ZyXEL

Firmware Release Note

ZyAIR G-3000

Release 3.50(HO.2)C0

Date: **June 21, 2005**
Author: **Chin-Te Huang**

ZyXEL ZyAIR G-3000 Standard Version release 3.50(HO.2)C0 Release Note

Date: June 21, 2005

Supported Platforms:

ZyXEL ZyAIR G-3000

Versions:

ZyNOS F/W Version : V3.50(HO.2) | 06/21/2005 11:51:35
Bootbase Version: V1.03 | 11/01/2004 17:53:54

Notes:

1. If the roaming is active, the wireless STA will not be able to associate with G-3000 unless the Ethernet port is connected and the IP is gotten from DHCP server while the IP assignment is configured as “Dynamic”.
2. ZyAIR G-3000 is a country dependent product. Please setup correct country code before shipping.
3. AP firmware is v1.2.8.0.
4. In WPA-PSK, no Mix-Mode support.
5. Minimum Fragment Threshold of WLAN is 800.
6. When Authentication server is “Local user database only” or “Local first, then RADIUS”, accounting process will be disabled.
7. Accounting process will be disabled in WPA-PSK mode or embedded RADIUS used.

Known Issues:

1. WinXP supplicant doesn't work when it configures as 802.1x authentication with static WEP key.
2. WPA interoperability issue : When centrino station configure as WPA (or WPA-PSK) mode and data encryption filed set as WEP, it can not work with G-3000 under WPA (or WPA-PSK) mode and using WEP as group key. In this case, user must configure the data encryption field as TKIP then stations will automatic switch the group key cipher as WEP after it received the WPA information element from G-3000.
3. After deleted backup accounting or authentication server, system will re-rotate the backup radius server in sequence.
4. WDS link with security enabled may break in heavy traffic, but system will recover it automatically.
5. If user uses embedded Web interface to upload new firmware and no "Firmware

Upload Successful" page shows. Please upload FW again after re-boot the device.

6. Use G-3000 as RADIUS server which performs PEAP authentication and STA uses WZC to authenticate to G3000 through G-560 which act as AP, STA can't authenticate successful.

CI Command List:

Features:

Modification in 3.50(HO.2)C0 | 06/21/2005

1. [FEATURE CHANGED]
   Change ZyNOS version from 3.50(HO.2)b1 to 3.50(HO.2)C0

Modification in 3.50(HO.2)b1 | 06/06/2005

1. [BUG FIXED]
   Symptom: Aegis client can't work with G3000.
   Condition: Configure the wireless security mode as WPA or 802.1X dynamic WEP and use internal PEAP server to authenticate STA with Aegis client, STA can't authenticate with G3000 successful.

2. [BUG FIXED]
   Symptom: G405 can't work with G3000.
   Condition: Configure the wireless security mode as WPA or 802.1X dynamic WEP and use internal PEAP server to authenticate STA (G405). G405 can't authenticate with G3000 successful.

3. [BUG FIXED]
   System: When G-3000 is configured as 802.1x with dynamic WEP key, STAs associated to the same G-3000 cannot communicate to each other.

Modification in 3.50(HO.1)C0 | 02/02/2005

2. [FEATURE CHANGED]
   Change ZyNOS version from 3.50(HO.1)b3 to 3.50(HO.1)C0

Modification in 3.50(HO.1)b3 | 01/12/2005

3. [FEATURE CHANGED]
   Accounting process will be disabled in WPA-PSK mode, embedded RADIUS used, and Local user database used.

4. [BUG FIXED]
   Symptom: Domain name will be erased when changed IP address assignment from dynamic to static.

Modification in 3.50(HO.1)b2 | 12/14/2004

1. [FEATURE ENHANCED]
   Support Layer-2 Isolation. See Appendix 8

2. [BUG FIXED]
   Symptom: System exception and reboot occur when system name is up to 30 characters long and enable 802.1x.

3. [BUG FIXED]
   Symptom: External accounting server can work when enable internal RADIUS server.

4. [BUG FIXED]
   Symptom: WPA-PSK STA cannot associate with DUT successfully when DUT changed configuration from WPA with external RADIUS and accounting server enable.

Modification in 3.50(HO.1)b1 | 11/01/2004

1. [FEATURE ENHANCED]
   Support backup radius server. See Appendix 4

2. [FEATURE ENHANCED]
   Support Configurable Output Power for Built-in WLAN card. See Appendix 6

3. [FEATURE ENHANCED]
   Support Blocking Intra-BSS traffic. See Appendix 5

4. [FEATURE ENHANCED]
   Support Embedded PEAP server. See Appendix 3

5. [FEATURE ENHANCED]
   Add WDS link information into association list table in eWC.

6. [FEATURE ENHANCED]
   eWC supports HTTPS link.

7. [FEATURE ENHANCED]
   Add Remote Manager in SMT/eWC.

8. [FEATURE ENHANCED]
   Support Vantage WLC 200

9. [FEATURE CHANGED]
   Disable WPA Mix-mode in WPA-PSK mode.

