:** Watties Lin

# ZyXEL ZyAIR G-2000PLUS v2 Standard Version release 3.60(AAF.1)C0 Release Note

**Date:** June 15, 2006

## **Supported Platforms:**

ZyXEL ZyAIR G-2000PLUS v2

## **Versions:**

ZyNOS Version: V3.60(AAF.1) | 06/15/2006 10:10:00

BootBase : V1.05 | 04/20/2004 10:36:26

## **Notes:**

1. If Wireless Port Control (SMT Menu 23.4) is “Authentication Required”, G-2000PLUS v2 will enable 802.1x/WPA/WPA-PSK user authentication mechanism, a wireless user must associate G-2000PLUS v2 successfully before accessing network service. If Wireless Port Control is “No Authentication Required”, G-2000PLUS v2 will allow all wireless users to access network service. If Wireless Port Control is “No Access Allowed”, G-2000PLUS v2 will not allow wireless user to access network service.
2. If the Key Management Protocol is “WPA/WPA2”, then you have to configure RADIUS server and the Authentication Databases will be “RADIUS only”.
3. G-2000PLUS v2 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”, G-2000PLUS v2 will use default shared secret “1234”. But leave blank is exception.
4. The Local User Database does not support key generation for 802.1x dynamic web key and WPA pairwise/group key.
5. As a wireless client roams from one wireless AP to another, it must perform a full 802.1X authentication with each wireless AP. WPA2 allows the wireless client and the wireless AP to cache the results of a full 802.1X authentication so that if a client roams back to a wireless AP with which it has previously authenticated, the wireless client needs to perform only the 4-way handshake and determine new pairwise transient keys. In the Association Request frame, the wireless client includes a PMK identifier that was determined during the initial authentication and stored with both the wireless client and wireless AP's PMK cache entries. PMK cache entries are stored for a finite amount of time, as configured on the wireless client and the wireless AP. So wireless client may reconnect to AP with error user name or password.

## **Known Issues:**

## **CI Command List**

### **Features:**

#### **Modification in 3.60(AAF.1)C0 | 06/15/2006**

1. [FEATURE CHANGED]  
Convert to FCS version.

#### **Modification in 3.60(AAF.0)C0 | 05/09/2006**

1. [FEATURE CHANGED]  
Convert to FCS version.

#### **Modification in 3.60(AAF.0)b4 | 05/03/2006**

1. [BUG FIXED]  
Symptom: Wireless Power Saving issue.  
Condition: When wireless station (G-162, Intel 2200BG or Conexant-3890) power saving enable, and connect to G-2000plus v2 with no security mode, nothing to do (no ping no FTP no...), more than 20 minutes, the wireless station can't ping to DUT.  
SPRID: 60424865
2. [BUG FIXED]  
Symptom: Port change to check SNMP service works with Access setting (LAN & WAN / Disable / LAN / WAN) works failed.  
Condition: 1) Encapsulation is Ethernet, and disables Firewall.  
2) Remote MGMT/ SNMP service access = all.  
3) LAN & WAN host access G-2000plus v2 via SNMP port 161 successful.  
4) Change port 161 to 1610.  
5) LAN & WAN host access G-2000plus v2 via port 1610 failed.  
SPRID: 60425015
3. [BUG FIXED]  
Symptom: Spoof Mac addresses issue.  
Condition: In wizard, whether you use Ethernet/PPPoE/PPTP to make IP address, if you choose "spoof Mac address", the device will exception.  
SPRID: 60425978
4. [BUG FIXED]  
Symptom: Local database user account can pass the authentication when using RADIUS only.  
Condition: 1) In eWC->Advanced->Wireless: choose security as "802.1X+NO WEP" and authentication database as "RADIUS only".  
2) In eWC->Advanced->AUTH. Server->Trusted User: add one active user "1234".  
3) Wireless STA can use "1234" to pass the authentication.  
SPRID: 060310888
5. [BUG FIXED]  
Symptom: WPA2-PSK (WPA2) mixed mode with WPA-PSK (WPA) station issue. If G-2000plus v2 configure with WPA2-PSK (WPA2) mixed mode, and the station which configure with WPA2-PSK (WPA2) connect to device first, then the other station that configure with WPA-PSK (WPA) will not connection any more.  
Condition: 1) Load default first.

2) Configure device with WPA2-PSK (WPA2) mixed mode, and STA1 (Intel 2200BG) configure with WPA2-PSK (WPA2) and connect to device first, then STA2 (Conexant wireless card) configure with WPA-PSK (WPA) try to connect with device, but STA2 always can't connect.

SPRID: 60428284

6. [FEATURE ENHANCED]

Extend share secrets of authentication and accounting from length 31 to 128.

SPRID: 60426109

7. [FEATURE ENHANCED]

Add a rule of default server (0.0.0.0) in address mapping.

SPRID: 60427229

**Modification in 3.60(AAF.0)b3 | 04/20/2006**

1. [BUG FIXED]

Symptom: System crash when user telnet in and modify configuration.

