

NWA-3500

802.11 a/b/g Wireless Access Point

Support Notes

Revision 0.8

[Nov 2006](#)



INDEX

1. Configuring the Profile Base.....	3
1.1 Profile definition	3
1.2 Deploying NWA-3500 profiles	3
1.3 Deploying NWA-3500 Layer-2 Isolation profile	5
1.4 Constructing SSID profiles	6
2. Application - Dual Radio support.....	8
2.1 Configuring the office NWA-3500.....	9
2.2 Configuring the warehouse NWA-3500.....	13
2.3 Checking the WDS availability.....	15
2.4 Troubleshooting the WDS	16
FAQ	17
A. ZyNOS FAQ.....	17
B. Wireless FAQ.....	20

1. Configuring the Profile Base

1.1 Profile definition

On NWA-3500, a new GUI style is adopted for configuration, and it's more flexible to configure different kinds of wireless SSID situations with the new interface. The idea is taking advantage of the "object-oriented" principle to design wireless setup functions; so when you finish making changes to each profile, a suitable profile can be chosen for the current configuration. With this method, we can easily use any profile without repeating the configuration process.

In this chapter, we will show you how to configure the wireless settings with profile-based configuration.

1.2 Deploying NWA-3500 profiles

Here we use profiles to configure the specific security mode for SSID. As NWA-3500 provides 16 sets of user-definable profiles, you may follow the Web GUI steps to set up the security profile.



Log into the NWA-3500 GUI, and select the wireless option to configure the wireless setting.

First of all, we'll configure profiles such as security, RADIUS and Layer-2 Isolation, where pre-configured profiles can be used to construct the new wireless environment.

NWA-3500 pre-defined 16 sets of security profiles as "security1" to "security16" successively; you may choose and edit any of these.

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter																																																			
		<table border="1"> <thead> <tr> <th>Index</th> <th>Profile Name</th> <th>Security Mode</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>security01</td> <td>WPA-PSK</td> </tr> <tr> <td>2</td> <td>security02</td> <td>None</td> </tr> <tr> <td>3</td> <td>security03</td> <td>None</td> </tr> <tr> <td>4</td> <td>security04</td> <td>None</td> </tr> <tr> <td>5</td> <td>security05</td> <td>None</td> </tr> <tr> <td>6</td> <td>security06</td> <td>None</td> </tr> <tr> <td>7</td> <td>security07</td> <td>None</td> </tr> <tr> <td>8</td> <td>security08</td> <td>None</td> </tr> <tr> <td>9</td> <td>security09</td> <td>None</td> </tr> <tr> <td>10</td> <td>security10</td> <td>None</td> </tr> <tr> <td>11</td> <td>security11</td> <td>None</td> </tr> <tr> <td>12</td> <td>security12</td> <td>None</td> </tr> <tr> <td>13</td> <td>security13</td> <td>None</td> </tr> <tr> <td>14</td> <td>security14</td> <td>None</td> </tr> <tr> <td>15</td> <td>security15</td> <td>None</td> </tr> <tr> <td>16</td> <td>security16</td> <td>None</td> </tr> </tbody> </table>	Index	Profile Name	Security Mode	1	security01	WPA-PSK	2	security02	None	3	security03	None	4	security04	None	5	security05	None	6	security06	None	7	security07	None	8	security08	None	9	security09	None	10	security10	None	11	security11	None	12	security12	None	13	security13	None	14	security14	None	15	security15	None	16	security16	None			
Index	Profile Name	Security Mode																																																						
1	security01	WPA-PSK																																																						
2	security02	None																																																						
3	security03	None																																																						
4	security04	None																																																						
5	security05	None																																																						
6	security06	None																																																						
7	security07	None																																																						
8	security08	None																																																						
9	security09	None																																																						
10	security10	None																																																						
11	security11	None																																																						
12	security12	None																																																						
13	security13	None																																																						
14	security14	None																																																						
15	security15	None																																																						
16	security16	None																																																						

Wireless security is vital for networks to protect wireless communication between wireless stations, access points and the wired network. Wireless security methods available on NWA-3500 include Data Encryption, Wireless Client Authentication, MAC access restriction and NWA-3500 identity cloaking.

Select a security configuration profile and enter the detailed information. As shown on the below figure, you need to provide the profile name and choose “security mode” in 10 security encryption types offered.

WIRELESS LAN

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Profile Name :		<input type="text" value="security02"/>			
Security Mode :		<div style="border: 1px solid black; padding: 2px;"> None WEP 8021x-Only 8021x-Static64 8021x-Static128 WPA WPA-PSK WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX </div>			<input type="button" value="Reset"/>

If you choose the “WPA2-PSK” security type, please assign a string of pre-shared key of up to 46 bits in length.

Wireless SSID Security RADIUS Layer-2 Isolation MAC Filter

Layer-2 Isolation Configuration


Profile Name

Allow devices with these MAC addresses

Set	MAC Address	Description	Set	MAC Address	Description
1	<input type="text" value="00:11:11:11:11:11"/>	<input type="text" value="test 1"/>	17	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
2	<input type="text" value="11:00:00:00:00:00"/>	<input type="text" value="test 2"/>	18	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
3	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	19	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
4	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	20	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
5	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	21	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
6	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	22	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
7	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	23	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
8	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	24	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
9	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	25	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
10	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	26	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>

Wireless SSID Security RADIUS Layer-2 Isolation MAC Filter


	Index	Profile Name
<input checked="" type="radio"/>	1	Jamie_ISOL_Test
<input type="radio"/>	2	l2isolation02
<input type="radio"/>	3	l2isolation03
<input type="radio"/>	4	l2isolation04
<input type="radio"/>	5	l2isolation05
<input type="radio"/>	6	l2isolation06
<input type="radio"/>	7	l2isolation07
<input type="radio"/>	8	l2isolation08
<input type="radio"/>	9	l2isolation09
<input type="radio"/>	10	l2isolation10
<input type="radio"/>	11	l2isolation11
<input type="radio"/>	12	l2isolation12
<input type="radio"/>	13	l2isolation13
<input type="radio"/>	14	l2isolation14
<input type="radio"/>	15	l2isolation15
<input type="radio"/>	16	l2isolation16



1.4 Constructing SSID profiles

When the NWA-3500 is configured as an access point in AP+Bridge of MBSSID mode, you need to choose the SSID profile(s) for the wireless network. Use the wireless -> SSID screen to see information of SSID profiles on the NWA-3500, then use the wireless->SSID->Edit screen to make changes.