10. [FEATURE CHANGED]
    In CI command, use “WLAN 0/1” to select which WLAN card will be configured.
    See CI command

11. [FEATURE CHANGED]
    Extend VLAN ID from 256 to 4094

12. [FEATURE CHANGED]
    Range of Fragment Threshold is from 800 to 2432.

13. [FEATURE CHANGED]
    Modify default ROM file value.
    - Change “ESSID” to “Name(SSID)”
    - Default SSID “Wireless” is changed to “ZyXEL”
    - Logs
      - ✓ Enable Send log: System Maintenance, System Error, PKI, SSL/TLS, 802.1x, Wireless and Internal RADIUA server.

14. [BUG FIXED]
    Symptom: SMT3.5:Available channel ID isn’t correct after changing sys country code on menu 24.8.
    Condition: MT3.5:Available channel ID isn’t correct after changing sys country code on menu 24.8.

15. [BUG FIXED]
    Symptom: eWC\Wizard setup:Pls add configurations of removable wireless LAN setup in the wizard setup.
    Condition: eWC\Wizard setup:Pls add configurations of removable wireless LAN setup in the wizard setup.

16. [BUG FIXED]
    Symptom: Wireless service was inactive sometimes
    Condition: Sometimes the wireless service will not work. When happened, the G-3000 will not issue beacon and the station card can not associate to G-3000 anymore.

17. [BUG FIXED]
    Symptom: WDS:After overnigh testing, FTP clients disconnect when running 6 AP+Bridge mode.
    Condition:
    (1). Setup the WDS link and enable RSTP(No WDS security) for 6 APs using AP+Bridge mode.
    (2). Setup the station1 that associate to AP1 and enable FTP server.
    (3). Setup the station2 that associate to AP2 and download/upload files to station1 by FTP_client.
    (4). Setup the station3 that connect to AP3 by Ethernet and download/upload files to station1 by FTP_client
    (5). after overnight test, you can find that all FTP clients disconnect.

18. [BUG FIXED]

Symptom: SMT menu1:Sometime DNS server configuration cannot save to rom when set to 'User-Defined'.
Condition: SMT menu1:Sometime DNS server configuration cannot save to rom when set to 'User-Defined'.

19. [BUG FIXED]
Symption: System crash when internal radios are dedicated to WDS bridge function with PSK security, removable radios implement AP only with WPA security and roaming enable.
Condition: System crash when internal radios are dedicated to WDS bridge function with PSK security, removable radios implement AP only with WPA security and roaming enable.

Modification in 3.50(HO.0)C0 | 08/13/2004

1 [FEATURE CHANGE]
Change ZyNOS version from 3.50(HO.0)b6 to 3.50(HO.0)C0

Modification in 3.50(HO.0)b6 | 08/09/2004

1. [BUG FIXED]
Symptom : The channel id field of WIRELESS LAN page in eWC is inconsistent after changing the channel id field in WIZARD SETUP page.

Modification in 3.50(HO.0)b5 | 07/26/2004

1. [BUG FIXED]
Symptom : Low performance issue.
Condition :
(1) STA connected to removable WLAN adapter and PC connected to LAN port of G-3000.
(2) Run Chariot to test the throughput between STA and PC, the result is lower than 18 Mbps.

2. [FEATURE CHANGED]
Change the number of WDS links from 6 to 5.

3. [FEATURE ENHANCED]
The WEP fields in SMT3.5 will show N/A if WPA/WPA-PSK/802.1x with dynamic WEP key enabled in SMT23.4.

Modification in 3.50(HO.0)b4 | 07/02/2004

1. [BUG FIXED]
Symptom : eWC\Maintenance\Association List :duplicate MAC address appear when enable both of built-in and removable WLAN.
Condition :
(1) STA1 connects to build-in WLAN adapter and then STA2 connects to removable WLAN adapter.
(2) The association list in eWC will show STA2's MAC address in the two WLAN

adapters.

2. [BUG FIXED]
   Symptom : Type error.
   Condition : eWC\system\Time Setting : Invalid string for 'Daylight Saving Setup'.

8. [BUG FIXED]
   Symptom : STA that configures as 802.1x mode with dynamic WEP key cannot associate with G-3000 which is set to WPA or WPA-PSK mode with mixed mode enabled.

9. [BUG FIXED]
   Symptom : eWC:\Wireless\802.1x/WPA: the configuration of Authentication Databases cannot be saved.
   Condition :
   (1) Configure the G-3000 as 802.1x mode with dynamic WEP key disabled.
   (2) Change the Authentication Databases field and then save it.
   (3) The setting is considered as an unchanged status and cannot perform saving process.

10. [FEATURE ENHANCED]
    Online help in eWC is updated.

11. [FEATURE ENHANCED]
    Log the same format for STA associated and disassociated.

12. [FEATURE ENHANCED]
    Warning message 'PSK field of WDS link cannot be empty' should appear on 802.1X/WPA web page when changing key management protocol to WPA(WPA-PSK) or 802.1x+dynamic WEP.

