ZyAIR G-3000H Support Notes

Last Update: July 15, 2005

ZyNOS FAQ

1. 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.

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 ZyAIR in users web browser. To access the ZyAIR's web configurator via web browser, the configuration PC must be in the same IP segment of ZyAIR and ZyAIR must be reachable to the configuration station.

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.

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 ZyAIR will reboot.

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

The ZyAIR allows you to transfer the firmware from/to ZyAIR 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 ZyAIR. 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 ZyAIR.

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

The ZyAIR allows you to transfer the firmware from/to ZyAIR 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 ZyAIR. 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 ZyAIR.

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.

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 ZyAIR.
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 ZyAIR.

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 ZyAIR.
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 ZyAIR.

Product FAQ

General FAQ

1. What is the ZyAIR Wireless Access Point?
2. Which Applications can I use with the ZyAIR?
3. What is the coverage range of ZyAIR?
4. What is the range coverage of B-100/B-200/B-300/B-400?
5. What can I do if I lost the password for my ZyAIRand can't access it's configuration any more?
6. How do I used the reset button, more over what field of parameter will be reset by reset button?
7. Why can't I configure B-100/B-200/B-300 with the supplied utility in Windows XP
8. What is the default user name and password to login the ZyAIR via the browser?
9. How can I manage the ZyAIR?
10. What network interface does the ZyAIR support?
11. What is the maximum number of wireless client can associated with ZyAIR simultaneously?

Advanced FAQ

1. What is the default antenna type and gain on ZyAIR?
2. Can I change the antenna on ZyAIR?
3. What are the connector type required on the replacement antenna?
4. What is the RF power output of ZyAIR?
5. What wireless security mechanism are supported by ZyAIR?
6. What is the difference between Open System and Shared Key of Authentication Type?
7. What authentication type does ZyAIR support?
8. Why is the supplied utility for B-100/B-200/B-300 keep on prompting "Invalid WEP key length" when I try to save my WEP configuration and I am sure the configuration is correct?
9. I have problem associated with ZyAIR with Symol wireless PcMCIA card when WEP is enabled, why?
10. What are 802.1x authentication type and which authentication type does ZyAIR 802.1x embeded server support.
11. How does the ZyAIR support TFTP and FTP?
12. Which 802.1x authentication software client can ZyAIR work with?

1. What is the ZyAIR Wireless Access Point?

The ZyAIR is a wireless access point solution complete with everything needed for providing high speed wireless capability to your existing wired network. The ZyAIR is equipped with 1 auto-MDI/MDIX Ethernet LAN port and a 802.11g wireless LAN interface. It is the simplest and affordable solution for adding wireless mobile capability to your existing wired Ethernet network.

Virtually all-popular applications over Internet, such as Web, E-Mail, FTP, Telnet, Gopher, are supported. The ZyAIR is designed for SOHO, branch offices, workgroups, and educational users.

2. Which Applications can I use with the ZyAIR?

ZyAIR is bridge between wired and wireless network, since bridge is a layer 2 device it can carry all the upper layer protocol in other words it is transparent to all applications.

You can use ZyAIR to add wireless capability to your existing wired network. To access network where wired network are difficult to reach, it can save time and money where frequent change of physical network structure or office relay out are required. Browse the World Wide Web (WWW), send and receive individual e-mail, and download software where you can do task you can do with wired network generally can also be done on wireless network via ZyAIR wireless access point.

3. What is the coverage range of ZyAIR?

The coverage range typically is 50m~80m indoor, 150m~300m outdoor. The actual range may very depends on environment, as to obstacles and walls, RF interference, etc in the environment.

4. What is the range coverage of B-100/B-101/B-200/B-220/B-300/B-400/G-100 client adapter?

The coverage range typically is 50m~80m indoor, 150m~300m outdoor. The actual range may very depends on environment, as to obstacles and walls, RF interference, etc in the environment.

5. What can I do if I lost the password for my ZyAIR and can't access it's configuration any more?

If you have lost the password there is no way to gain access to the device except to reset the device by pressing the reset button located by the power jack.

6. How do I used the reset button? More over what field of parameter will be reset by reset button?

You can used a sharp pointed object insert it into the little reset hole beside the power connector.

The procedures to reset the unit is as follow

1. Used a sharp pointed object insert it into the little reset hole beside the power connector.
2. Press down the reset button and hold down for approx 10 second, the unit will be reset .

Note: When the reset button is pressed all parameters will be reset back to factory default including ESSID, password, IP address, WEP Keys.

The basic default configuration after reset is as follow.

1. IP address default: 192.168.1.2
2. Password default: 1234
3. ESSID default: Wireless
4. WEP:disabled

7. Why can't I configure B-100/B-101/B-200/B-220/B-300/B-400/G-100 client adapter with the supplied utility in Windows XP?

This is because XP uses it’s default configuration for wireless adapter. You can disable it by entering Control Panel->Network and Dialup Connections->Wireless network connection->Advance and uncheck the use Windows to configure wireless configuration check box and click OK. Now you need to exit the supplied configuration utility in the Windows task bar and restart it again. Now you can use the supplied utility to configure your B-100.

8. What is the default user name and password to login the ZyAIR via the browser?

To restrict only the adminstrator can configure the router, there is a login procedure prompted for asking User Name and Password. The default User Name is **'admin'** and the default password is the default SMT password, **'1234'**.

9. How can I manage the ZyAIR?

- Configuration via web browser to the embedded Web Configurator.
- Telnet remote management
- TFTP (Trivial File Transfer Protocol), FTP firmware upgrade and configuration backup and restore.

10. What network interface does the ZyAIR support?

The ZyAIR supports 1 auto MDX/MDIX 10/100M Ethernet interface to connect to your existing wired Ethernet network and 1 802.11g wireless interface to connect to the wireless stations in the coverage range..

11. What is the maximum number of wireless client can associated with ZyAIR simultaneously?

We did not limit the number of wireless client can associated with ZyAIR simultaneously, the suggest number are no more than 32, a good number is under 10 to ensure the performance of each wireless client.

Advanced FAQ

1. What is the default antenna type and gain on ZyAIR?

The ZyAIR are equip with omni directional antenna with 2 dBi Gains.

2. Can I change the antenna on ZyAIR?

Yes, you can change the antenna on ZyAIR to fit your implementation needs. To change antenna you must remove it first. You can remove the antenna by holding the outer ring of the antenna and turn it counter clock wise, and firmly remove the antenna from the ZyAIR. To install it simply reverse the removing procedure.

3. What are the connector type required on the replacement antenna?

ZyAIR are equip with Reverse Polarity SMA jack, so it will work with any 2.4Ghz wireless antenna with Reverse Polarity SMA Plug.

4. What is the RF power output of ZyAIR?

The output power of ZyAIR is 12dBm or 16mW from the RF module.

5. What wireless security mechanism are supported by ZyAIR?

ZyAIR supports below security mechanisms.

1. MAC address filtering.
2. 64bit/128bit WEP (Wired Equivalent Privacy).
3. 802.1x/WPA authentication support.

6. 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.

7. What authentication type does ZyAIR support?

ZyAIR support null authentication when WEP is disabled as specified by IEEE 802.11b/802.11g standard, and when WEP is enabled it is using shared key authentication and data are encrypted at the same time.

8. Why is the supplied utility for B-100/B-101/B-200/B-220/B-300/G-100 keep on prompting "Invalid WEP key length" when I try to save my WEP configuration and I am sure the configuration is correct?

Please make sure all 4 set of keys are with correct and WEP key length are also correct. Do not leave any key field blank.

Note: Please make sure all 4 set of keys are consistent with the 4 set of keys configured in AP.

9. I have problem associated with ZyAIR with Symbol wireless PCMCIA card when WEP is enabled, why?

This is because when WEP is enabled in ZyAIR it is authenticating using Shared key authentication. Symbol PcMCIA client do not support Shared key Authentication. When configuring WEP encryption please ensure open system is selected for authentication method. If you have several wireless NIC card in your network and all are from different vendor please configure the authentication method to 'Auto'. The system will auto detect the authentication method of the station.

10. What are 802.1x authentication type and which authentication type does ZyAIR 802.1x embedded server support.

802.1x specify the following authentication type, and the ZyAIR's embedded 802.1x server only support MD5/CHAP authentication.

1. MD5/CHAP
2. One time password
3. Generic Token Card
4. TLS

5. TTLS
6. LEAP
7. PEAP

11. How does the ZyAIR support TFTP and FTP?

In addition to the direct console port connection, the Prestige supports the uploading/download of the firmware and configuration file using TFTP (Trivial File Transfer Protocol) or FTP over LAN.

12. Which 802.1x authentication software client can ZyAIR work with?

ZyAIR can work with the below test 802.1x authentication software.

For embedded MD5/CHAP authentication server

1. Windows XP embedded 802.1x client (Before SP1 patch).

2. Meetinghouse AEGIS client.

3. Funk Software Odyssey client.

For external TLS authentication server (Odyssey server).

1. Windows XP embedded 802.1x client

2. Funk Software Odyssey client

For external TTLS authentication server (Odyssey server)

1. Funk Software Odyssey client.

Note: 1. XP only support MD5/CHAP and TLS before SP1 patch, after upgrade SP1, XP support only PEAT authentication.