Wireless								
	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter			
●	1	VoIP_SSID	ZyXEL01	security01	radius01	VoIP	Disable	Disable
●	2	Guest_SSID	ZyXEL02	security01	radius01	NONE	Jamie_ISOL_Test	Disable
●	3	SSID03	cso8537_andy	security01	radius01	NONE	Disable	Disable
●	4	SSID04	ZyXEL04	security01	radius01	NONE	Disable	Disable
●	5	SSID05	ZyXEL05	security01	radius01	NONE	Disable	Disable
●	6	SSID06	ZyXEL06	security01	radius01	NONE	Disable	Disable
●	7	SSID07	ZyXEL07	security01	radius01	NONE	Disable	Disable
●	8	SSID08	ZyXEL08	security01	radius01	NONE	Disable	Disable
●	9	SSID09	ZyXEL09	security01	radius01	NONE	Disable	Disable
●	10	SSID10	ZyXEL10	security01	radius01	NONE	Disable	Disable
●	11	SSID11	ZyXEL11	security01	radius01	NONE	Disable	Disable
●	12	SSID12	ZyXEL12	security01	radius01	NONE	Disable	Disable
●	13	SSID13	ZyXEL13	security01	radius01	NONE	Disable	Disable
●	14	SSID14	ZyXEL14	security01	radius01	NONE	Disable	Disable
●	15	SSID15	ZyXEL15	security01	radius01	NONE	Disable	Disable
●	16	SSID16	ZyXEL16	security01	radius01	NONE	Disable	Disable




Each SSID profile on NWA-3500 refers to a set of settings made on the following screens:

- ✓ Wireless ->security (one of the security profiles).
- ✓ Wireless ->RADIUS (one of the RADIUS profiles).
- ✓ Wireless ->MAC filter (the MAC filter list, if activated in the SSID profile).
- ✓ Wireless ->Layer-2 Isolation (the Layer-2 isolation filter list, if activated in the SSID profile)
- ✓ Also, use the VLAN screen to set up wireless VLANs based on SSID.

Configuring the fields on above screens in order to use the SSID profile settings. Select an SSID profile in the wireless -> SSID screen and click “Edit” to display the following screen.

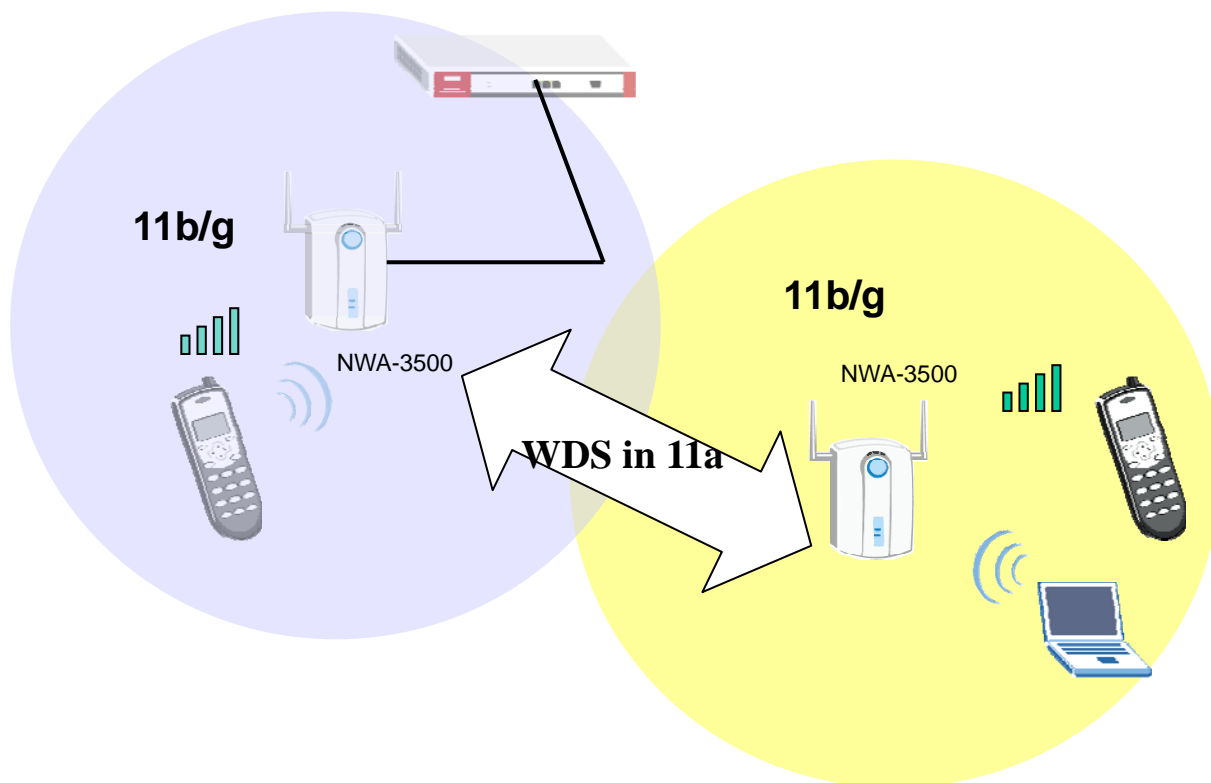
WIRELESS LAN

Wireless	
SSID	Security
Profile Name :	Jamie_NWA3500
SSID :	ZyXEL_NWA3500
Hide Name(SSID) :	Disable
Security :	JamieWPA2_PSK
RADIUS :	radius01
QoS :	NONE
L2 Isolation :	Jamie_ISOL_Test
Intra-BSS Traffic blocking :	Enable
MAC Filtering :	Jamie_MACF_Test