13. [BUG FIXED]
    Symptom : Build-in WLAN interface stopped working after running FTP 15 hours with WPA mode enabled in G-3000.
    Condition :
    (1) Configure G-3000 as AP mode and enable WPA.
    (2) STA1 associated with build-in WLAN and STA2 associated with removable WLAN by WPA.
    (3) Running FTP service between STA1 and STA2.
    (4) After 15 hours, STA1 disconnected with build-in WLAN and the error message, "Error: Management FreeQ not enough entries, fragments: 0x01", displayed in the SMT.

Modification in 3.50(HO.0)b3 | 06/07/2004

1. [BUG FIXED]
   Symptom : ESSID field can only key in 30 characters on Wizard Setup function. It

should be 32 characters.

2. [BUG FIXED]
   Symptom : G-3000 can accept the 0.0.0.0 IP address on Wizard Setup function.

3. [BUG FIXED]
   Symptom : G-3000 can accept the illegal IP address (EX:225.1.1.1) on Wizard Setup function.

4. [BUG FIXED]
   Symptom : G-3000 can accept the 0.0.0.0 subnet mask on Wizard Setup function.

5. [BUG FIXED]
   Symptom : If the log items are more than 80, the display list doesn't work.

6. [BUG FIXED]
   Symptom : eWC\ADVANCED\WIRELESS\RADIUS: Shared secret key can accept 32 characters in Radius function but in help page it shows that the key accept up to 31 characters.

7. [BUG FIXED]
   Symptom : eWC\WIRELESS\RADIUS: IP Address field can accept the 0.0.0.0 and 255.255.255.255.

8. [BUG FIXED]
   Symptom : eWC\ADVANCED\SYSTEM\Time Setting: "Dalight Saving Setup" can accept invalid Date. For example, 0 month 0 day / 2 month 31 day

9. [BUG FIXED]
   Symptom : STA can not connect to G-3000 after changing WPA-PSK mode to static WEP mode.

10. [BUG FIXED]
    Symptom : STA can not access bridge link when enabling native VLAN ID.
    Condition :
    (1). Configure the WDS link with two APs (AP+Bridge mode) and don't enable WDS security/native VLAN ID. (AP1---AP2)
    (2). Establish the connection of STA1 to AP1.
    (3). Make sure STA1 can access AP1 and AP2.
    (4). Enable the same native VLAN ID on AP1 and AP2.
    (5). You can find STA1 can not access AP2.

11. [BUG FIXED]
    Symptom : 802.1x with dynamic WEP key can not work when shared secret of accounting server is invalid.

12. [BUG FIXED]
    Symptom : SMT22:SNMP Trap function can not work.

13. [BUG FIXED]
    Symptom : eWC: It does not remove left menu from screen when users logout.

14. [BUG FIXED]
    Symptom : eWC / Maintenance / Show Statistics: Bridge link status should be hidden when operating mode is AP.

15. [BUG FIXED]
    Symptom : eWC:Javascript error when entering IP address for DNS.

16. [BUG FIXED]
    Symptom : eWC:The statistics popup window contents are obscured at the bottom. System Up Time is only visible at the top half.

17. [BUG FIXED]
    Symptom : Show the ESSID when operating mode is bridge/repeater mode. It should be hidden.

18. [BUG FIXED]
    Symptom : eWC: Left menu area has horizontal scrollbar.

19. [BUG FIXED]
    Symptom : G-3000 can not get IP address from WDS link when dynamic IP is configured.

20. [FEATURE CHANGED]
    Upgrade uAP version from 1.0.2.0 to 1.0.4.3.

21. [FEATURE ENHANCED]
    Online help in eWC is ready.

22. [FEATURE CHANGED]
    Default value of time protocol is consistent between SMT and eWC.

23. [FEATURE ENHANCED]
    Show the associated WLAN adapter and its ESSID in Maintenance /Association List page.

24. [FEATURE ENHANCED]
    Add system name in the eWC generated tile.

25. [FEATURE ENHANCED]
    Add source address and destination address in the logs page of eWC when time

synchronization is successful.

26. [FEATURE CHANGED]
    eWC\Show statistics: Instead of showing bridge link #1 through #16, the table is broken into two tables. One table is for Build-in card and another is for removable card.

27. [FEATURE ENHANCED]
    Add the logs of Bridge Association (Up/Down), Client Association/Disassociation.

Modification in 3.50(HO.0)b2 | 04/29/2004

1. [BUG FIXED]
   Symptom : Sometime the station can not associate with Built-in WLAN adapter by WPA after passing the WPA authentication with Removable WLAN adapter.
   Condition :
   (1). Establish the connection with Removable WLAN adapter by WPA.
   (2). Disconnect and then change the connection to Build-in WLAN adapter by WPA.
   (3). The client can not associate with Build-in WLAN adapter by WPA.

2. [BUG FIXED]
   Symptom : If the VLAN ID of WLAN adapter that STA associated with is different from RADIUS server, WPA(WPA-PSK) can not work after re-authentication timer expired.
   Condition :
   (1). Enable VLAN mechanism (SMT16) and set different VLAN ID for built-in and removable WLAN adapters (SMT 3.5). (Only one WLAN adapter's VLAN ID can be the same with device's native VLAN ID)
   (2). STA associated with the WLAN adapter that its VLAN ID is different from the device's VLAN ID.
   (3). The connection that STA established will be broken after re-authentication timer expired.