2. When using external server ZyAIR only act as a pass-through thus no extra setting are required.

Wireless FAQ

General FAQ

1. What is a Wireless LAN ?
2. What are the main advantages of Wireless LANs ?
3. What are the disadvantages of Wireless LANs ?
4. Where can you find wireless 802.11 networks ?
5. What is an Access Point ?
6. What is IEEE 802.11 ?
7. What is IEEE 802.11b ?
8. How fast is 802.11b ?
9. What is IEEE 802.11a ?
10. What is IEEE 802.11g ?
11. Is it possible to use products from a variety of vendors ?
12. What is Wi-Fi ?
13. What types of devices use the 2.4GHz Band ?
14. Does Bluetooth interfer with wireless 802.11 LAN ?
15. Can radio signals pass through walls ?
16. What are potential factors that may cause interference among WLAN products ?
17. What's the difference between a WLAN and a WWAN ?

Advanced FAQ

1. What is Ad Hoc mode ?
2. What is Infrastructure mode ?
3. How many Access Points are required in a given area ?
4. What is Direct-Sequence Spread Spectrum Technology – (DSSS) ?
5. What is Frequency-hopping Spread Spectrum Technology – (FHSS) ?
6. Do I need the same kind of antenna on both sides of a link ?
7. Why the 2.4 Ghz Frequency range ?
8. What is Server Set ID (SSID) ?
9. What is an ESSID ?

Security FAQ

Basic FAQ

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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).

9. What is 802.11a ?

802.11a 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.

10. 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 utilize the 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.

11. 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.

12. 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.

13. 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.

14. 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 same2.4-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 interefere. 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.

15. 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.

16. 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.

17. 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.

Advanced FAQ

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

Security FAQ

1. 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.

2. 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.

3. 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.

4. What is a WEP key ?

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

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. What is the difference between force-authorized, force-unauthorized and auto ?

force-authorized—disables 802.1X and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client.

force-unauthorized—causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.

auto—enables 802.1X and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the switch by using the client's MAC address.

13. 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.

14. 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.

15. 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 solation, the status of Intra-BSS Traffic is not changed (still blocked).

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

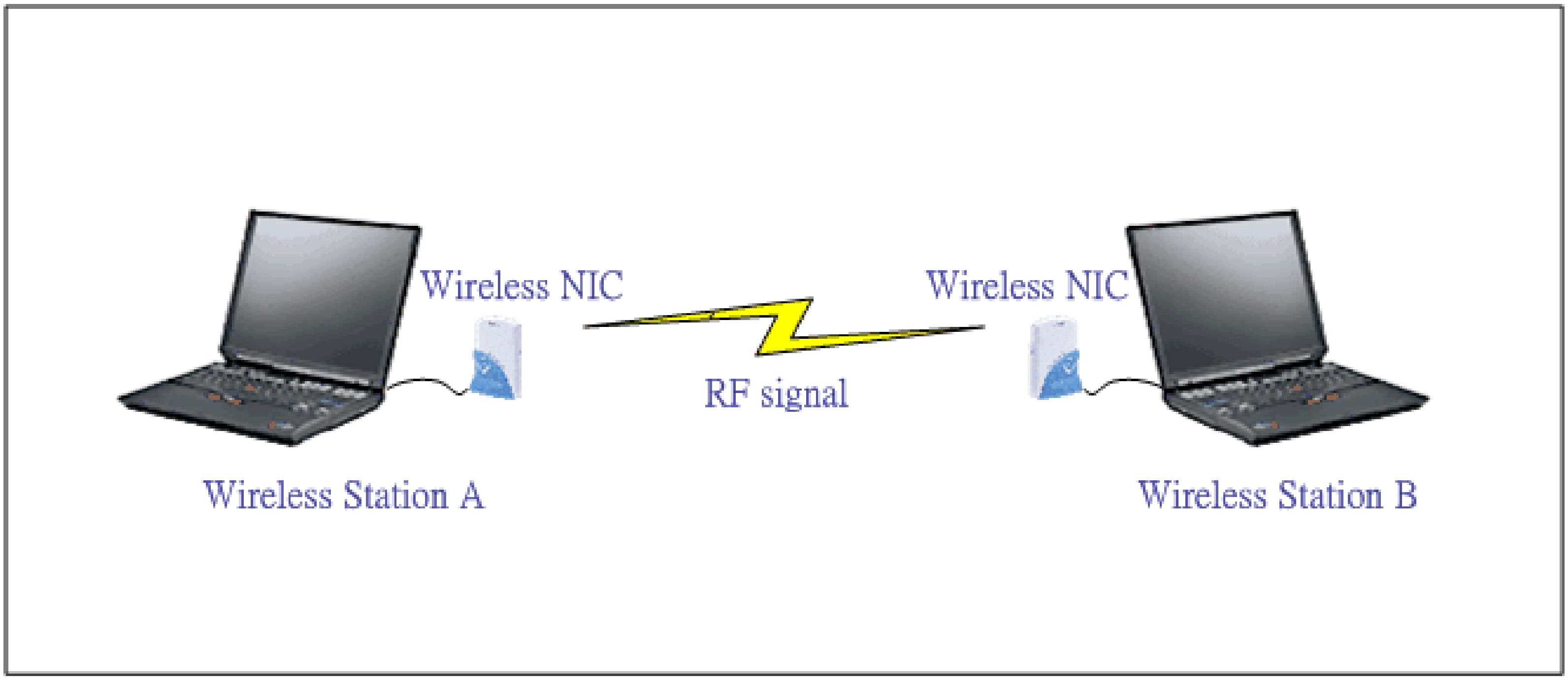
When you config the ZyAIR as AP/Bridge mode, the security mode of bridge depends on the security mode of AP.
When the security mode of AP is non-security, the security mode of bridge must be non-security.
When the security mode of AP is 64-bit WEP/128-bit WEP/WPA-PSK/WPA, the security mode of bridge is WPA-PSK.

Configure a Wireless Client to Ad hoc mode

- ***Introduction***

What is Ad Hoc mode ?
Ad hoc mode is a wireless network consists of a number of stations without access points. Without using an access point or any connection to a wired network.

A client unit in Ad hoc operation mode can communicate directly to other client units just as using a cross over Ethernet cable connecting 2 host together via a NIC card for direct connection when configured in Ad hoc mode without an access point being present. Ad hoc operation is ideal for small networks of no more than 2-4 computers. Larger networks would require the use of one, or perhaps several, access points.

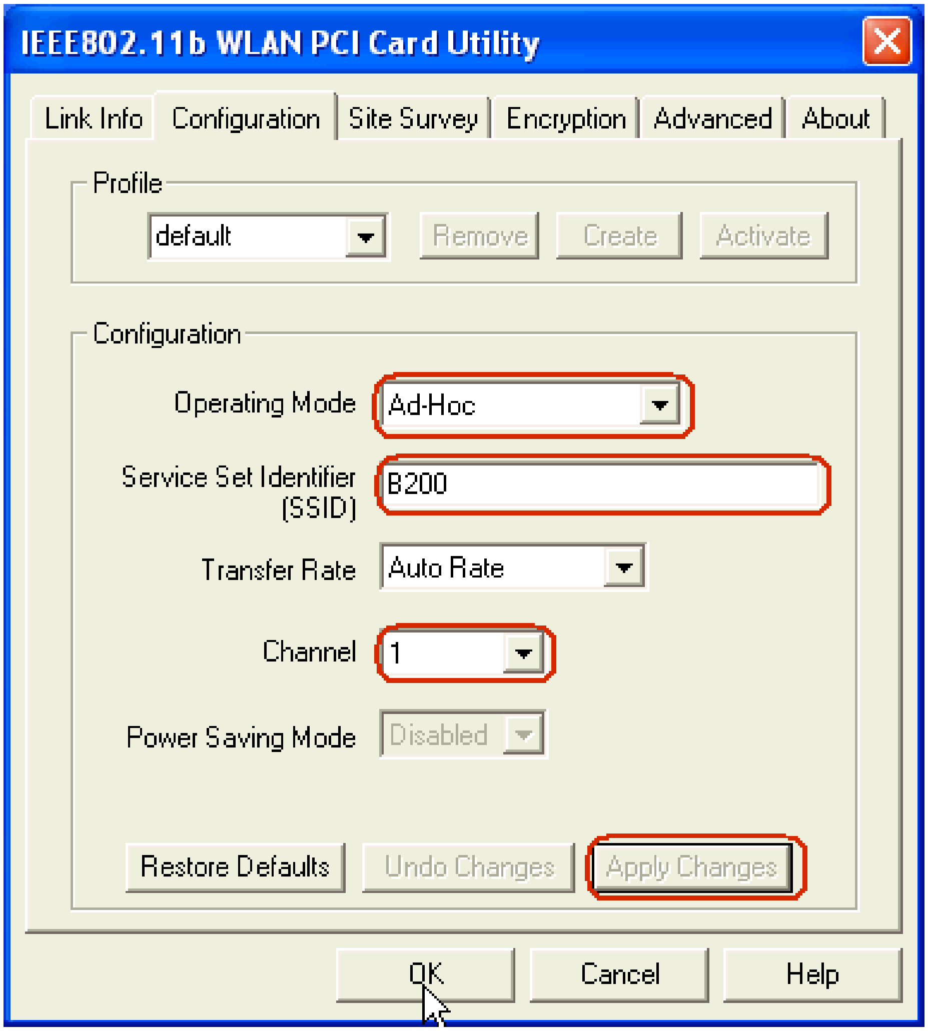


- ***Configuration for Wireless Station A***

To configure Ad hoc mode on your ZyAIR B-100/B-200/B-300 wireless NIC card please follow the following step.