2. Application - Dual Radio support

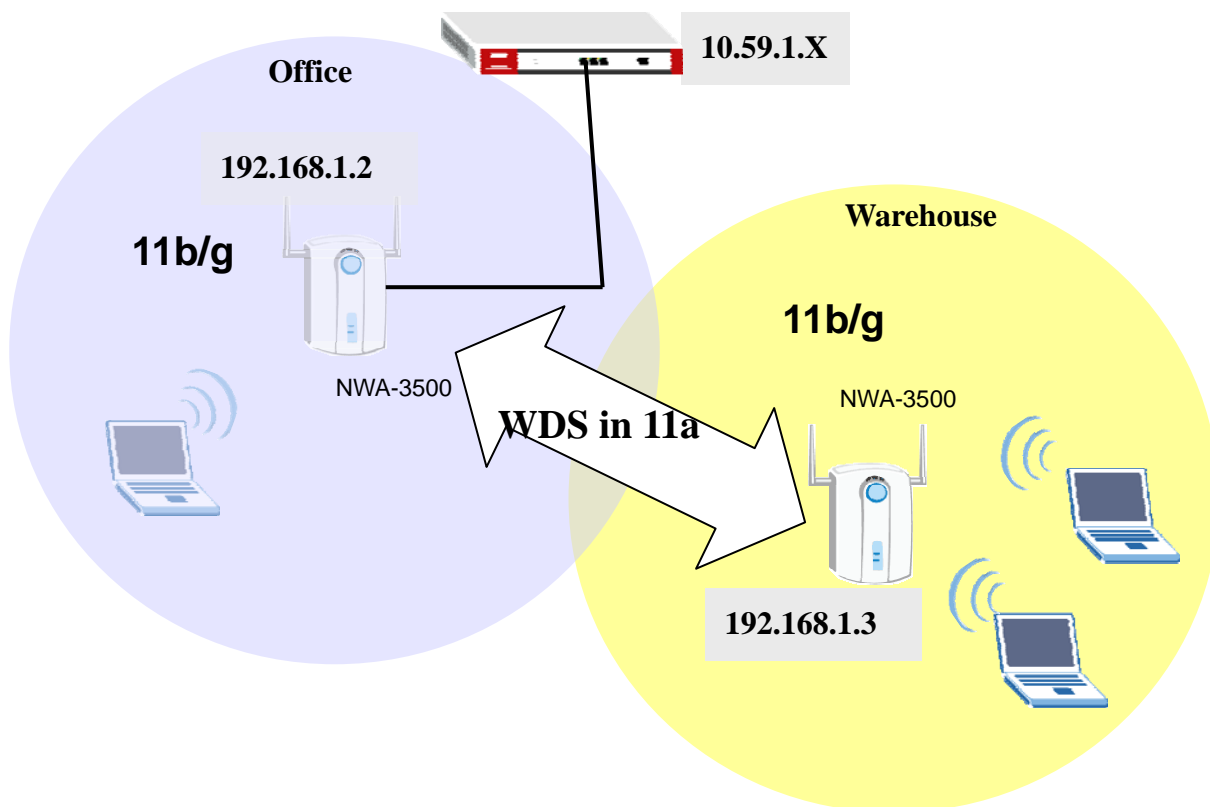
When connect from outside the network to inside with 802.11a mode running WDS, you will benefit from more throughput and lower interference.



The network topology above is for illustrating this application. We installed one NWA-3500 as the main office access point that connects to the router, and the other NWA-3500 was deployed in the warehouse separately.

In some cases, the outside NWA-3500 may not connect to the Ethernet through physical wires; therefore we provided the WDS feature to assist establishing network connection wirelessly.

NWA-3500 separates its antennas for 802.11a mode and b/g mode respectively, and each WAN for 802.11 a/b/g wireless modes can be configured separately. Please see the following application example.



Configuration information in this example:

NWA-3500 in the Office	NWA-3500 in the Warehouse
LAN address: 192.168.1.2	LAN address:192.168.1.3
WLAN1: 802.11 b/g (Access Point mode)	WALN1: 802.11 b/g (Access Point mode)
WLAN2: 802.11a (Bridge/Repeater mode)	WLAN2: 802.11a (Bridge/Repeater mode)

To achieve this, we have to complete the following tasks:

- ◆ Configure Dual WLAN to 802.11a and 802.11b/g modes separately.
- ◆ On the warehouse NWA-3500, the clients will connect to the Internet through WDS to the office NWA-3500.

Please see the following step-by-step process.