3. [BUG FIXED]
   Symptom : eWC\ADVANCED\WIRELESS: Operating mode will not be changed to correct mode.
   Condition :
   (1). Set the operation mode of built-in WLAN adapter to "access point" and then saved the configuration.
   (2). Then set the operation mode of removable WLAN adapter to "AP + bridge" and saved the configuration.
   (3). Select the built-in WLAN adapter, the operation mode change to "AP + bridge".

Modification in 3.50(HO.0)b1 | 04/09/2004

1. First release for C3 firmware

Appendix 1: CI Command List

Command Class List Table		
System Related Command	Exit Command	Ethernet Related Command
Wireless LAN Related Command	IP Related Command	Bridge Related Command
802.1x Related Command	RADIUS Related Command	Certificates Related Command
Vantage Related Command		

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		
	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
	edit			
		load	<ether no.>	load ether data from spt
		save		save ether data to spt

Wireless LAN Related Command Home

Command				Description
wlan				
	[0/1]			Select WLAN Card (0:Built-in, 1:Removable)
		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
	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		

		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
	status			display ip statistic counters
	udp			
		status		display udp status
	rip			
	tcp			
		status	[tcb] [<interval>]	display TCP statistic counters
	telnet		<host> [port]	execute telnet clinet command
	tftp			
	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

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

802.1x Related Command Home

Command				Description
8021x				
	debug	reauth	<0:off 1:on>	set IEEE802.1x reauthentication method
		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

RADIUS Related Command Home

Command				Description
radius				
	showRunInfo			Show server running information

	auth	show		Show current RADIUS authentication server configuration.
		addAuthServer		Add an authentication server.
		delAuthServer		Delete an authentication server.
	acct	show		Show current RADIUS accounting server configuration.
		addAcctServer		Add an accounting server.
		delAcctServer		Delete an accounting server.
radserv				
	time_out	[time out value (ms)]		Time out value for one session (in millisecond)
	authenticator	Set	[entry_no] [active]	Activate/deactivate the authenticator of entry_no
			[entry_no] [active] [IP] [secret]	Set the information of the authenticator
		Remove	[entry_no]	Remove authenticator of entry_no
		List		Show all the setting of authenticators

Certificates Related Command Home

Command				Description
certificates				
	my_cert	create		Create Self-Signed Certificate
		import		Import Self-Signed Certificate
		export	<name>	Export Self-Signed Certificate
		view		Display Self-Signed Certificate
		delete	<name>	Delete Self-Signed Certificate
		list		List Self-Signed Certificate
	ca_trusted	create		Create Trusted Certificate

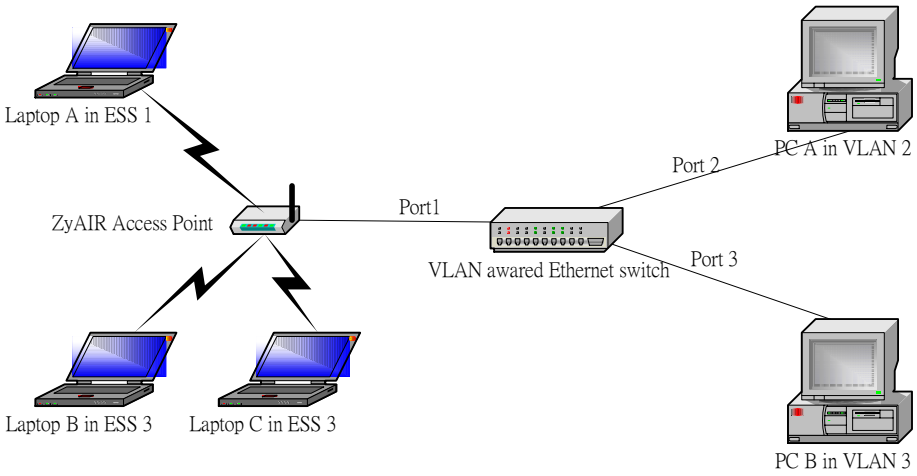
Vantage Related Command Home

Command				Description
cnm	active	[0/1]		Display or set the CNM features to enable or disable . 0: disable 1: enable CNM features and communicate through WAN interface.
	sgid			Display sgid which is the unique ID of the device in Vantage.
	managerIP	[addr]		Display or set the IP of Vantage server/COMServer which manage this device. [addr] specifies the IP of the Vantage serve/COMServer.
	debug	[0/1]		Display or set the way of outputting CNM debug messages. 0: disable debug messages. 1: output the debug messages to console and can accept SGMP inquire message only after the device is registered to Vantage server.
	reset			Reset the state machine of SGMP and return to the state of SGMP_STATE_UNKNOWN. Device will re-register to Vantage server if CNM is active.
	encrykey	[string]		Display or set encryption key. [string] specifies the encryption key. to be set. Key length can not less than 8 alphanumeric characters long, if ecrymode is DES. Key length can not less than 24 alphanumeric characters long, if ecrymode is 3DES.
	encrymode	[0/1/2]		Display or set the encryption mode for SGMP

				messages. [0:NONE /1:DES/2:3DES] specifies the encryption mode to be set.
	keepalive			Display the time(second) to report agent keepalive 0: disable. Set the time(second) to report agent keepalive; the valid range : 10 ~ 2147483647
	version			Display the Vantage agent version.

