

ZyXEL

Firmware Release Note

ZyAIR G-3000H

Release 3.50(AAC.2)C0

ZYXEL
CONFIDENTIAL

Date: June 15, 2006
Author: Morris, Lee

ZyXEL ZyAIR G-3000H Standard Version

Release 3.50(AAC.2)C0

Release Note

Date: June 15, 2006

Supported Platforms:

ZyXEL ZyAIR G-3000H

Versions:

ZyNOS Version : V3.50(AAC.2) | 06/15/2006 10:14:11

Bootbase Version : V1.03 | 05/25/2005 16:49:07

Notes:

1. ZyAIR G-3000H is a country dependent product. Please setup correct country code before shipping.
2. When AP is working under MESSID mode and security mode is WEP, 8021X-STATIC64, or 8021X-STATIC128 (which use static WEP key for encryption / decryption), only key1 is usable, no matter which key index is assigned in the security profile. This implies that all clients can only, and must set WEP key index 1. Other key index will be meaningless.
3. Please use eWC (WEB) or CI command to edit SSID profile properties. SMT doesn't support SSID profile edit.
4. If STA1 and STA2 connected to same BSS, but got different VLAN number from RADIUS server, the traffic between STA1 and STA2 won't be blocked when intra-BSS traffic is enabled.
5. When AP is running under MESSID mode, the first entry of selected SSID profiles will be visible. The term "visible" here means AP will send probe response of that SSID when it receives probe request which is broadcast or doesn't include any specific SSID. This will affect client's wireless scan result. For example, if user enabled SSID profile index 3, 5, 7 under MESSID mode and SSID profile index 3 is at the first entry of eight available selections, then SSID profile 3 will be visible. If the first entry of eight available selections is not enabled, then no SSID will be visible.

- WPA2 support of Windows XP service pack 2 may need to install **Update for Windows XP (KB893357)** manually. Additionally, please update latest wireless adapter driver from vender site in order to get WPA2 / WMM support.
- Please add an additional MAC entry “FF:FF:FF:FF:FF:FF” in the L2isolation when operating mode is MESSID to make L2isolation work properly.
- Current MESSID mode can set different security mode for different SSID, but not all types of combinations can work if supplicant is windows wireless zero configuration (shorten as WZC below). If AP is configurated to a security combination which is not listed below, WZC may not connect to some SSID successfully. Please reference detailed information from the following table. Other supplicants (Funk Odyssey / ZyXEL client tool) may connect to security combination which is not listed on the table.

	NONE	WEP	8021X-ONLY	8021X-DYNAMIC64	8021X-DYNAMIC128	8021X-STATIC64	8021X-STATIC128	WPA	WPA-PSK	WPA-MIX	WPA2	WPA2-PSK	WPA2-MIX	WPA2-PSK-MIX	NO ACCESS
NONE	●	●	●	●	●	●	●								●
WEP	●	●	●	●	●	●	●								●
8021X-ONLY	●	●	●	●	●	●	●								●
8021X-DYNAMIC64	●	●	●	●	●	●	●								●
8021X-DYNAMIC128	●	●	●	●	●	●	●								●
8021X-STATIC64	●	●	●	●	●	●	●								●
8021X-STATIC128	●	●	●	●	●	●	●								●
WPA								●			●	●			
WPA-PSK									●		●	●			
WPA-MIX										●	●	●			
WPA2								●	●	●	●				
WPA2-PSK								●	●	●		●			
WPA2-MIX													●		
WPA2-PSK-MIX														●	
NO ACCESS	●	●	●	●	●	●	●								

■ *Compatibility table of Security policies of windows XP supplicant*

Known Issues:

- WinXP supplicant doesn't work when it configures as 802.1x authentication with static WEP key.
- 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-3000H 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-3000H.