Condition: Copy a long character string (ex: 12345678901234567890123456789012), telnet to G-2000plus v2, then paste the string in any item (Ex System name or domain name), system will crash.

SPRID: 60414066

2. [BUG FIXED]

Symptom: Conexant chipset wireless client (Mixed mode) can't associate to G-2000plus v2 (802.11b only mode).

Condition: In eWC->Advanced->Wireless: change 802.11 mode to 802.11b only, Setting Conexant STA 802.11 mode as b/g mixed mode, then STA can't associate to G-2000plus v2.

SPRID: 60418320

3. [BUG FIXED]

Symptom: Report function doesn't work.

Condition: In eWC->Advanced->LOGS->Reports: press "Start Collection" to monitor "Web Site Hits", "LAN IP Address", and "Protocol/Port". Press "Refresh" to update the information, but nothing appears.

SPRID: 60418347

**Modification in 3.60(AAF.0)b2 | 04/07/2006**

1. [BUG FIXED]

Symptom: Mass 64 bytes packets will cause switch interrupt fail and doesn't receive packets.

Condition: 1) Configure G-2000plus v2: NAT on, Firewall off, Quick Route 0x9bf2, Flow Control off.

2) Configure LAN to WAN performance test for SmartBits.

3) Under 64 bytes packets, Rx interrupt fail, and doesn't receive packets.

SPRID: 060307557

2. [BUG FIXED]

Symptom: WAN MAC Address Spoof failed.

Condition: In eWC->Advanced->WAN->MAC: when choose "Spoof this computer's MAC Address - IP Address" and press applies, an error messages"Can not get the WAN MAC Address" occurred.

SPRID: 060307559

3. [BUG FIXED]

Symptom: ZyAIR G-100 can't associate with G-2000plus v2 when 802.11 mode is set to 802.11b only.

Condition: 1) In eWC->Advanced->wireless: choose "802.11 mode" as "802.11b only".

2) Because preamble setting doesn't match, some STA like "ZyAIR G-100" can't associate successfully.

SPRID: 060309804

4. [BUG FIXED]

Symptom: Local database user account can pass the authentication when using RADIUS only.  
 Condition: 1) In eWC->Advanced->Wireless: choose security as “802.1X+NO WEP” and authentication database as “RADIUS only”.

2) In eWC->Advanced->AUTH. Server->Trusted User: add one active user “1234”.

3) Wireless STA can use “1234” to pass the authentication.

SPRID: 060310888

5. [BUG FIXED]

Symptom: system reboot many times after overnight stress test. (16 STAs run FTP+HTTP data transmission)

Condition: The below two test cases can reproduce this issue.

1) Let 16 wireless clients associate to DUT at the same time, run the FTP and HTTP data transmission between eSTA and all wireless clients. After overnight test, DUT reboot many times.

2).DUT reboot when run WLAN throughput test for 64 WEP\128 WEP and WPA-PSK\WPA2-PSK.

SPRID: 060311932

6. [BUG FIXED]

Symptom: STA using wrong password and CA can still pass the WPA2 authentication once STA passed the WPA2 authentication before.

Condition: STA using wrong password and CA can still pass the WPA2 authentication once STA passed the WPA2 authentication before.

SPRID: 060313945

7. [FEATURE CHANGED]

-USA(255), Taiwan(238), Philippine(216), India(214), Brazil(208) use 11 channels.

-Not Used(223, 251, 210), Morocco(239), Slovak(228), Slovenia(215), European CTR21(212), ZyXEL(000) use 13 channels.

-Others (include Japan 234) use 13 channels.

**Modification in 3.60(AAF.0)b1 | 02/22/2006**

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	Callhist		
	display		display call history
	remove	<index>	remove entry from call history
	countrycode	[countrycode]	set country code
	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
Logs			
	Clear		clear log error
	Display		display log error
	Syslog		
		active [0:no/1:yes]	
		display <FacilityNo>	set/display syslog type flag
		facility [Local ID(1-7)]	set syslog facility
		server [domainName/IP]	set syslog server IP address
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
Trcdisp	parse, brief, disp		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		
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.
		tosctrl		
			destination	Display TOS destination hash
			incomplete	Display TOS incomplete List.
		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.
		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
	breathLED	[0 1]	Turn off/on breath LED
	chid	[channel id]	set channel
	chgmod	<0: B+G, 1: B only, 3: G only>	
	essid	[ess id]	set ESS ID
	hideessid	<on, off>	
	intrabssblock	<0: Disable, 1: Enable>	
	preamble	<0: Dynamic, 1: Long>	
	removeSTA	<MAC ADDRESS>	Remove STA
	reset		Reset WLAN
	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		
	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
	ftp		
	traceroute	<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> groupmtm <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]
		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_manage r	Reinit		Reinitialize the certificate manager.
	Debug_tools	Cm_reset		Reset the certificate manager.

Radserv Related Command

[Home](#)

Command				Description
Radserver				
	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.
	enable		<1 0>	Enable   disable internal RADIUS server.