2.1 Configuring the office NWA-3500

- Step 1. Make sure NWA-3500 links to the router correctly
- Step 2. Pre-define SSID profiles and Security profiles

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter			
	Index	Profile Name	SSID	Security	RADIUS	QoS	Layer-2 Isolation	MAC Filter
	1	VoIP_SSID	ZyXEL01	security01	radius01	VoIP	Disable	Disable
	2	Guest_SSID	ZyXEL02	security01	radius01	NONE	Jamie_ISOL_Test	Disable
	3	SSID03	Jamie_WDS	security01	radius01	NONE	Disable	Disable
	4	Jamie_NWA3500	ZyXEL_NWA3500	security01	radius01	NONE	Disable	Disable
	5	SSID05	ZyXEL05	security01	radius01	NONE	Disable	Disable
	6	SSID06	ZyXEL06	security01	radius01	NONE	Disable	Disable
	7	SSID07	ZyXEL07	security01	radius01	NONE	Disable	Disable
	8	SSID08	ZyXEL08	security01	radius01	NONE	Disable	Disable
	9	SSID09	ZyXEL09	security01	radius01	NONE	Disable	Disable
	10	SSID10	ZyXEL10	security01	radius01	NONE	Disable	Disable
	11	SSID11	ZyXEL11	security01	radius01	NONE	Disable	Disable
	12	SSID12	ZyXEL12	security01	radius01	NONE	Disable	Disable
	13	SSID13	ZyXEL13	security01	radius01	NONE	Disable	Disable
	14	SSID14	ZyXEL14	security01	radius01	NONE	Disable	Disable
	15	SSID15	ZyXEL15	security01	radius01	NONE	Disable	Disable
	16	SSID16	ZyXEL16	security01	radius01	NONE	Disable	Disable


We took “SSID04” to configure, as shown on the following screen. Provide a SSID name to identify the wireless connection, and then assign a security profile to protect the wireless connection. We will introduce the security configuration in the next section.

WIRELESS LAN

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Profile Name :	Jamie_NWA3500				
SSID :	ZyXEL_NWA3500				
Hide Name(SSID) :	Disable				
Security :	JamieWPA2_PSK				
RADIUS :	radius01				
QoS :	NONE				
L2 Isolation :	Disable				
Intra-BSS Traffic blocking :	Disable				
MAC Filtering :	Disable				

Select “Security02” to configure the security profile. Provide a name to the Security profile, choose “WPA-PSK” security mode, and then assign a pre-shared key to the field.

WIRELESS LAN

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
WLAN Adaptor	WLAN1 				
Operating Mode	Access Point				
802.11 Mode	802.11b+g				
<input type="checkbox"/> Super Mode					
Choose Channel ID	Channel-10 2457MHz <input type="button" value="Scan"/>				
RTS/CTS Threshold	2346 (256 ~ 2346)				
Fragmentation Threshold	2346 (256 ~ 2346)				
Output Power	100%				
SSID Profile	Jamie_NWA3500				
<input checked="" type="checkbox"/> Enable Breathing LED					
<input checked="" type="checkbox"/> Enable Spanning Tree Protocol (STP)					
<input type="checkbox"/> Roaming Active					
<input type="button" value="Apply"/> <input type="button" value="Reset"/>					

Step 4. Set up the WDS Bridge mode for WLAN 2.

Select WLAN2 and 802.11a mode. The most important WLAN2 setting is enabling WDS Security, where you must enter the remote bridge MAC Address and a PSK to negotiate with the warehouse counterpart.

****Note:** The two NWA-3500 sites should use the same PSK.

Wireless

WLAN Adaptor: WLAN2
 Operating Mode: Bridge/Repeater
 802.11 Mode: 802.11a
 Choose Channel ID: Channel-040 5200MHz
 Operating Channel: Channel-040
 RTS/CTS Threshold: 2346 (256 ~ 2346)
 Fragmentation Threshold: 2346 (256 ~ 2346)
 Enable WDS Security

#	Active	Remote Bridge MAC Address	PSK
1	<input checked="" type="checkbox"/>	00:13:49:df:42:7c	12345678
2	<input type="checkbox"/>	00:00:00:00:00:00	
3	<input type="checkbox"/>	00:00:00:00:00:00	
4	<input type="checkbox"/>	00:00:00:00:00:00	
5	<input type="checkbox"/>	00:00:00:00:00:00	

Enable Breathing LED
 Enable Spanning Tree Protocol (STP)

Apply Reset

2.2 Configuring the warehouse NWA-3500

Similar to the office site, the Security and SSID profiles should be configured first. WLAN1 is assigned to the 802.11b+g mode for local users, and WLAN2 to the 802.11a mode for WDS.

Please refer to the following screen to set up the remote wireless environment.

Choose “WPA-PSK” to set up the security mode and assign a pre-shared key.

WIRELESS LAN

Wireless SSID Security RADIUS Layer-2 Isolation MAC Filter

Profile Name : security01
 Security Mode : WPA-PSK
 Pre-Shared Key : 12345678
 ReAuthentication Timer : 1800 (in seconds)
 Idle Timeout : 3600 (in seconds)
 Group Key Update Timer : 1800 (in seconds)

Apply Reset

Wireless								
SSID		Security	RADIUS	Layer-2 Isolation	MAC Filter			
Index	Profile Name	SSID	Security	RADIUS	QoS	Layer-2 Isolation	MAC Filter	
1	VoIP_SSID	ZyXEL01	security01	radius01	VoIP	Disable	Disable	
2	Guest_SSID	ZyXEL02	security01	radius01	NONE	l2isolation01	Disable	
3	SSID03	Jamie_WareHouse	security01	radius01	NONE	Disable	Disable	
4	SSID04	ZyXEL04	security01	radius01	NONE	Disable	Disable	
5	SSID05	ZyXEL05	security01	radius01	NONE	Disable	Disable	
6	SSID06	ZyXEL06	security01	radius01	NONE	Disable	Disable	
7	SSID07	ZyXEL07	security01	radius01	NONE	Disable	Disable	
8	SSID08	ZyXEL08	security01	radius01	NONE	Disable	Disable	
9	SSID09	ZyXEL09	security01	radius01	NONE	Disable	Disable	
10	SSID10	ZyXEL10	security01	radius01	NONE	Disable	Disable	
11	SSID11	ZyXEL11	security01	radius01	NONE	Disable	Disable	
12	SSID12	ZyXEL12	security01	radius01	NONE	Disable	Disable	
13	SSID13	ZyXEL13	security01	radius01	NONE	Disable	Disable	
14	SSID14	ZyXEL14	security01	radius01	NONE	Disable	Disable	
15	SSID15	ZyXEL15	security01	radius01	NONE	Disable	Disable	
16	SSID16	ZyXEL16	security01	radius01	NONE	Disable	Disable	

Edit

Configure a SSID name with “Jamie_WareHouse” to identify the wireless network and choose the pre-defined security mode.