Appendix 2: Multi-ESS with VLAN

Since G-3000 supports 2 WLAN adapters to enhance wireless access, it can work with VLAN to extend the group of users from wireless LAN to wired Ethernet. Compared with the function of multiple ESSID that supported by ZyDAS, some differences exist. G-3000 just assigns VLAN ID to each WLAN adapters to separate the user group. The following graph is an illustration to test the function. Please refer to the document "Multi-ESS with VLAN test plan" for detail information.



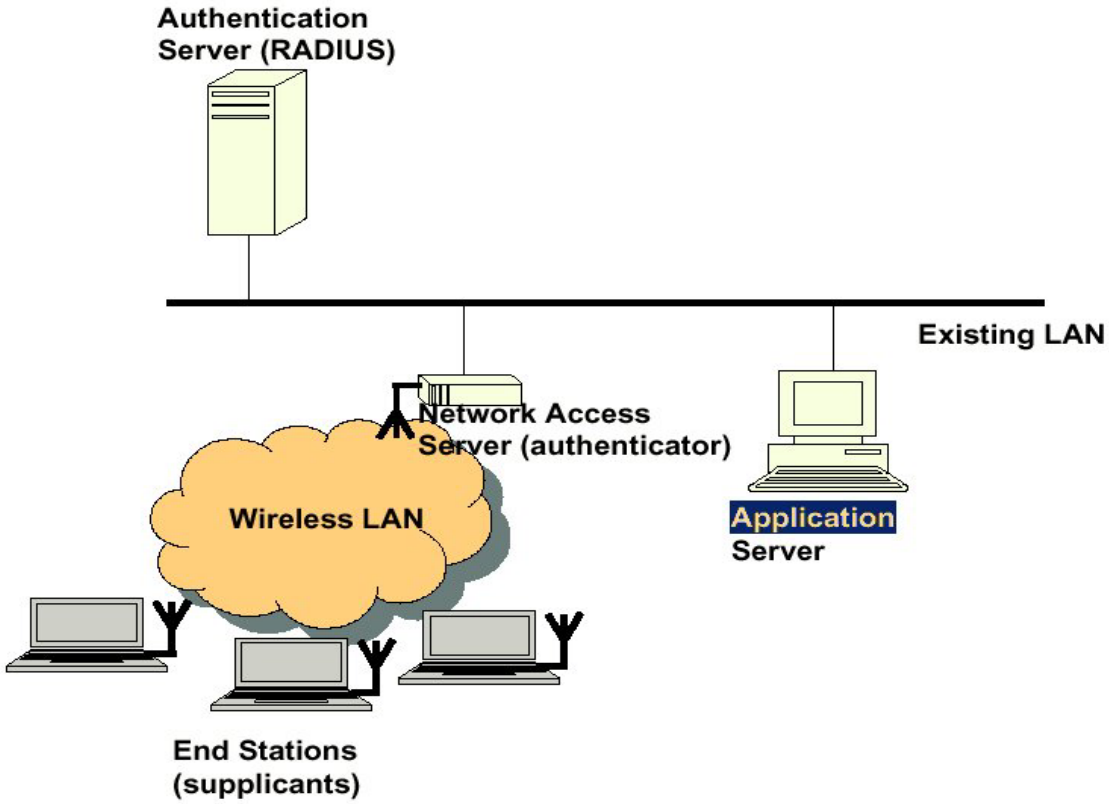
Appendix 3: Embedded RADIUS Server (PEAP)

1. Introduction

Security has always been one of the crucial issue of network connection. To assure information safety, the identities of the peers must be authenticated first. RADIUS stands for Remote Access Dial-In User Service, which has a database of all the peers and is responsible for authentication. The RADIUS server plays the role of the authentication server of an authentication protocol like IEEE 802.1X. Extensible Authentication Protocol (EAP) was first invented to deal with PPP link authentication. With its flexibility, EAP can carry almost every user authentication protocols, for example, PEAP (Protected EAP) and MD5-Challenge. Because of this advantage, IEEE 802.1X uses EAP on the link between supplicant and authenticator, and the RADIUS extension has set EAP as a standard attribute as well. To provide EAP with advanced security, engineers from Microsoft proposed PEAP that utilizes TLS (Transport Layer Security) to protect all the authenticating information. By embedding the RADIUS server in our APs (Access Points), customers can take advantage of better wireless security with lower cost than buying an extra standalone RADIUS server.

2. IEEE 802.1X

[IEEE Std 802.1X-2001] defines a mechanism for Port based network access control that makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases where the authentication and authorization process fails.



3. RADIUS

Remote Access Dial-In User Service or RADIUS is an access-control protocol that verifies and authenticates users based on the commonly used challenge/response method. While RADIUS has a prominent place among Internet service providers, it also belongs in any environment where central authentication, regulated authorization, and detailed user accounting is needed or desired.