1. Double click on the utility icon in your windows task bar the utility will pop up on your windows screen.

2. Select configuration tab.



IEEE802.11b WLAN PCI Card Utility

Profile: default

Operating Mode: Ad-Hoc

Service Set Identifier (SSID): B200

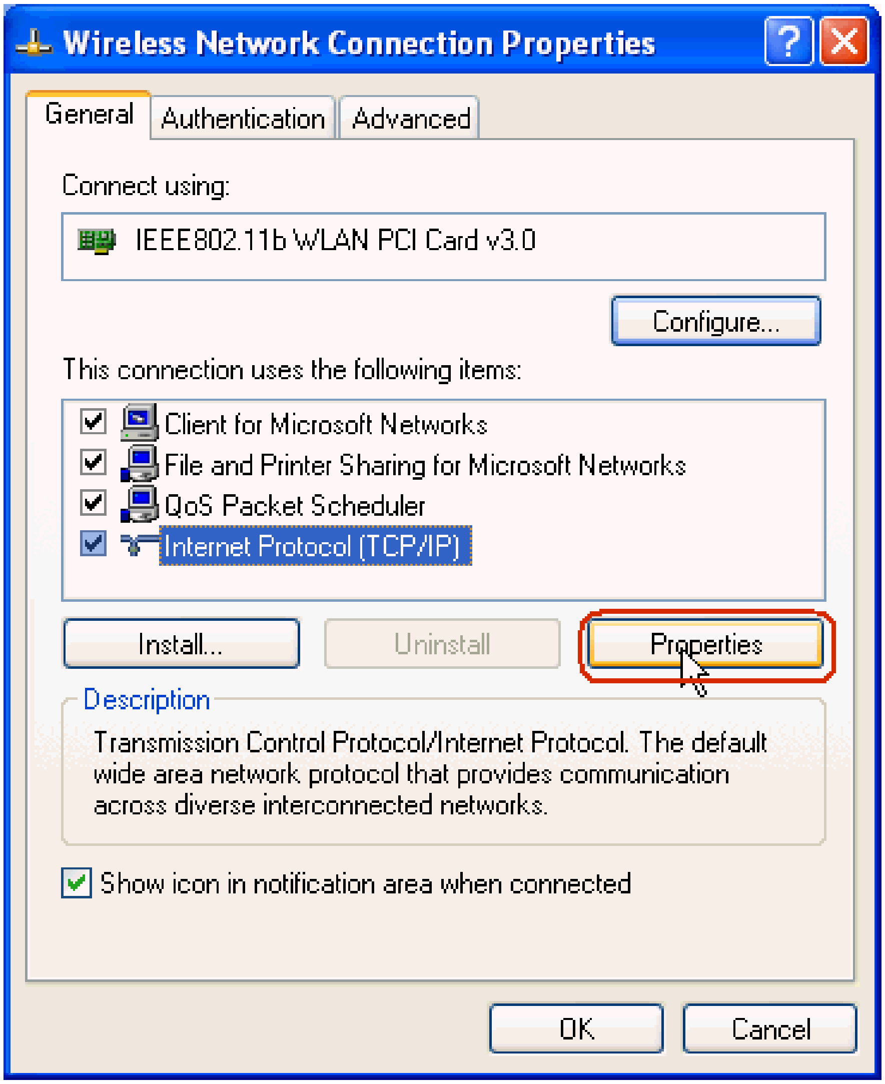
Transfer Rate: Auto Rate

Channel: 1

Power Saving Mode: Disabled

3. Select Ad hoc from the operation mode pull down menu, fill you an SSID and select a channel you want to use than press OK to apply.

4. Since there is no DHCP server to give the host IP you must first designate a static IP for your station. From Windows Start select Control Panel >Network Connection>Wireless Network Connection.



Connect using:

IEEE802.11b WLAN PCI Card v3.0

This connection uses the following items:

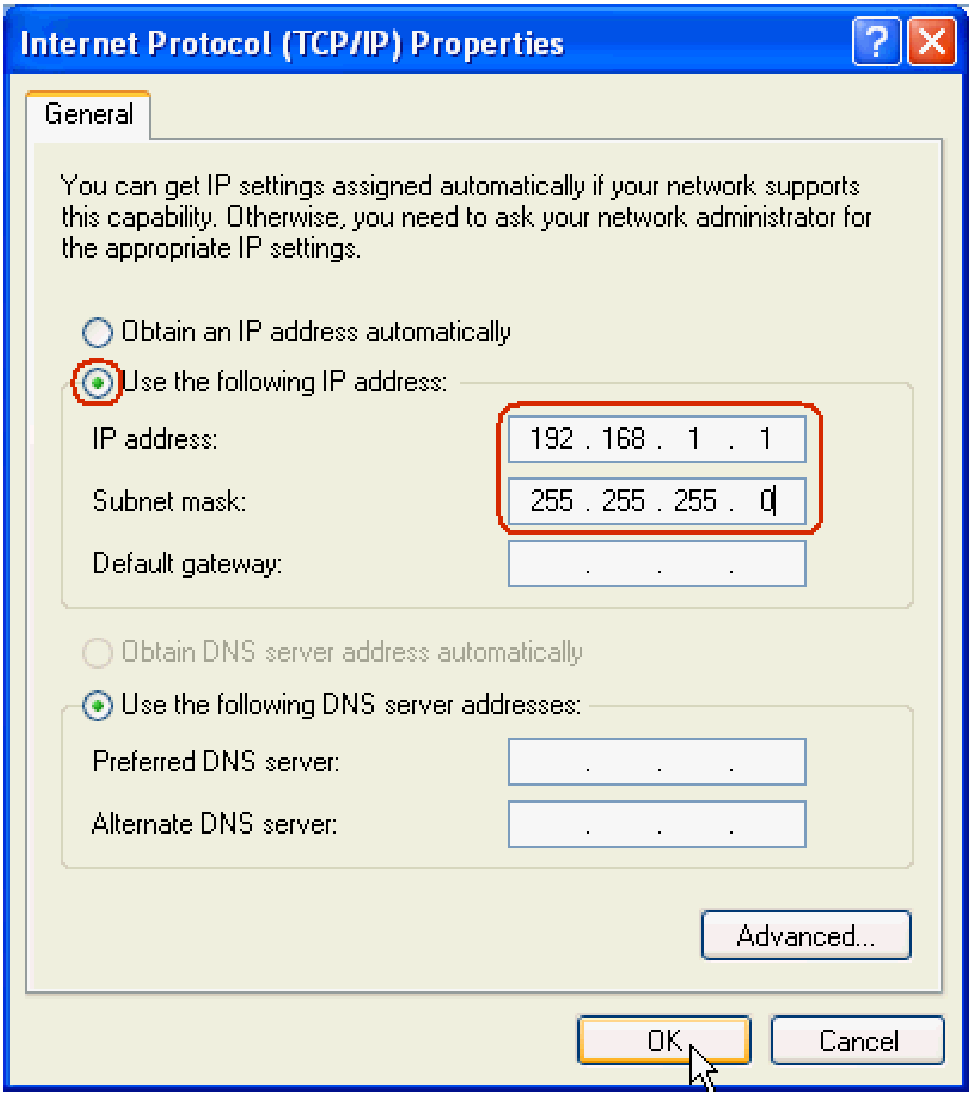
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

5. From general tab select TCP/IP and click property



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

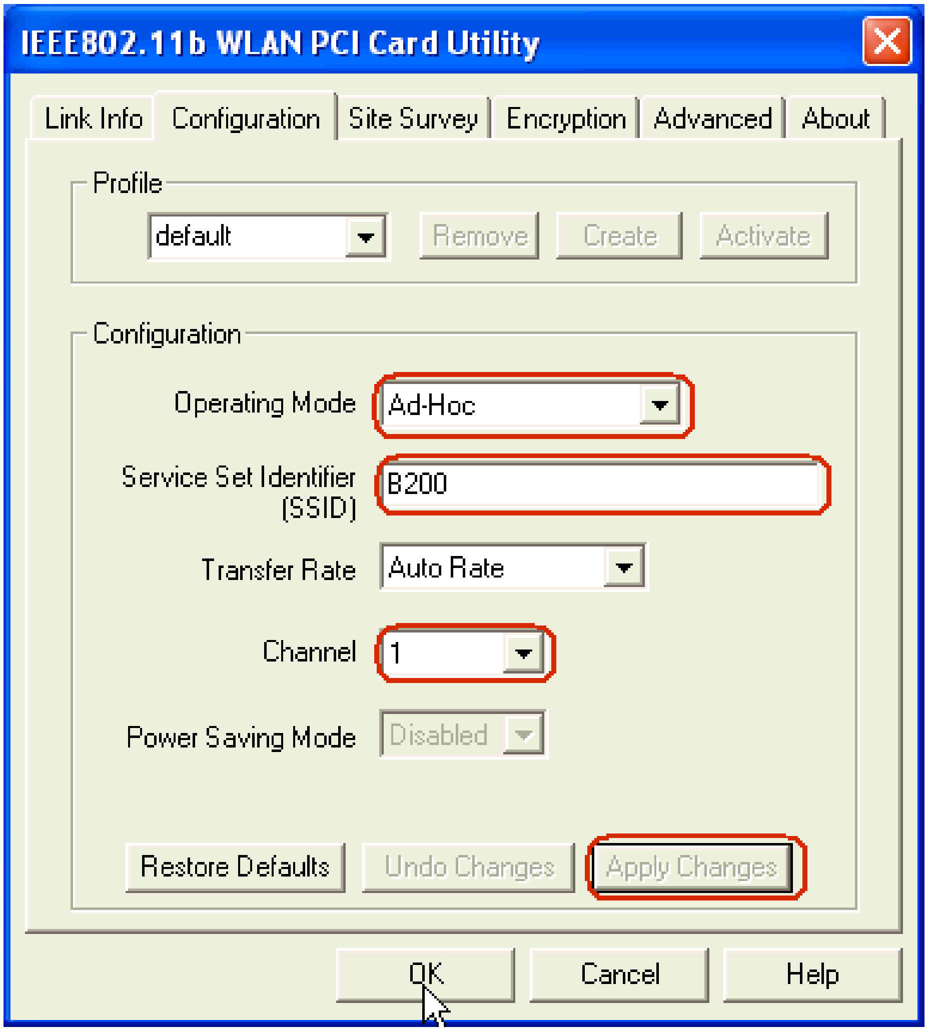
6. Fill in your network IP address and subnet mask and click OK to finish.