3. WDS links will be broken temporarily with heavy traffics.
4. WMM/QoS is always enabled in this release.
5. When AP is configured with WPA2-MIX, or WPA2-PSK-MIX mode, the ZyXEL G-220F can't connect with WPA or WPA-PSK.
6. If AP is configurated as
 - a. AP is working under MESSID mode
 - b. Two wireless client associate to two different SSID,
 - c. Two different SSID have same VLAN ID,the traffic between two wireless client will not be forwarded by AP.
7. In Web GUI, configure the 255.255.248.0 as the network submask, then, the device will pop up a error message "Subnet Mask error", if want to set the submast, configure it in the console or telnet.

CI Command List:

Features:

Modification in 3.50(AAC.2)C0 | 06/15/2006

1. [FEATURE CHANGE]
Modify to FCS version.

Modification in 3.50(AAC.2)b1 | 05/29/2006

1. [FEATURE ENHANCED]
Enlarge four public SSID numbers on MSSID mode
2. [FEATURE CHANGED]
Symptom: Change WLAN channel usage of some countries.
Condition:
 ch1 ~ ch11: USA, Philippines, Taiwan, India, Brazil.
 ch1 ~ ch13: Others
3. [BUG FIXED]
G3000H cant work with G405 in WPA-PSK mode.
(SPRID: 051216017)
4. [BUG FIXED]
Auto configuration by DHCP can't run with windows server 2003.
(SPRID: 060112602)
5. [BUG FIXED]
When G3000H works in MESSID mode, wireless client can't get IP address from Win2003 DHCP server.
(SPRID: 060308648)
6. [BUG FIXED]
The bridge light won't turn on

(SPRID: 060314036)

7. [BUG FIXED]

The Enable intra-BSS Traffic check box isn't cleared when you enable layer-2 isolation.

(SPRID: 051214835)

(SPRID: 060510603)

8. [BUG FIXED]

WPA-PSK\WPA2-PSK cannot work (EAPOL MIC Error v1) after DUT changed security mode from WPA to WPA-PSK or WPA2-PSK mode

(SPRID: 060213541)

Modification in 3.50(AAC.1)C0 | 10/19/2005

2. [FEATURE CHANGE]

Modify to FCS version.

Modification in 3.50(AAC.1)b5 | 10/04/2005

1. [BUG FIXED]

In SMT or telnet mode, item 23.5 , create max string length profile name, then change the index from 1 ~ 16, observe the Profile name status, it will show superfluous characters.

2. [BUG FIXED]

In AP mode, set DUT to WPA-PSK or WPA2-PSK mode, let one STA associate to DUT, In SMT, change the DUT mode to MESSID, DUT will reboot.

3. [BUG FIXED]

AP+bridge mode performance is unstable. (Bridge/Repeater mode is fine)

4. [BUG FIXED]

In MIB browser, use AUTO CONFIGURATION Remote Triggering command to update configuration more than 3 times, DUT would reboot with error message.

5. [BUG FIXED]

SNMP:MIB-pwTrap(1.3.6.1.4.1.890.1.9.2)[Wireless trap / StationAssociated] [Deassociated] [FailAssociate] [FailAuthenticate] trap function doesn't work properly.

6. [BUG FIXED]

eWC: Fix incorrect output at Wireless - Channel Usage if SSID is empty.

Modification in 3.50(AAC.1)b4 | 09/14/2005

1. [BUG FIXED]

SNMP autocfg function doesn't work properly.

2. [BUG FIXED]

There are some issues in WPA2-MIX and WPA2-PSK-MIX mode.

3. [FEATURE CHANGED]

Change MIB name from PROWIRELESS-MIB to ZYXEL-PROWIRELESS-MIB.

4. [FEATURE CHANGED]

Modify limitation of minimum RTS threshold from 0 to 800.

5. [FEATURE CHANGED]

Modify eWC wizard setup. Now it will write appropriate setting to SSID profile 1 and security profile 1 automatically.

6. [FEATURE ENHANCED]

Change MESSID operation. Now only the first selected SSID will response broadcast probing request. The others will act as they are hidden SSIDs.

7. [FEATURE ENHANCED]

Support WLM EMS 1.0.

Modification in 3.50(AAC.1)b3 | 08/30/2005

1. [BUG FIXED]

After config SSID profile from Web, then select SSID profile from SMT 3.5 with operating mode=AccessPoint, device will reboot.