Fig. IEEE 802.1X w/ Standalone RADIUS server

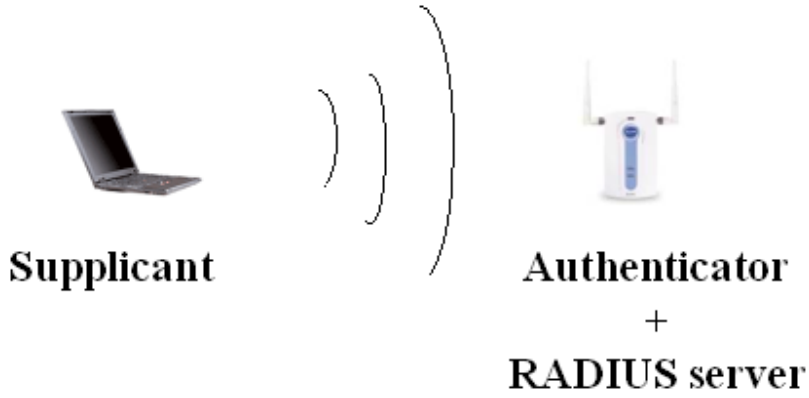


Fig. IEEE 802.1X w/ Embedded RADIUS server

4. EAP

Extensible Authentication Protocol (EAP) is a general protocol for authentication which supports multiple authentication mechanisms. EAP does not select any specific authentication mechanism at first. This allows the authenticator to request more information before determining the specific authentication mechanism. This also permits the use of a “back-end” server which actually implements the various mechanisms while the authenticator merely passes through the authentication exchange.

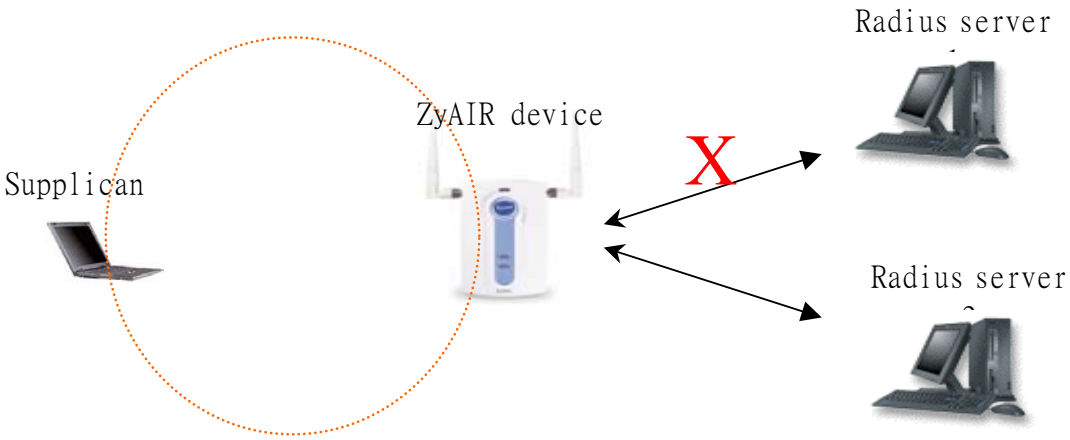
5. PEAP

EAP was developed or used on wired networks, where physical security was presumed. Where an attacker can easily gain access to the medium (such as on a wireless network or where EAP is run over IP), the presumption of physical security is no longer valid. Since the EAP method negotiation is unprotected, an attacker can inject packets in order to cause the negotiation of a method with lesser security. Denial of service attacks

are also possible. PEAP is an EAP type that addresses this security issue by first creating a secure channel that is both encrypted and integrity-protected with Transport Level Security (TLS). Then, a new EAP negotiation with another EAP type occurs, authenticating the network access attempt of the client. Because the TLS channel protects EAP negotiation and authentication for the network access attempt, password-based authentication protocols that are normally susceptible to an offline dictionary attack can be used for authentication in wireless environments.