- ***Configuration for Wireless Station B***

To configure Ad hoc mode on your ZyAIR B-100/B-200/B-300 wireless NIC card please follow the following step.

1. Double click on the utility icon in your windows task bar the utility will pop up on your windows screen.

2. Select configuration tab.



IEEE802.11b WLAN PCI Card Utility

Profile: default

Configuration

Operating Mode: Ad-Hoc

Service Set Identifier (SSID): B200

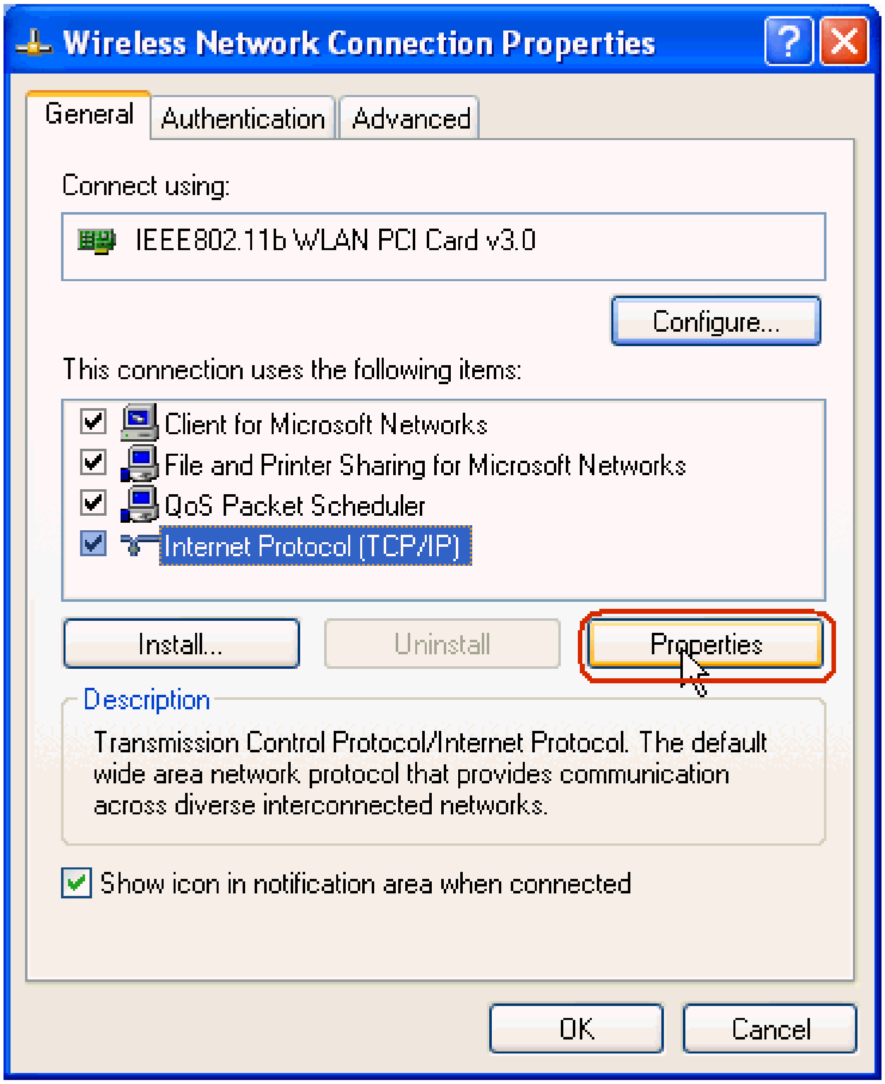
Transfer Rate: Auto Rate

Channel: 1

Power Saving Mode: Disabled

3. Select Ad hoc from the operation mode pull down menu, fill you an SSID and select a channel you want to use than press OK to apply.

4. Since there is no DHCP server to give the host IP you must first designate a static IP for your station. From Windows Start select Control Panel >Network Connection>Wireless Network Connection.



Wireless Network Connection Properties

General | Authentication | Advanced

Connect using:

IEEE802.11b WLAN PCI Card v3.0

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

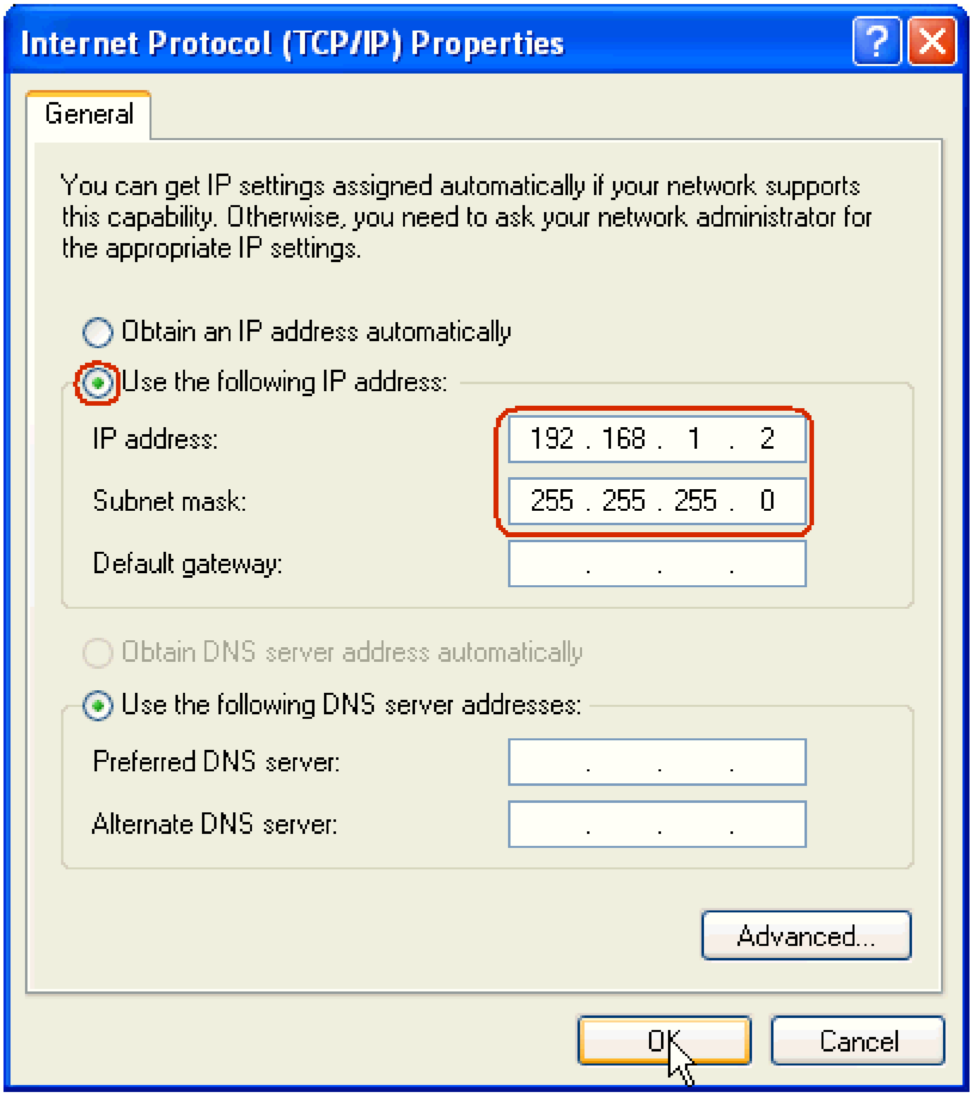
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