WIRELESS LAN

Wireless		SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Profile Name :	SSID03					
SSID :	Jamie_WareHouse					
Hide Name(SSID) :	Disable					
Security :	security01					
RADIUS :	radius01					
QoS :	NONE					
L2 Isolation :	Disable					
Intra-BSS Traffic blocking :	Disable					
MAC Filtering :	Disable					

Apply Reset

Assign WLAN1 to the 802.11b+g mode for user to join the network, and assign WLAN2 to the 802.11a mode mainly for WDS. Remember, the pre-shared key must be identical to the office site.

WIRELESS LAN

Wireless SSID Security RADIUS Layer-2 Isolation MAC Filter

WLAN Adaptor WLAN1

Operating Mode Access Point

802.11 Mode 802.11b+g

Super Mode

Choose Channel ID Channel-10 2457MHz or Scan

RTS/CTS Threshold 2346 (256 ~ 2346)

Fragmentation Threshold 2346 (256 ~ 2346)

Output Power 100%

SSID Profile SSID03

Enable Breathing LED

Enable Spanning Tree Protocol (STP)

Roaming Active

Apply Reset

Wireless

WLAN Adaptor WLAN2

Operating Mode Bridge/Repeater

802.11 Mode 802.11a

Choose Channel ID Channel-040 5200MHz

Operating Channel Channel-040

RTS/CTS Threshold 2346 (256 ~ 2346)

Fragmentation Threshold 2346 (256 ~ 2346)

Enable WDS Security

#	Active	Remote Bridge MAC Address	PSK
1	<input checked="" type="checkbox"/>	00:13:49:df:42:ac	12345678
2	<input type="checkbox"/>	00:00:00:00:00:00	
3	<input type="checkbox"/>	00:00:00:00:00:00	
4	<input type="checkbox"/>	00:00:00:00:00:00	
5	<input type="checkbox"/>	00:00:00:00:00:00	

Enable Breathing LED

Enable Spanning Tree Protocol (STP)

Apply Reset

2.3 Checking the WDS availability

When individual configuration of the office and warehouse NWA-3500s is completed, you can use a PC to access the network through the warehouse NWA-3500. The

PC will request an IP address from the office router, and then you can check any external IP address with the “PING” command to assure that the Internet can be accessed successfully.

2.4 Troubleshooting the WDS

If you can't join to network through the warehouse NWA-3500, please check the following steps:

1. Does the connection between office NWA-3500 and the router work correctly? You can hook up a PC with the office NWA-3500 and use “PING” command to check the connection. If you cannot PING an external IP address successfully, then check to the WAN configuration on the router.
2. Have the clients been connected to the warehouse NWA-3500 correctly? You can connect a PC to the NWA-3500 directly to assure that the connection between NWA-3500 and PC has been established properly.
3. If your PC can't connect to the NWA-3500, you may check to the WLAN1 mode configuration, including 802.11b+g mode, security mode and Layer-2 Isolation.
4. Check the WDS configuration of both local site and remote site.
 - A. Check Remote Bridge MAC address is correct
 - B. Check if the two sites have the same pre-shared key.
 - C. Make sure that the WDS has the same operation channel. Ex. Channel-040
5200MHz

FAQ

A. ZyNOS FAQ

A1. What is ZyNOS?

ZyNOS is ZyXEL's proprietary Network Operating System. It is the platform on all ZyXEL device that delivers network services and applications. It is designed in a modular fashion so it is easy for developers to add new features. New ZyNOS software upgrades can be easily downloaded from our FTP sites as they become available.

A 2. How do I access the embeded web configurator?

The Web configurator is configuration interface via user's web browser, which can be access by typing in the IP address of the NWA-3100 in users web browser. To access the NWA-3100's web configurator via web browser, the configuration PC must be in the same IP segment of NWA-3100 and NWA-3100 must be reachable to the configuration station.

A 3. What is the default username and password? Moreover, how do I change it?

The default username is "admin" and can not be changed, the default password is 1234. You can change the password once you enter the web configuration menu under "ADVANCED"->"SYSTEM" and press the Password tab. At the password screen type in the old password and the new password and retype to confirm than press "Apply" button to save the change.

A 4. How do I upload the ZyNOS firmware code via embeded web configurator?

The procedure for uploading ZyNOS via embeded web configurator is as follows.

- a. Log on into the web configurator
- b. Press "MAINTENANCE" from the left menu.

- c. Press "F/W Upload" from the left menu.
- d. Press "browse" button and point to the directory where the firmware you want to upload is kept and press "Upload" button
- e. It will prompt you the firmware is upload successful and NWA-3100 will reboot.

A 5. How do I upgrade/backup the ZyNOS firmware by using TFTP client program via LAN?

The NWA-3100 allows you to transfer the firmware from/to NWA-3100 by using TFTP program via LAN. The procedure for uploading ZyNOS via TFTP, FTP is as follows.

- a. Use the TELNET client program in your PC to login to your Prestige.
- b. Enter CI command **'sys stdio 0'** in menu 24.8 to disable console idle timeout
- c. To upgrade firmware, use TFTP client program to put firmware in file **'ras'** in the NWA-3100. After data transfer is finished, the Prestige will program the upgraded firmware into FLASH ROM and reboot itself.
- d. To backup your firmware, use the TFTP client program to get file **'ras'** from the NWA-3100.