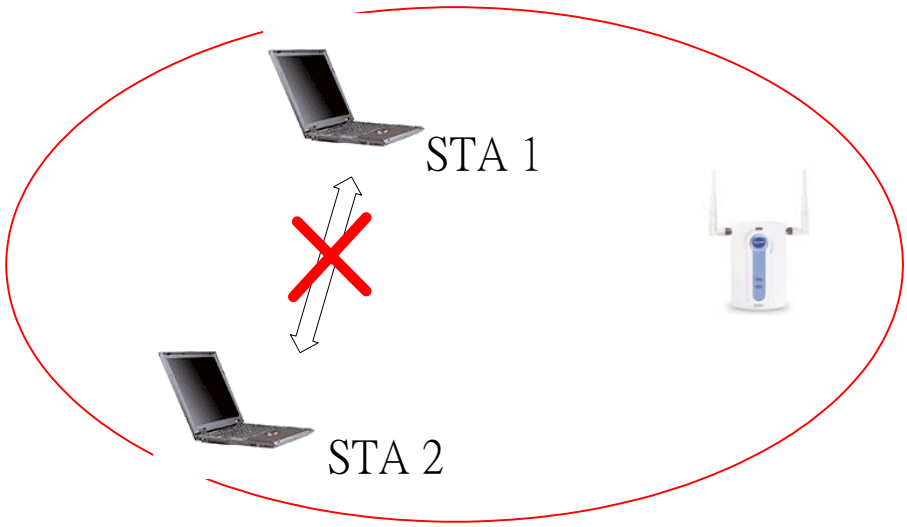
Appendix 4: Backup RADIUS Server

ZyAIR devices support at most 5/2 (eWC/CI command) backup radius servers and accounting servers setting. ZyAIR devices use the first radius server setting as the default configuration. Figure shows the backup radius server concept. There are two radius servers can be reached by ZyAIR device. If supplicant issue an authentication request to ZyAIR device and trying to authenticate with radius server, ZyAIR device will keep trying forward this request to radius server 1. If ZyAIR device keep trying for 3 times and radius server still doesn't response the request then ZyAIR device will auto switch the authentication request packet to radius server 2. The trying time interval is depending on the supplicant re-try interval.



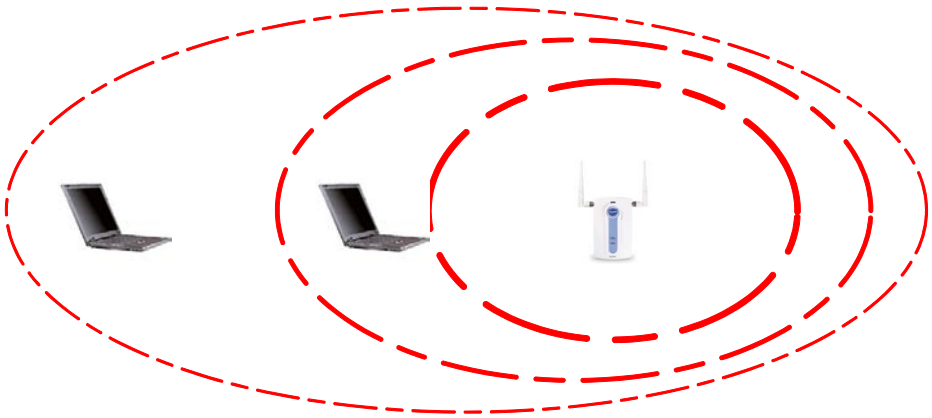
Appendix 5: Blocking Intra-BSS traffic

For performance and security issues, G-3000 supports Blocking Intra-BSS Traffic feature. In public access WLAN, the users are not necessary to receive others' traffic. Therefore, Blocking Intra-BSS Traffic feature make AP not to forward STAs' traffic in a BSS area. This feature raises the security and performance obviously.



Appendix 6: Configurable Output Power

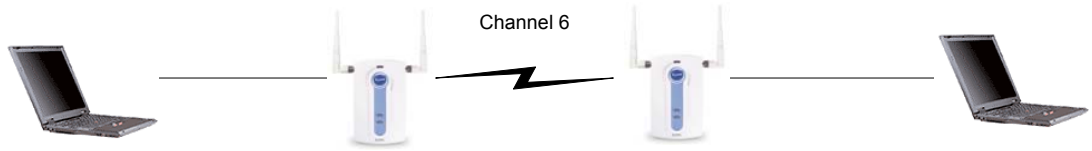
G-3000 provides configurable power to adjust AP's output power dynamically. This feature makes operator could limit AP's signal range and reduce the signal interference. On the other hand, it also strengthens the network security because the wireless signal will not leak out the undesired place.
G-3000 uses 5 output power levels (0~4) to configure the RF's output power. 0 for max. and 4 for min..



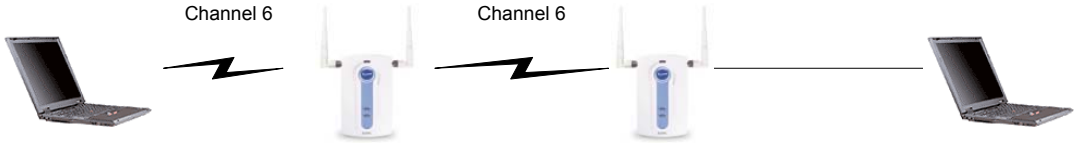
Appendix 7: WDS

G-3000 can maintain up to 5 different wireless connections to other APs. For that to be possible the channel will need to be the same for the wireless links to the other APs. The following diagrams provides the test scenarios :

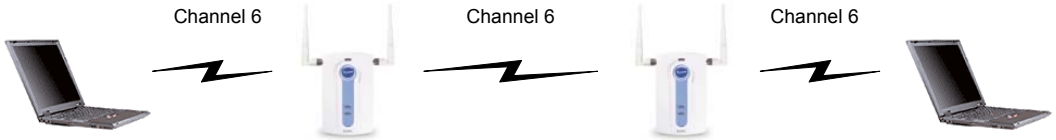
(1)