OK | Cancel

5. From general tab select TCP/IP and click property



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

6. Fill in your network IP address and subnet mask and click OK to finish.

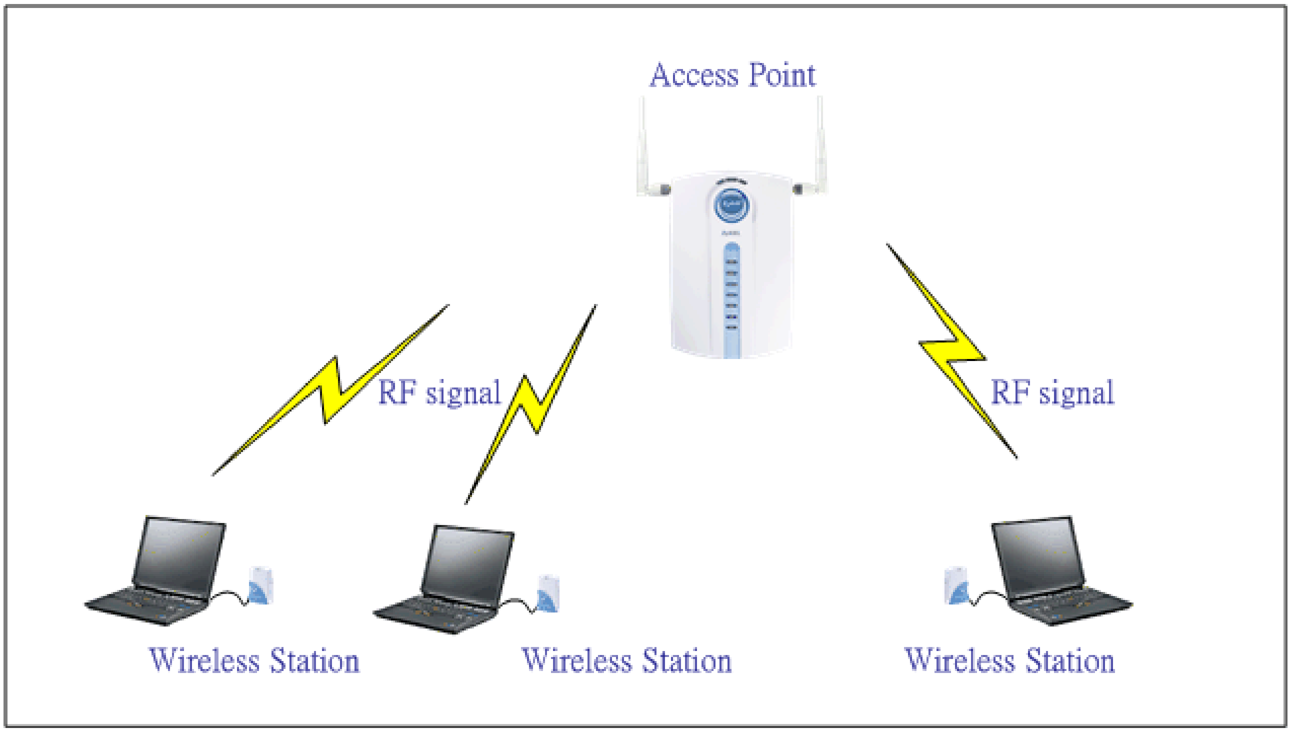
7. Station A now are able to connect to Station B.

Configuring Infrastructure mode

- Introduction

What is Infrastructure mode ?

Infrastructure mode, sometimes referred to as Access Point mode, is an operating mode of an 802.11b/Wi-Fi client unit. In infrastructure mode, the client unit can associate with an 802.11b/Wi-Fi Access Point and communicate with other clients in infrastructure mode through that access point.



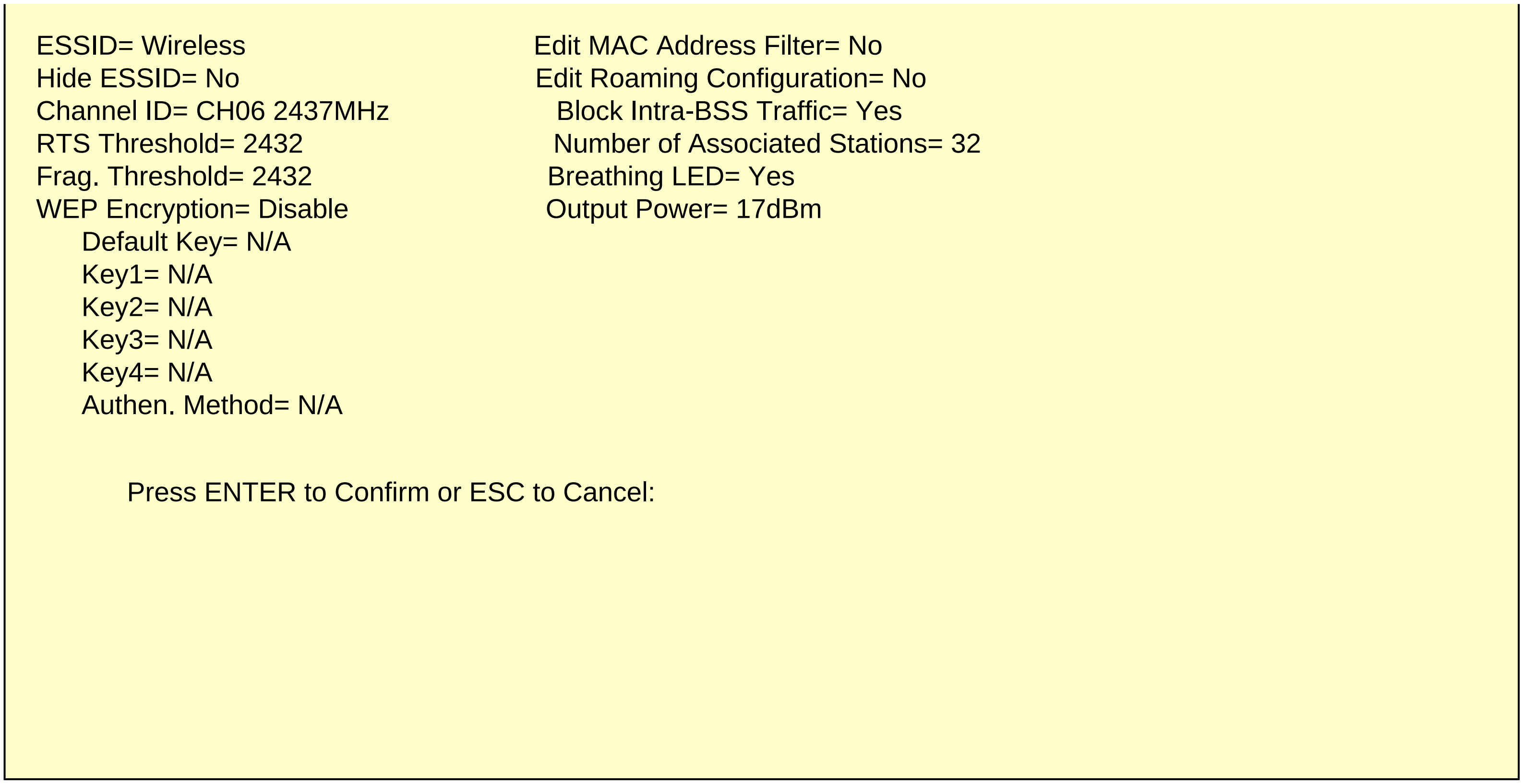
Configuration Wireless Access Point to Infrastructure mode using SMT.

To configure Infrastructure mode of your ZyAIR wireless AP please follow the steps below.