A 6. How do I upgrade/backup the ZyNOS firmware by using FTP client program via LAN?

The NWA-3100 allows you to transfer the firmware from/to NWA-3100 by using FTP program via LAN. The procedure for uploading ZyNOS via FTP is as follows.

- a. Use the TELNET client program in your PC to login to your Prestige.
- b. To upgrade firmware, use FTP client program to put firmware in file **'ras'** in the NWA-3100. After data transfer is finished, the Prestige will program the upgraded firmware into FLASH ROM and reboot itself.
- c. To backup your firmware, use the FTP client program to get file **'ras'** from the NWA-3100.

A 7. How do I upload or backup ROMFILE via web configurator?

In some situations, you may need to upload the ROMFILE, restore to previous saved configuration, or the need of resetting SMT to factory default.

The procedure for uploading ROMFILE via the web configurator is as follows.

- a. Log on into the Web Configurator
- b. Press "MAINTENANCE" from the left menu.
- c. Press "Configuration" from the left menu.
- d. Press "Restore" tab and press browse button point to the directory where the romfile you want to upload is stored.
- e. Press "Upload" button.

The procedure for backup ROMFILE via the Web Configurator is as follow

- a. Log on into the Web Configurator
- b. Press "MAINTENANCE" from the left menu.
- c. Press "Configuration" from the left menu.
- d. Press "Backup" tab and press "Backup" button, a pop up windows will ask you where to store the back up ROMFILE.
- e. Press "Save file" and browse to where you want the file be save.
- f. Press "Save" button.

A 8. How do I backup/restore configurations by using TFTP client program via LAN?

- a. Use the TELNET client program in your PC to login to your NWA-3100.
- b. Enter CI command **'sys stdio 0'** in menu 24.8 to disable console idle timeout.
- c. To backup the configurations, use TFTP client program to get file **'rom-0'** from the Prestige.
- d. To restore the configurations, use the TFTP client program to put your configuration in file **ROM-0** in the NWA-3100.

A 9. How do I backup/restore configurations by using FTP client program via LAN?

- a. Use the TELNET client program in your PC to login to your NWA-3100.
- b. To backup the configurations, use FTPclient program to get file **'rom-0'** from the Prestige.
- c. To restore the configurations, use the FTP client program to put your configuration in file **ROM-0** in the NWA-3100.

B. Wireless FAQ

B1. What is a Wireless LAN ?

Wireless LANs provide all the functionality of wired LANs, without the need for physical connections (wires). Data is modulated onto a radio frequency carrier and transmitted through the ether. Typical bit-rates are 11Mbps and 54Mbps, although in practice data throughput is half of this. Wireless LANs can be formed simply by equipping PC's with wireless NICs. If connectivity to a wired LAN is required an Access Point (AP) is used as a bridging device. AP's are typically located close to the centre of the wireless client population.

B2. What are the advantages of Wireless LANs ?

a. Mobility:

Wireless LAN systems can provide LAN users with access to real-time information anywhere in their organization. This mobility supports productivity and service opportunities not possible with wired networks.

b. Installation Speed and Simplicity:

Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.

c. Installation Flexibility:

Wireless technology allows the network to go where wire cannot go.

d. Reduced Cost-of-Ownership:

While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves and changes.

e. Scalability:

Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that enable roaming over a broad area.

B3. What are the disadvantages of Wireless LANs ?

The speed of Wireless LAN is still relative slower than wired LAN. The most popular wired LAN is operated in 100Mbps, which is almost 10 times of that of Wireless LAN (10Mbps). A faster wired LAN standard (1000Mbps), which is 100 times faster, becomes popular as well. The setup cost of Wireless LAN is relative high because the equipment cost including access point and PCMCIA Wireless LAN card is higher than hubs and CAT 5 cables.

B4. Where can you find wireless 802.11 networks ?

Airports, hotels, and even coffee shops like Starbucks are deploying 802.11 networks so people can wirelessly browse the Internet with their laptops. As these types of networks increase, this will create additional security risk for the remote user if not properly protected.

B5. What is an Access Point ?

The AP (access point also known as a base station) is the wireless server that with an antenna and a wired Ethernet connection that broadcasts information using radio signals. AP typically act as a bridge for the clients. It can pass information to wireless LAN cards that have been installed in computers or laptops allowing those computers to connect to the campus network and the Internet without wires.

B6. What is IEEE 802.11 ?

The IEEE 802.11 is a wireless LAN industry standard, and the objective of IEEE 802.11 is to make sure that different manufactures' wireless LAN devices can communicate to each other. 802.11 provides 1 or 2 Mbps transmission in the 2.4 GHz ISM band using either FHSS or DSSS.

B7. What is 802.11b ?

802.11b is the first revision of 802.11 standard allowing data rates up to 11Mbps in the 2.4GHz ISM band. Also known as 802.11 High-Rate and Wi-Fi. 802.11b only uses DSSS, the maximum speed of 11Mbps has fallbacks to 5.5, 2 and 1Mbps.

B8. How fast is 802.11b ?

The IEEE 802.11b standard has a nominal speed of 11 megabits per second (Mbps). However, depending on signal quality and how many other people are using the wireless ethernet through a particular Access Point, usable speed will be much less (on the order of 4 or 5 Mbps, which is still substantially faster than most dialup, cable and DSL modems).

B9. What is 802.11a ?