2. [BUG FIXED]

In eWC, when operating mode = AP+Bridge, and AP security is enable (wep 802.1x, wpa or wpa2), then "Enable WDS Security" function enable or not, the WDS always can connect.

3. [BUG FIXED]

Change the output power config items of eWC and SMT 3.5 to be the same.

Modification in 3.50(AAC.1)b2 | 08/11/2005

1. [FEATURE CHANGED]

Change AP code.

UMAC from 2.12.15.0.fix to 2.12.23.0, LMAC from 2.13.8.0 to 2.13.12.0.

2. [FEATURE CHANGED]

Remove VLAN support for RADIUS client.

3. [FEATURE ENHANCED]

Support VLAN assigned by RADIUS server.

4. [FEATURE ENHANCED]

Support local user database authentication for some specific security mode.

5. [FEATURE ENHANCED]

Support encrypted auto configuration script file.

6. [BUG FIXED]

Symptom: In eWC, the WPA-PSK mode can't accept 63 chars

7. [BUG FIXED]

Symptom: Copy one string with 30 characters, in telnet mode, paste this string in 23.1 ==> old password, system will reboot.

8. [BUG FIXED]
Symptom: From the SMT command 24.6 ,when restore configuration , device crash and show error message.
9. [BUG FIXED]
Symptom: In eWc ,when config the Security profile ,select WEP mode ,and 64bit or 128bit ,relead the Web page it show error.
10. [FEATURE CHANGED]
Change eWC UI. WEP key will be masked by “*****”.
11. [BUG FIXED]
In eWC, when edit the MAC filter, sometimes device will crash..
12. [BUG FIXED]
Symptom: In WebUI fragmentation threshold range is 256 to 2432, in SMT it is from 800 to 2432.
13. [BUG FIXED]
Symptom: MAC filter function doesn't work properly.
14. [BUG FIXED]
System: Web will hang after changing setting in RADIUS page.
15. [BUG FIXED]
In web UI page, create 16 different security, edit 8 different SSID setting, sometimes web UI hang, sometimes DUT reboot with some message.
16. [BUG FIXED]
Fix the problem of creating WDS link between APs, it must set block intra-BSS traffic.
17. [BUG FIXED]
Merge ICMP bug solution from G-3000.

Modification in 3.50(AAC.1)_20050712 | 07/12/2005

1. [FEATURE CHANGED]
Change AP code from FullMAC to SoftMAC.
2. [FEATURE ENHANCED]
Support multiple ESSID feature.
3. [FEATURE ENHANCED]
Support alternative incoming vlan tag.
4. [FEATURE ENHANCED]
Support WPA2 AES encryption.
5. [FEATURE ENHANCED]
Change configuration style to profile-based setting. eWC and SMT menu are changed as configuration style changes.
6. [FEATURE ENHANCED]

www.zyxel.com

Support for auto configuration, including TFTP client.

7. [FEATURE ENHANCED]

Support for WLAN SNMP proprietary MIB.

8. [FEATURE ENHANCED]

Support QoS policy control for SSID.

Modification in 3.50(AAC.0)C0 | 07/13/2005

1. [FEATURE CHANGE]

Modify to FCS version.

Modification in 3.50(AAC.0)b1 | 05/25/2005

1. First release for C3 firmware

ZYXEL
CONFIDENTIAL

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	Vantage Related Command	Wireless LAN Profile Configuration 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				
	active		[on/off]	set on/off wlan
	association			display association list
	chid		[channel id]	set channel
	essid		[ess id]	set ESS ID
	scan			scan wireless channels
	version			display WLAN version information
	ssidprofile			apply ssid profile to AP
	bksan		<period, 0:off>	set background scan period
	bkshow			show background scan result

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 client 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
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.
8021x	debug	reauth	<index, 1~16> <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

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.