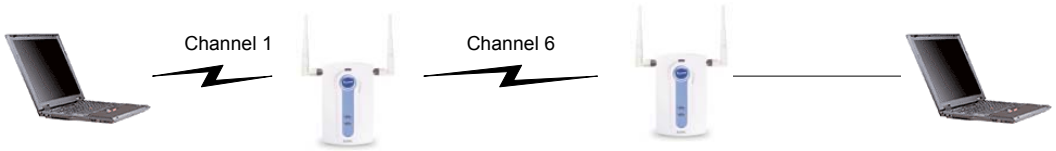
(2)



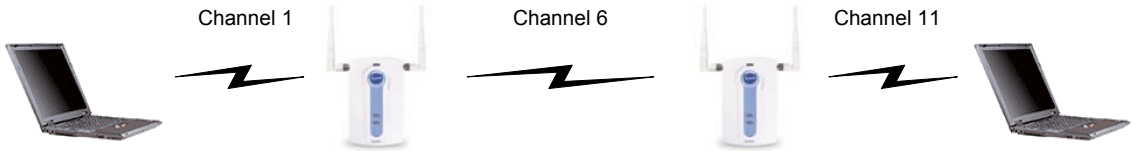
(3)



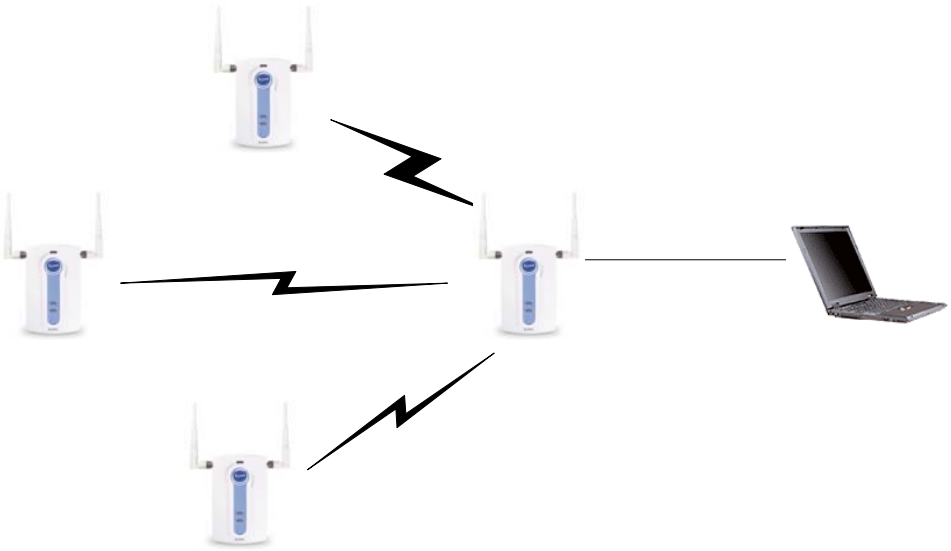
(4)



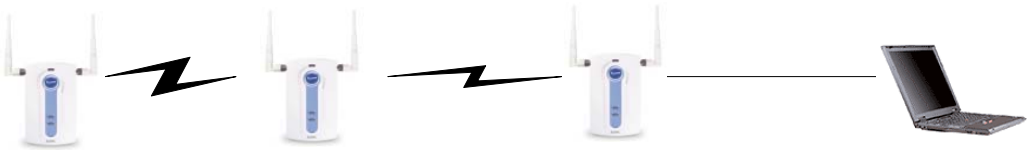
(5)



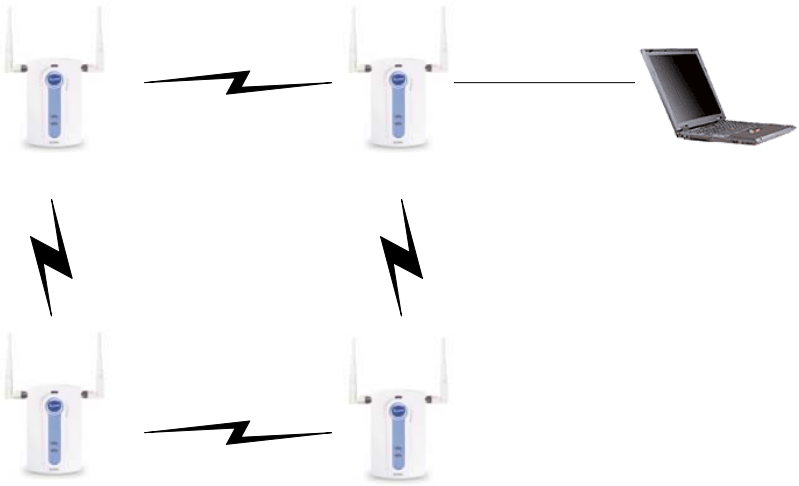
(6)



(7)



(8)



Appendix 8: Layer-2 Isolation

In Layer-2 isolation mode, all frames received from wireless clients that want to be forwarded to the connected AP or another interfaces will be dropped. AP will perform the packet filtering function to drop the client's traffics.

G-3000 can configure up to 32 different MAC addresses to which the G-3000 allows to forward wireless packets.