802.11a is the second revision of 802.11 that operates in the unlicensed 5 GHz band and allows transmission rates of up to 54Mbps. 802.11a uses OFDM (orthogonal frequency division multiplexing) as opposed to FHSS or DSSS. Higher data rates are possible by combining channels. Due to higher frequency, range is less than lower frequency systems (i.e., 802.11b and 802.11g) and can increase the cost of the overall solution because a greater number of access points may be required. 802.11a is not directly compatible with 802.11b or 802.11g networks. In other words, a user equipped with an 802.11b or 802.11g radio card will not be able to interface directly to an 802.11a access point. Multi-mode NICs will solve this problem.

B10. What is 802.11g ?

802.11g is an extension to 802.11b. 802.11g increases 802.11b's data rates to 54 Mbps and still utilizes the 2.4 GHz ISM. Modulation is based upon OFDM (orthogonal frequency division multiplexing) technology. An 802.11b radio card will interface directly with an 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. The range at 54 Mbps is less than for 802.11b operating at 11 Mbps.

B11. Is it possible to use products from a variety of vendors ?

Yes. As long as the products comply to the same IEEE 802.11 standard. The Wi-Fi logo is used to define 802.11b compatible products. Wi-Fi5 is a compatibility standard for 802.11a products running in the 5GHz band.

B12. What is Wi-Fi ?

The Wi-Fi logo signifies that a product is interoperable with wireless networking equipment from other vendors. A Wi-Fi logo product has been tested and certified by the Wireless Ethernet Compatibility Alliance (WECA). The Socket Wireless LAN Card is Wi-Fi certified, and that means that it will work (interoperate) with any brand of Access Point that is also Wi-Fi certified.

B13. What types of devices use the 2.4GHz Band ?

Various spread spectrum radio communication applications use the 2.4 GHz band. This includes WLAN systems (not necessarily of the type IEEE 802.11b), cordless phones, wireless medical telemetry equipment and Bluetooth™ short-range wireless applications, which include connecting printers to computers and connecting modems or hands-free kits to mobile phones.

B14. Does the 802.11 interfere with Bluetooth devices ?

Any time devices are operated in the same frequency band, there is the potential for interference.

Both the 802.11b and Bluetooth devices occupy the same 2.4-to-2.483-GHz unlicensed frequency range-the same band. But a Bluetooth device would not interfere with other 802.11 devices much more than another 802.11 device would interfere. While more collisions are possible with the introduction of a Bluetooth device, they are also possible with the introduction of another 802.11 device, or a new 2.4 GHz cordless phone for that matter. But, Bluetooth devices are usually low-power, so the effects that a Bluetooth device may have on an 802.11 network, if any, aren't far-reaching.

B15. Can radio signals pass through walls ?

Transmitting through a wall is possible depending upon the material used in its construction. In general, metals and substances with a high water content do not allow radio waves to pass through. Metals reflect radio waves and concrete attenuates radio waves. The amount of attenuation suffered in passing through concrete will be a function of its thickness and amount of metal re-enforcement used.

B16. What are potential factors that may causes interference among WLAN products ?**Factors of interference:**

1. Obstacles: walls, ceilings, furniture... etc.
2. Building Materials: metal door, aluminum studs.
3. Electrical devices: microwaves, monitors, electric motors.

Solution :

1. Minimizing the number of walls and ceilings
2. Antenna is positioned for best reception
3. Keep WLAN products away from electrical devices, eg: microwaves, monitors, electric motors, ..., etc.
4. Add additional APs if necessary.

B17. What's the difference between a WLAN and a WWAN ?

WLANs are generally privately owned, wireless systems that are deployed in a corporation, warehouse, hospital, or educational campus setting. Data rates are high and there are no per-packet charges for data transmission.

WWANs are generally publicly shared data networks designed to provide coverage in metropolitan areas and along traffic corridors. WWANs are owned by a service provider or carrier. Data rates are low and charges are based on usage. Specialized applications are characteristically designed around short, burst messaging.

B18. What is Ad Hoc mode ?

A wireless network consists of a number of stations without access points. Without using an access point or any connection to a wired network.

B19. What is Infrastructure mode ?

Infrastructure mode implies connectivity to a wired communications infrastructure. If such connectivity is required the Access Points must be used to connected to the wired LAN backbone. Wireless clients have their configurations set for "infrastructure mode" in order to utilize access points relaying.

B20. How many Access Points are required in a given area ?

This depends on the surrounding terrain, the diameter of the client population, and the number of clients. If an area is large with dispersed pockets of populations then extension points can be used for extend coverage.

B21. What is Direct-Sequence Spread Spectrum Technology – (DSSS) ?

DSSS spreads its signal continuously over a wide frequency band. DSSS maps the information bearing bit-pattern at the sending station into a higher data rate bit sequence using a "chipping" code. The chipping code (also known as processing gain) introduces redundancy which allows data recovery if certain bit errors occur during transmission. The FCC rules the minimum processing gain should be 10, typical systems use processing gains of 20. IEEE 802.11b specifies the use of DSSS.

B22. What is Frequency-hopping Spread Spectrum Technology – (FHSS) ?

FHSS uses a narrowband carrier which hops through a predefined sequence of several frequencies at a specific rate. This avoids problems with fixed channel narrowband noise and simple jamming. Both transmitter and receiver must have their hopping sequences synchronized to create the effect of a single "logical channel". To an unsynchronised receivers an FHSS transmission appears to be short-duration impulse noise. 802.11 may use FHSS or DSSS.

B23. Do I need the same kind of antenna on both sides of a link ?

No. Provided the antenna is optimally designed for 2.4GHz or 5GHz operation. WLAN NICs often include an internal antenna which may provide sufficient

reception.

B24. Why the 2.4 Ghz Frequency range ?

This frequency range has been set aside by the FCC, and is generally labeled the ISM band. A few years ago Apple and several other large corporations requested that the FCC allow the development of wireless networks within this frequency range. What we have today is a protocol and system that allows for unlicensed use of radios within a prescribed power level. The ISM band is populated by Industrial, Scientific and Medical devices that are all low power devices, but can interfere with each other.