Wireless LAN Profile Configuration Related Command

[Home](#)

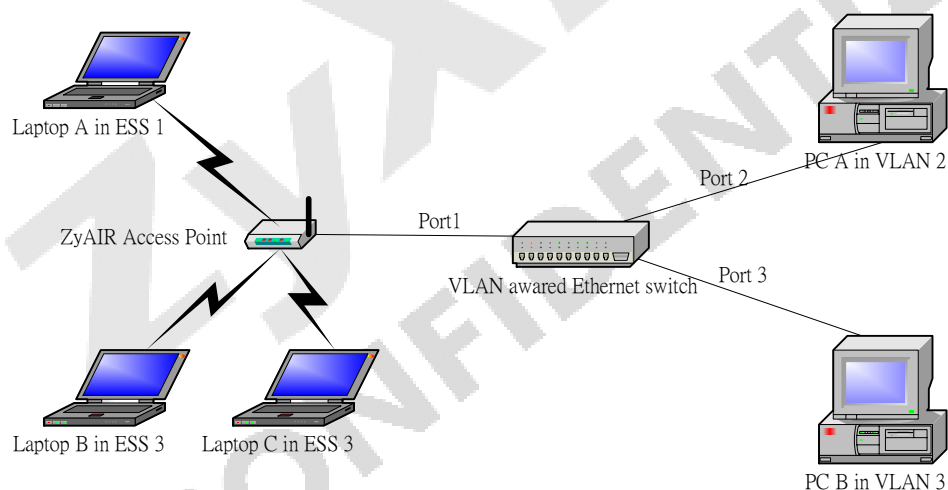
Command						Description
wcfg						
	ssid					
		<1/2/3/.../16>				
			name		<profile name>	set name of the SSID profile
			ssid		<ssid>	set SSID
			vlan		<vlan ID>	set VLAN ID
			rxvlan		<rx vlan ID>	set Rx VLAN ID
			security		<security profile name>	set selected security profile index

			radius		<radius profile name>	set selected radius profile index
			qos		<qos profile name>	set selected qos profile index
			l2isolation		<enable disable>	set L2 isolation enable / disable
			macfilter		<enable disable>	set macfilter enable / disable
			clear			clear profile setting to default
			save			save current profile to flash
			show			display current profile information
		display				display a brief list of all SSID profiles
		saveall				save all changed profiles into flash
	security					
		<1/2/3/.../16>				
			name		<profile name>	set name of the security profile
			mode		<security mode>	security system mode selection.
			wep			
				keysize	<64 128> <ascii hex>	set WEP keysize (64-bits / 128-bits) and WEP key encoding
				auth	<open shared auto>	set WEP authentication method
				key1		set WEP key string 1
				key2		set WEP key string 2
				key3		set WEP key string 3
				key4		set WEP key string 4
				keyindex		key index (1~4)
			reauthtime		<seconds>	time for re-authentication
			idletime		<seconds>	idle time before force de-association
			groupkeytime		<seconds>	time for group key update
			passphrase		<key string>	passphrase for WPA-PSK and WPA2-PSK
			clear			clear profile setting to default
			save			save current profile to flash
			show			display current profile information
		display				display a brief list of all security profiles
		saveall				save all changed profiles into flash
	radius					
		<1/2/3/4>				
			name		<profile name>	set name of the radius profile
			primaryauth		<host> <port> <shared secret> <enable disable>	set primary radius authentication server setting
			primaryacct		<host> <port> <shared secret> <enable disable>	set primary radius accounting server setting
			backupauth		<host> <port> <shared secret> <enable disable>	set backup radius authentication server setting
			backupacct		<host> <port> <shared secret> <enable disable>	set backup radius accounting server setting
			clear			clear profile setting to default
			save			save current profile to flash

			show			display current profile information
		display				display a brief list of all radius profiles
		saveall				save all changed profiles into flash
	autocfg					
		server			<IP> <filename>	setup auto configuration TFTP server IP and filename, only works when static IP is used
		dhcp			[enable disable]	control auto configuration through DHCP setting