1. From the SMT main menu, enter 3 to display Menu 3 – LAN Setup.

2. Enter 5 to display Menu 3.5 – Wireless LAN Setup.

```
                    Menu 3.5 - Wireless LAN Setup
```



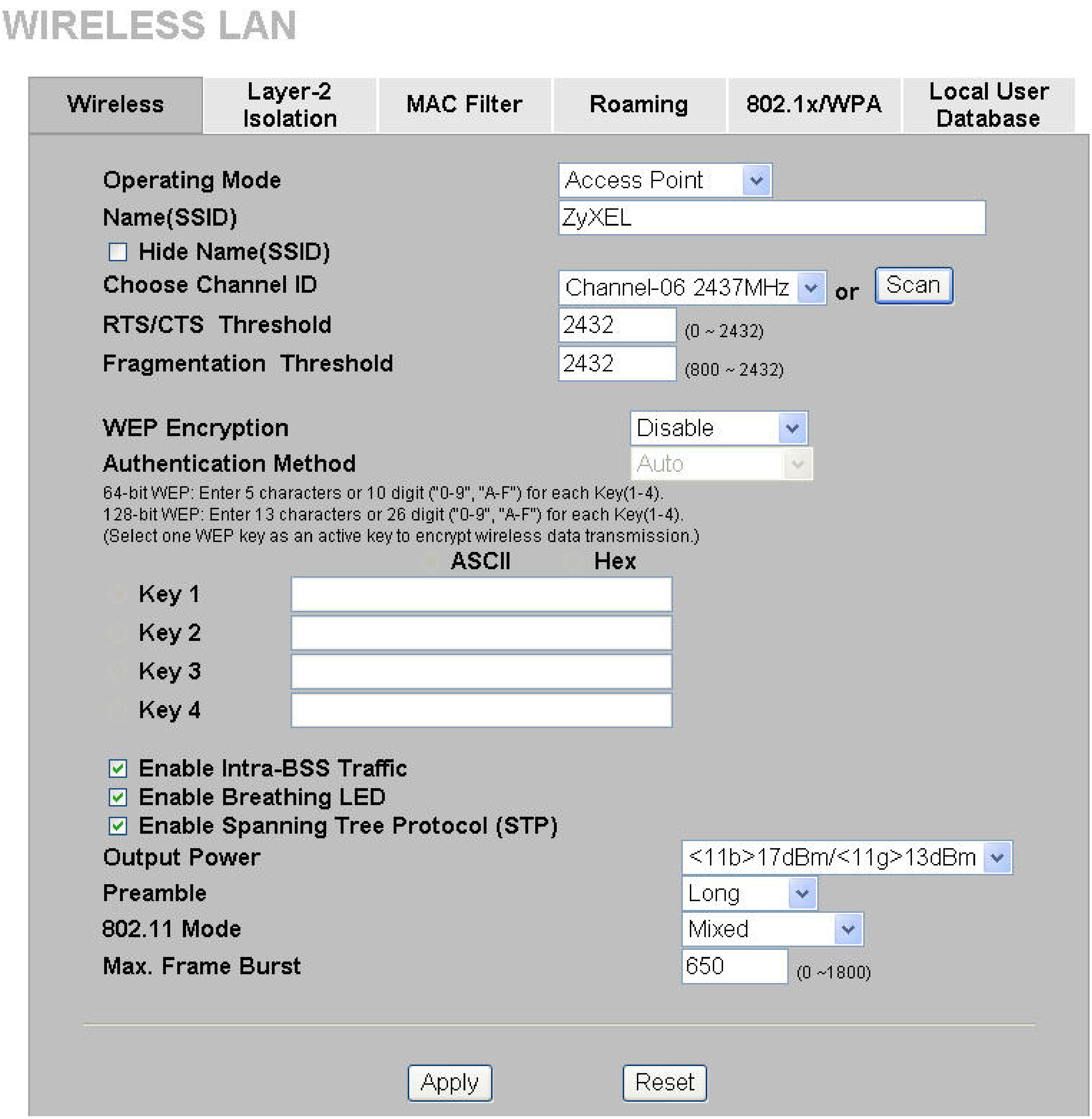
```
ESSID= Wireless                         Edit MAC Address Filter= No
Hide ESSID= No                          Edit Roaming Configuration= No
Channel ID= CH06 2437MHz                  Block Intra-BSS Traffic= Yes
RTS Threshold= 2432                       Number of Associated Stations= 32
Frag. Threshold= 2432                    Breathing LED= Yes
WEP Encryption= Disable                  Output Power= 17dBm
    Default Key= N/A
    Key1= N/A
    Key2= N/A
    Key3= N/A
    Key4= N/A
    Authen. Method= N/A


        Press ENTER to Confirm or ESC to Cancel:
```

3. Configure ESSID, Channel ID, WEP, Default Key and Keys as you desire.

Configuration Wireless Access Point to Infrastructure mode using Web configurator.

To configure Infrastructure mode of your ZyAIR wireless AP please follow the steps below.

1. From the web configurator main menu, click advanced->wireless to display – Wireless LAN.



WIRELESS LAN

Operating Mode: Access Point

Name(SSID): ZyXEL

□ Hide Name(SSID)

Choose Channel ID: Channel-06 2437MHz or Scan

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (800 ~ 2432)

WEP Encryption: Disable

Authentication Method: Auto

64-bit WEP: Enter 5 characters or 10 digit ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 characters or 26 digit ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

○ ASCII ○ Hex

○ Key 1
○ Key 2
○ Key 3
○ Key 4

☑ Enable Intra-BSS Traffic
☑ Enable Breathing LED
☑ Enable Spanning Tree Protocol (STP)

Output Power: <11b>17dBm/<11g>13dBm

Preamble: Long

802.11 Mode: Mixed

Max. Frame Burst: 650 (0 ~1800)

3. Configure the desired configuation on ZyAIR.

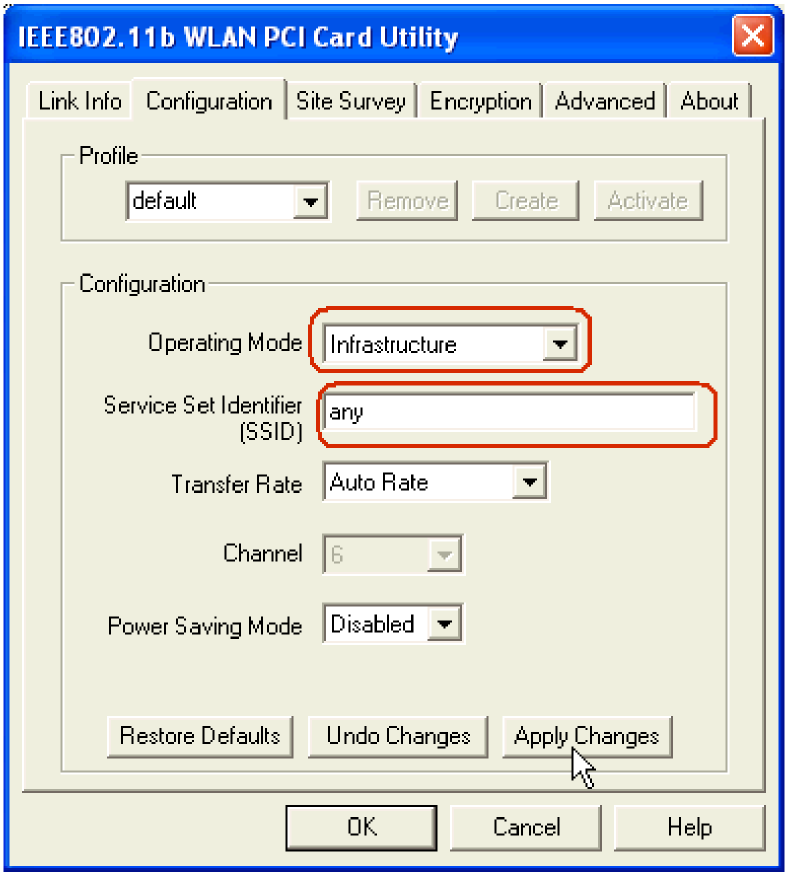
4. Finished.

- Configuration Wireless Station to Infrastructure mode

To configure Infrastructure mode on your ZyAIR B-100/B-200/B-300 wireless NIC card please follow the following steps.

1. Double click on the utility icon in your windows task bar the utility will pop up on your windows screen.

2. Select configuration tab.



Profile

default

Configuration

Operating Mode: Infrastructure

Service Set Identifier (SSID): any

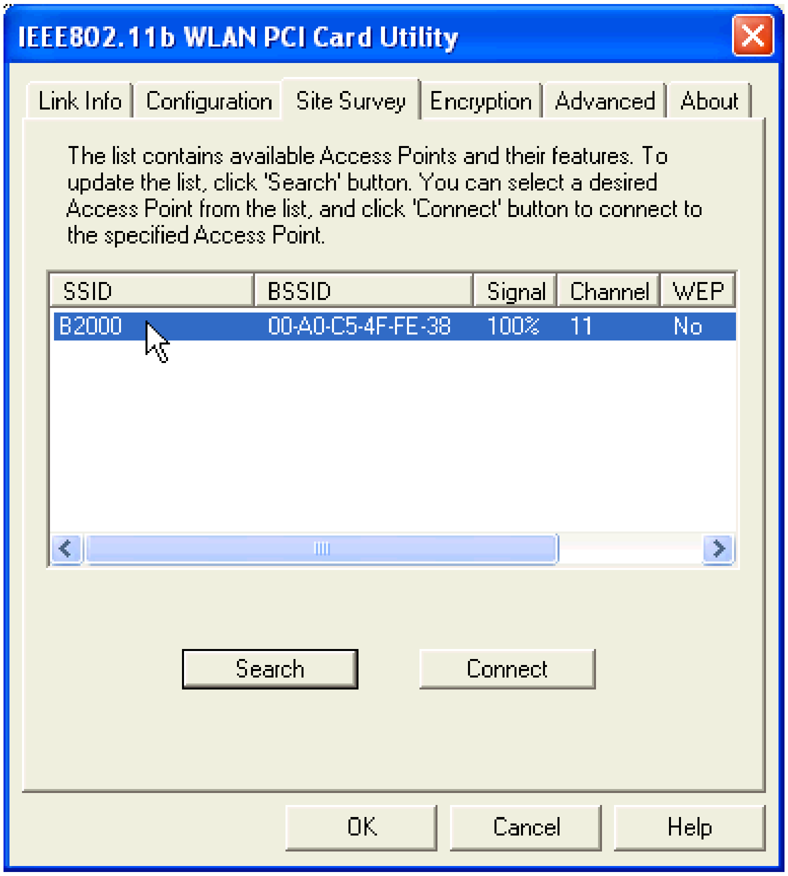
Transfer Rate: Auto Rate

Channel: 6

Power Saving Mode: Disabled

3. Select Infrastructure from the operation mode pull down menu, fill in an SSID or leave it as any if you wish to connect to any AP than press Apply Change to take effect.