B25. What is Server Set ID (SSID) ?

SSID is a configurable identification that allows clients to communicate to the appropriate base station. With proper configuration, only clients that are configured with the same SSID can communicate with base stations having the same SSID. SSID from a security point of view acts as a simple single shared password between base stations and clients.

B26. What is an ESSID ?

ESSID stands for Extended Service Set Identifier and identifies the wireless LAN. The ESSID of the mobile device must match the ESSID of the AP to communicate with the AP. The ESSID is a 32-character maximum string and is case-sensitive.

B27. How do I secure the data across an Access Point's radio link ?

Enable Wired Equivalency Protocol (WEP) to encrypt the payload of packets sent across a radio link.

B28. What is WEP ?

Wired Equivalent Privacy. WEP is a security mechanism defined within the 802.11 standard and designed to make the security of the wireless medium equal to that of a cable (wire). WEP data encryption was designed to prevent access to the network by "intruders" and to prevent the capture of wireless LAN traffic through eavesdropping. WEP allows the administrator to define a set of respective "Keys" for each wireless network user based on a "Key String" passed through the WEP encryption algorithm. Access is denied by anyone who does not have an assigned key. WEP comes in 40/64-bit and 128-bit encryption key lengths. Note, WEP has shown to have fundamental flaws in its key generation processing.

B29. What is the difference between 40-bit and 64-bit WEP ?

40 bit WEP & 64 bit WEP are the same encryption level and can interoperate. The lower level of WEP encryption uses a 40 bit (10 Hex character) as "secret key" (set

by user), and a 24 bit " Initialization Vector " (not under user control) (40+24=64). Some vendors refer to this level of WEP as 40 bit, others as 64 bit.

B30. What is a WEP key ?

A WEP key is a user defined string of characters used to encrypt and decrypt data.

B31. A WEP key is a user defined string of characters used to encrypt and decrypt data ?

No. 128-bit WEP will not communicate with 64-bit WEP. Although 128 bit WEP also uses a 24 bit Initialization Vector, but it uses a 104 bit as secret key. Users need to use the same encryption level in order to make a connection.

B32. Can the SSID be encrypted ?

WEP, the encryption standard for 802.11, only encrypts the data packets not the 802.11 management packets and the SSID is in the beacon and probe management messages. The SSID is not encrypted if WEP is turned on. The SSID goes over the air in clear text. This makes obtaining the SSID easy by sniffing 802.11 wireless traffic.

B33. By turning off the broadcast of SSID, can someone still sniff the SSID ?

Many APs by default have broadcasting the SSID turned on. Sniffers typically will find the SSID in the broadcast beacon packets. Turning off the broadcast of SSID in the beacon message (a common practice) does not prevent getting the SSID; since the SSID is sent in the clear in the probe message when a client associates to an AP, a sniffer just has to wait for a valid user to associate to the network to see the SSID.

B34. What are Insertion Attacks ?

The insertion attacks are based on placing unauthorized devices on the wireless network without going through a security process and review.

B35. What is Wireless Sniffer ?

An attacker can sniff and capture legitimate traffic. Many of the sniffer tools for Ethernet are based on capturing the first part of the connection session, where the data would typically include the username and password. An intruder can masquerade as that user by using this captured information. An intruder who monitors the wireless network can apply this same attack principle on the wireless.

B36. What is the difference between Open System and Shared Key of Authentication Type ?**Open System:**

The default authentication service that simply announces the desire to associate with another station or access point. A station can authenticate with any other station or access point using open system authentication if the receiving station designates open system authentication.

Share Key:

The optional authentication that involves a more rigorous exchange of frames, ensuring that the requesting station is authentic. For a station to use shared key authentication, it must implement WEP.

B37. What is 802.1x ?

IEEE 802.1x Port-Based Network Access Control is an IEEE (Institute of Electrical and Electronics Engineers) standard, which specifies a standard mechanism for authenticating, at the link layer (Layer 2), users' access to IEEE 802 networks such as Ethernet (IEEE 802.3) and Wireless LAN (IEEE 802.11). For IEEE 802.11 WLAN, IEEE 802.1x authentication can be based on username/password or digital certificate.

B38. What is AAA ?

AAA is the acronym for Authentication, Authorization, and Accounting and refers to the idea of managing subscribers by controlling their access to the network, verifying that they are who they say they are (via login name and password or MAC address) and accounting for their network usage.

B39. What is RADIUS ?

RADIUS stands for Remote Authentication Dial-In User Service. RADIUS is a standard that has been implemented into several software packages and networking devices. It allows user information to be sent to a central database running on a RADIUS Server, where it is verified. RADIUS also provides a mechanism for accounting.

B40. What is the different between "Enable Intra-BSS Traffic" and "Layer-2 Isolation" ?

Intra-BSS traffic is traffic between wireless stations in the same BSS. When Intra-BSS traffic is enabled, all wireless stations in the same BSS communicate with each other.

When layer-2 isolation is enabled, wireless client, AP, computer or router MAC addresses that are not listed in the "Allow devices with these MAC addresses" table are blocked from communicating with the wireless clients.

When you enable layer-2 isolation, Intra-BSS Traffic is blocked. When you disable layer-2 Isolation, the status of Intra-BSS Traffic is not changed (still blocked).

B41. What is the relationship of security mode between AP and Bridge in AP/Bridge mode?

When you configure the ZyAIR as AP/Bridge mode, the security mode of bridge depends on the security mode of AP.

When the security mode of AP is non-security, the security mode of bridge must be non-security.

When the security mode of AP is 64-bit WEP/128-bit WEP/WPA-PSK/WPA, the security mode of bridge is WPA-PSK.