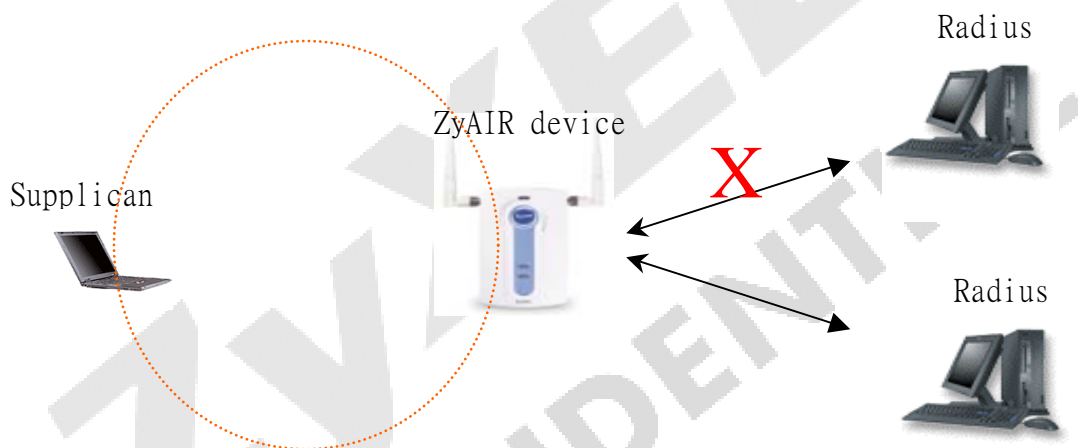
Appendix 2: Multi-ESS with VLAN

Since G-3000H supports multiple ESSID to enhance wireless access, it can work with VLAN to extend the group of users from wireless LAN to wired Ethernet. Administrator can assign a VLAN ID to each configurable SSID profile. The following graph is an illustration to test the function.



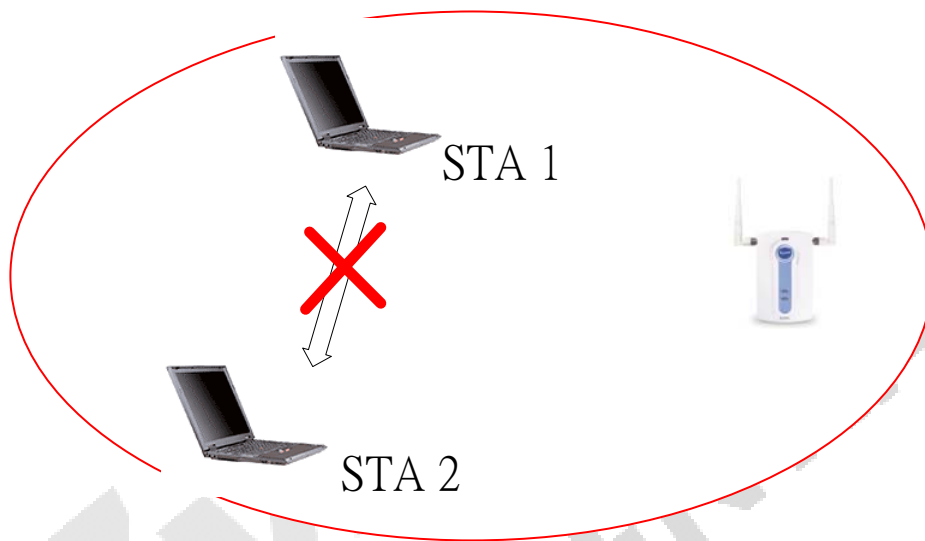
Appendix 3: Backup RADIUS Server

ZyAIR devices support backup radius server and accounting server 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.