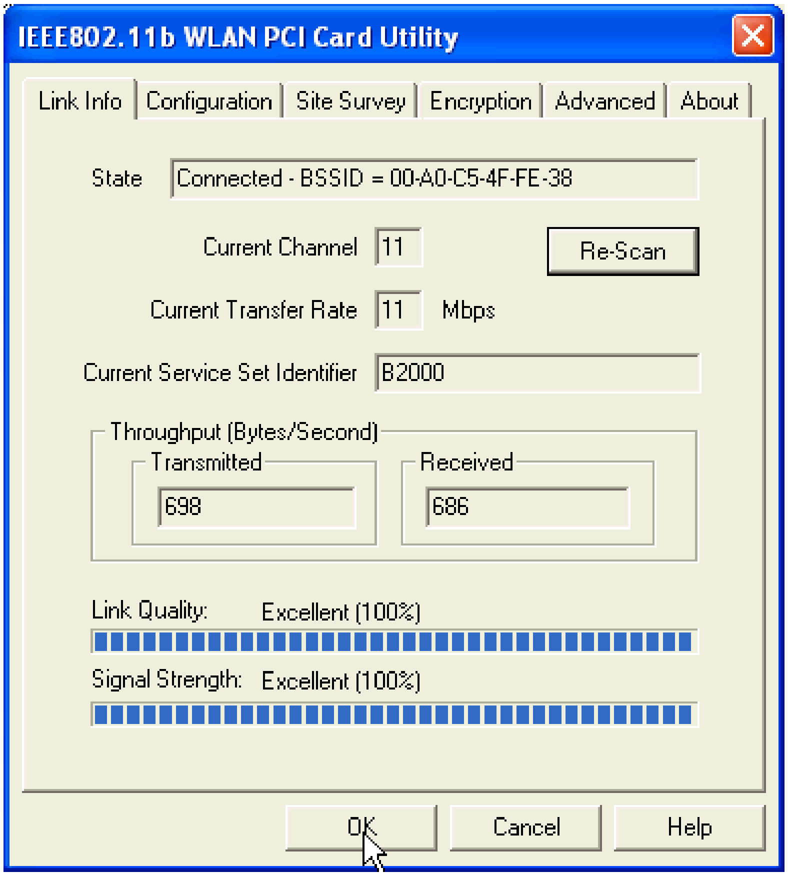
4. Click on Site Survey tab, and press search all the available AP will be listed.



The list contains available Access Points and their features. To update the list, click 'Search' button. You can select a desired Access Point from the list, and click 'Connect' button to connect to the specified Access Point.

SSID	BSSID	Signal	Channel	WEP
B2000	00-A0-C5-4F-FE-38	100%	11	No

5. Double click on the AP you want to associated with.



State: Connected - BSSID = 00-A0-C5-4F-FE-38

Current Channel: 11

Current Transfer Rate: 11 Mbps

Current Service Set Identifier: B2000

Throughput (Bytes/Second)

Transmitted: 698

Received: 686

Link Quality: Excellent (100%)

Signal Strength: Excellent (100%)

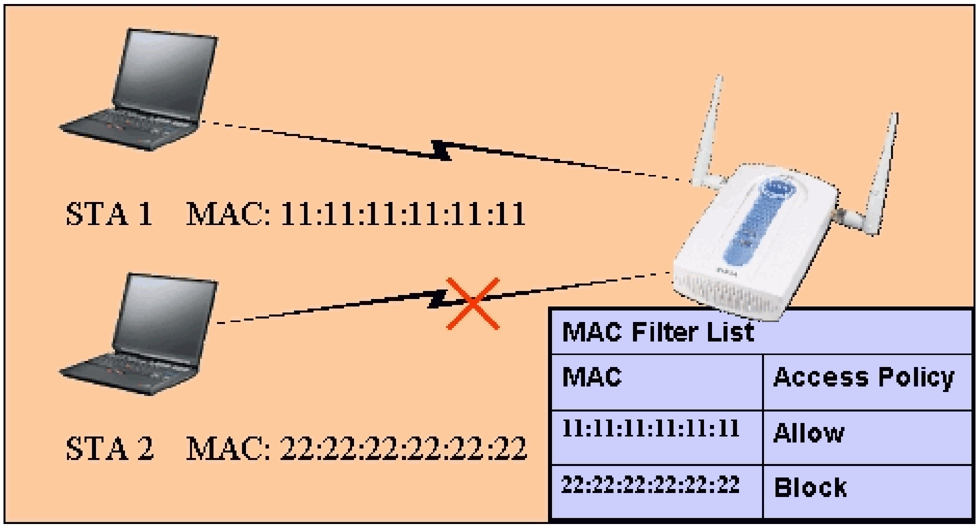
6. After the client have associated with the selected AP. The linked AP's channel, current linkup rate, SSID, link quality, and signal strength will show on the Link Info page. You now successfully associate with the selected AP with Infrastructure

Mode.

MAC Filter

1. MAC Filter Overview

Users can use MAC Filter as a method to restrict unauthorized stations from accessing the APs. ZyXEL's APs provide the capability for checking MAC address of the station before allowing it to connect to the network. This provides an additional layer of control layer in that only stations with registered MAC addresses can connect. This approach requires that the list of MAC addresses be configured.



MAC Filter List

MAC	Access Policy
11:11:11:11:11:11	Allow
22:22:22:22:22:22	Block

2. ZyXEL MAC Filter Implementation

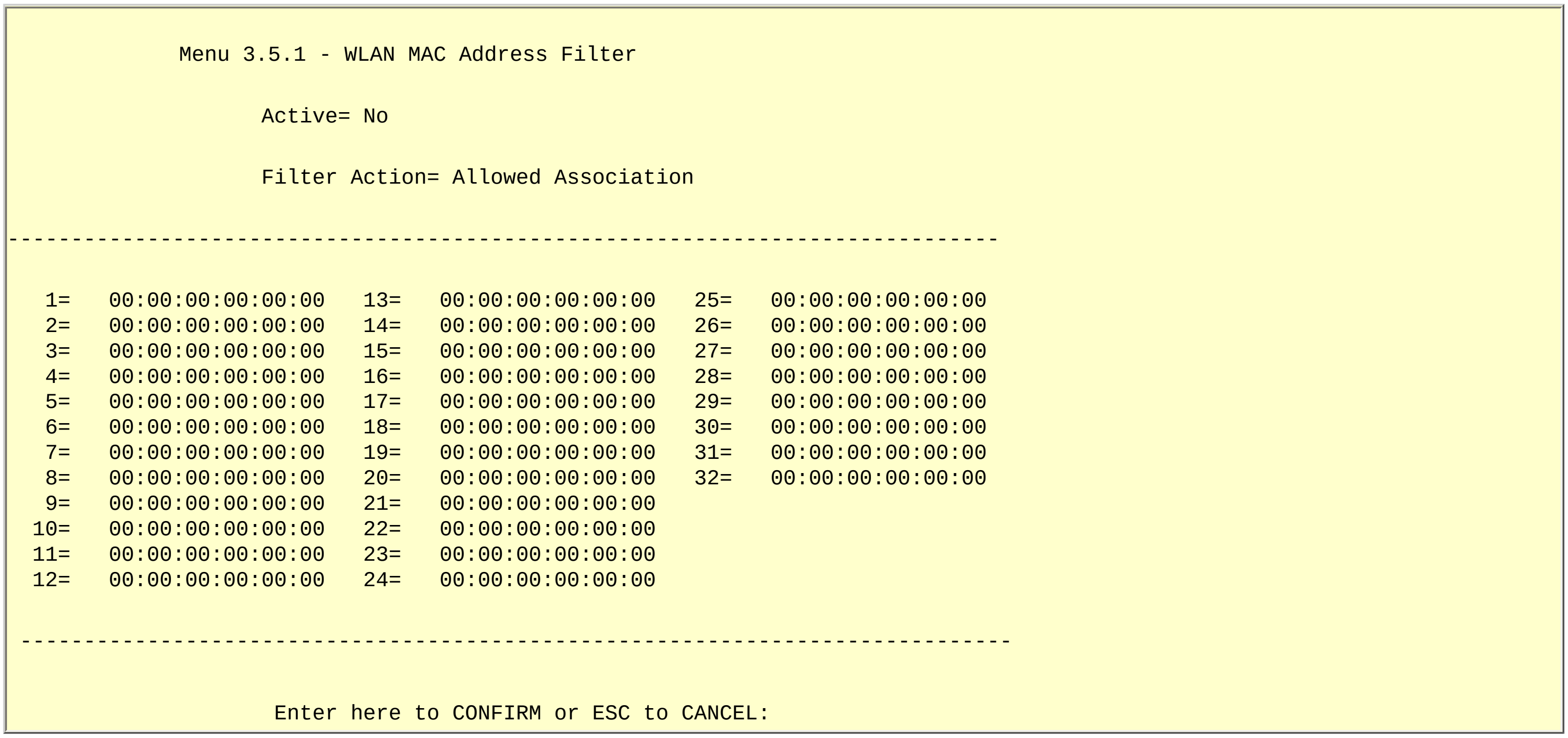
ZyXEL's MAC Filter Implementation allows users to define a list to allow or block association from STAs. The filter set allows users to input 12 entries in the list. If Allow Association is selected, all other STAs which are not on the list will be denied. Otherwise, if Deny Association is selected, all other STAs which are not on the list will be allowed for association. Users can choose either way to configure their filter rule.

3. Configure the WLAN MAC Filter

The MAC Filter related settings in ZyXEL APs are configured in menu 3.5.1, WLAN MAC Address Filter Configuration. Before you configure the MAC filter, you need to know the MAC address of the client first. If not knowing what your MAC address is, please enter a command "ipconfig /all" after DOS prompt to get the MAC (physical) address of your wireless client.