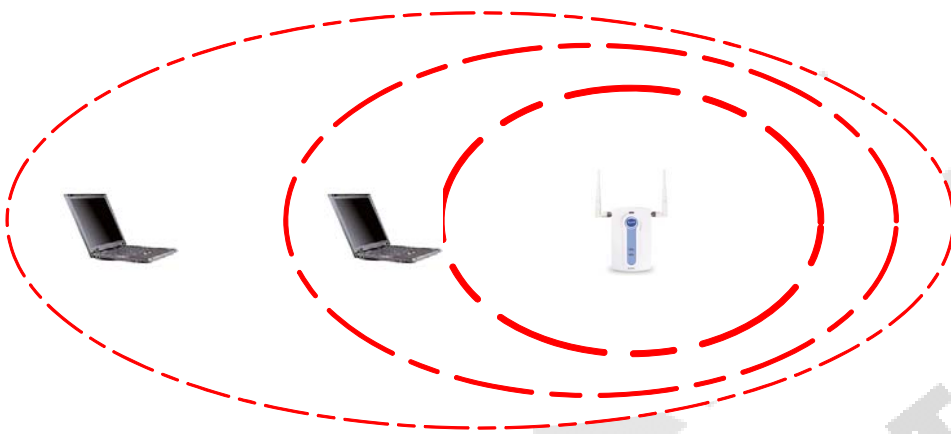
Appendix 4: Blocking Intra-BSS traffic

For performance and security issues, G-3000H 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.



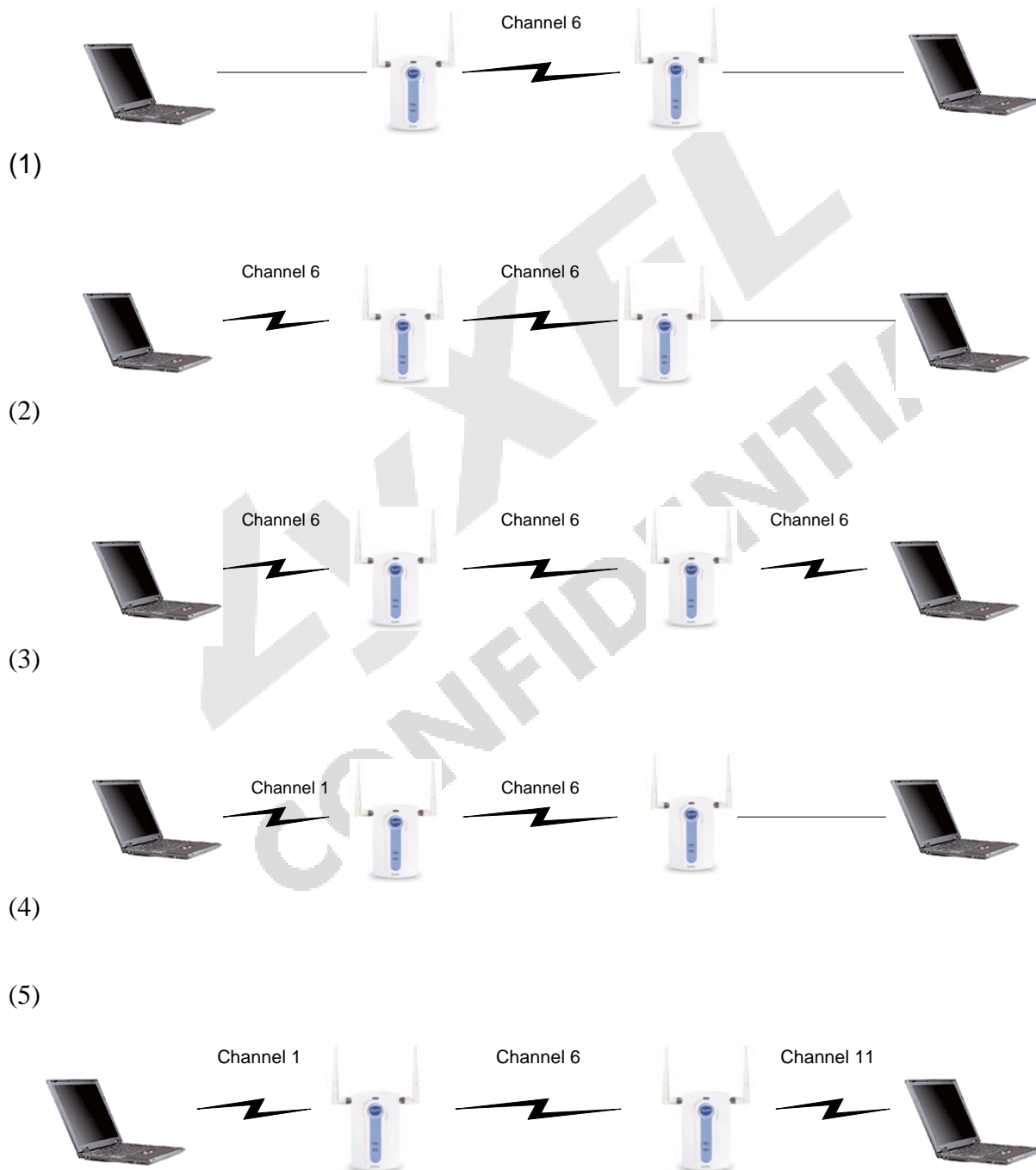
Appendix 5: Configurable Output Power

G-3000H 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.

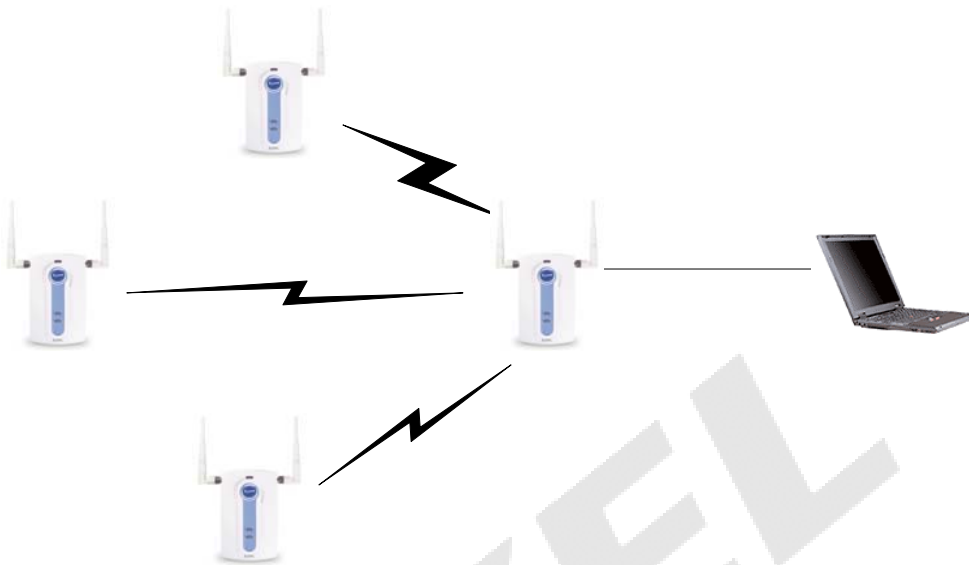


Appendix 6: WDS

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 :



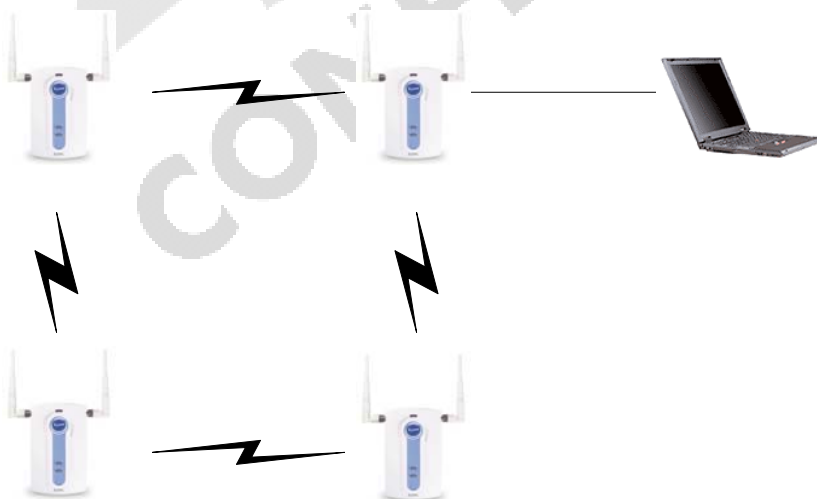
(6)



(7)



(8)



Appendix 7: 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.