If you use SMT management, the MAC Address Filter configuration are as shown below.

Enter the MAC Addresses of wireless cards in the filter set to allow or deny association from these cards.



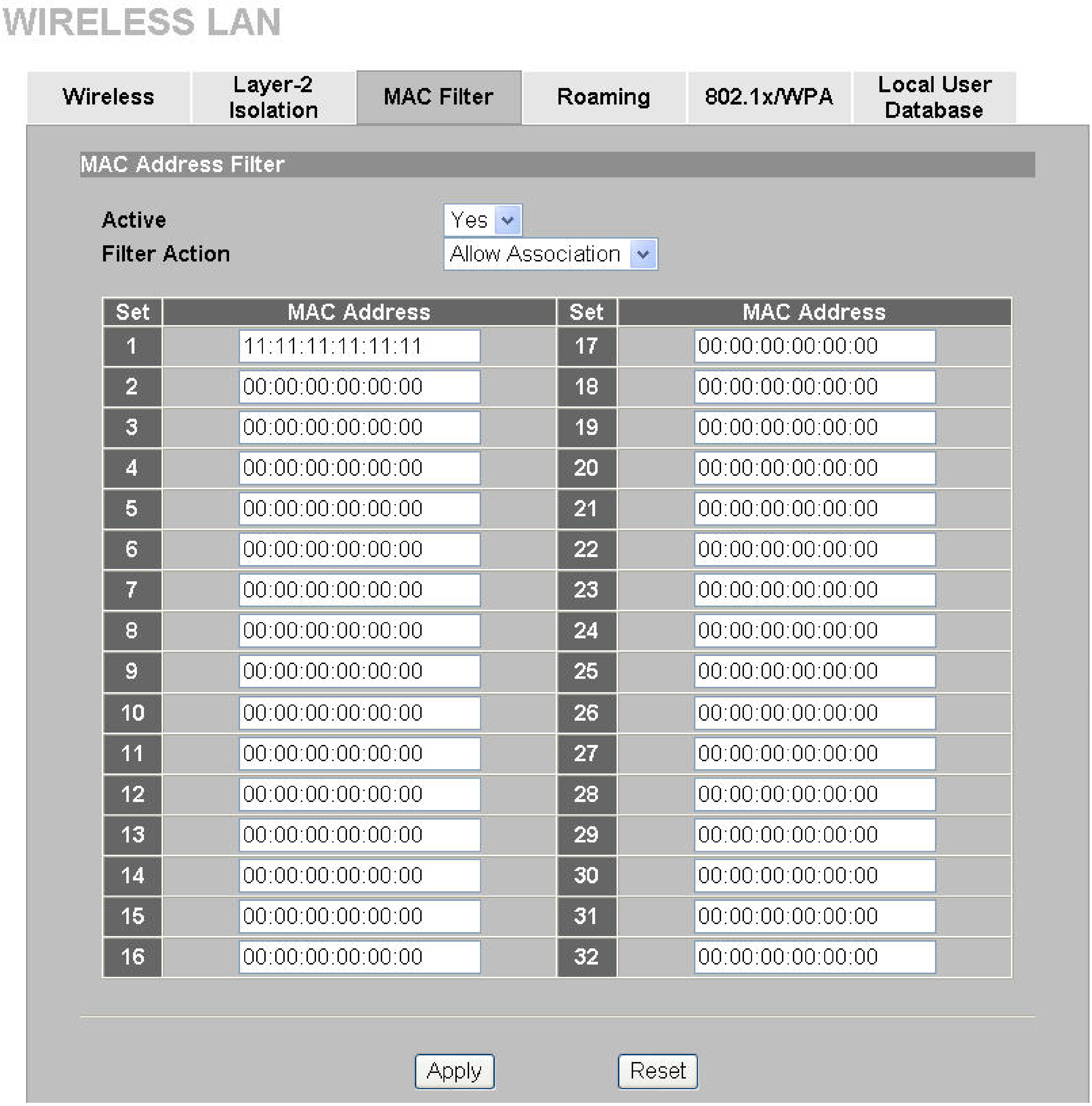
```
             Menu 3.5.1 - WLAN MAC Address Filter

                    Active= No

                    Filter Action= Allowed Association

------------------------------------------------------------------------------

   1=   00:00:00:00:00:00   13=   00:00:00:00:00:00   25=   00:00:00:00:00:00
   2=   00:00:00:00:00:00   14=   00:00:00:00:00:00   26=   00:00:00:00:00:00
   3=   00:00:00:00:00:00   15=   00:00:00:00:00:00   27=   00:00:00:00:00:00
   4=   00:00:00:00:00:00   16=   00:00:00:00:00:00   28=   00:00:00:00:00:00
   5=   00:00:00:00:00:00   17=   00:00:00:00:00:00   29=   00:00:00:00:00:00
   6=   00:00:00:00:00:00   18=   00:00:00:00:00:00   30=   00:00:00:00:00:00
   7=   00:00:00:00:00:00   19=   00:00:00:00:00:00   31=   00:00:00:00:00:00
   8=   00:00:00:00:00:00   20=   00:00:00:00:00:00   32=   00:00:00:00:00:00
   9=   00:00:00:00:00:00   21=   00:00:00:00:00:00
  10=   00:00:00:00:00:00   22=   00:00:00:00:00:00
  11=   00:00:00:00:00:00   23=   00:00:00:00:00:00
  12=   00:00:00:00:00:00   24=   00:00:00:00:00:00

 ------------------------------------------------------------------------------

                     Enter here to CONFIRM or ESC to CANCEL:
```

Key Settings:

Option	Descriptions
Filter Action	Allow or block association from MAC addresses contained in this list. If Allow Association is selected in this field, hosts with MAC addresses configured in this list will be allowed to associate with AP. If Deny Association is selected in this field, hosts with MAC addresses configured in this list will be blocked.
MAC Address	This field specifies those MAC Addresses that you want to add in the list.

If you use WEB configuration, the MAC Address Filter configuration are as shown below.

1. Using a web browser, login AP by giving the LAN IP address of AP in URL field. Default LAN IP is 192.168.1.1, default password to login web configurator is 1234.
2. Click Advanced, and click Wireless tab on the left.
3. Click MAC Filter tab on the top and select Yes in the Active field to enable MAC Filter.
4. Select the Filter Action to allow or deny association from hosts in the list.
5. Enter the MAC Addresses which you may want to apply the filter to allow or block associations from.
6. Click Apply to make your setting work.



MAC Address Filter

Active: Yes

Filter Action: Allow Association

Set	MAC Address	Set	MAC Address
1	11:11:11:11:11:11	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
4	00:00:00:00:00:00	20	00:00:00:00:00:00
5	00:00:00:00:00:00	21	00:00:00:00:00:00
6	00:00:00:00:00:00	22	00:00:00:00:00:00
7	00:00:00:00:00:00	23	00:00:00:00:00:00
8	00:00:00:00:00:00	24	00:00:00:00:00:00
9	00:00:00:00:00:00	25	00:00:00:00:00:00
10	00:00:00:00:00:00	26	00:00:00:00:00:00
11	00:00:00:00:00:00	27	00:00:00:00:00:00
12	00:00:00:00:00:00	28	00:00:00:00:00:00
13	00:00:00:00:00:00	29	00:00:00:00:00:00
14	00:00:00:00:00:00	30	00:00:00:00:00:00
15	00:00:00:00:00:00	31	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

Setup WEP (Wired Equivalent Privacy)

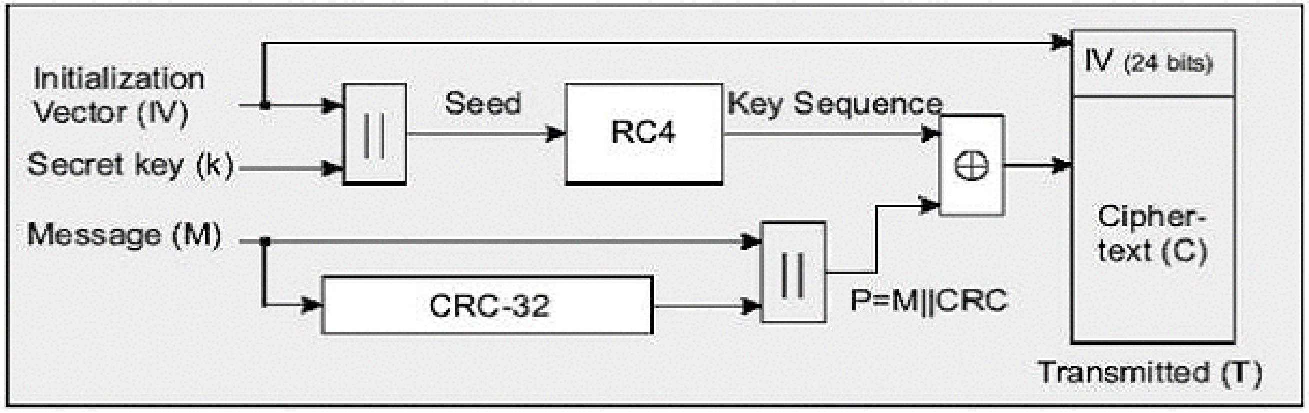
Introduction

The 802.11 standard describes the communication that occurs in wireless LANs.

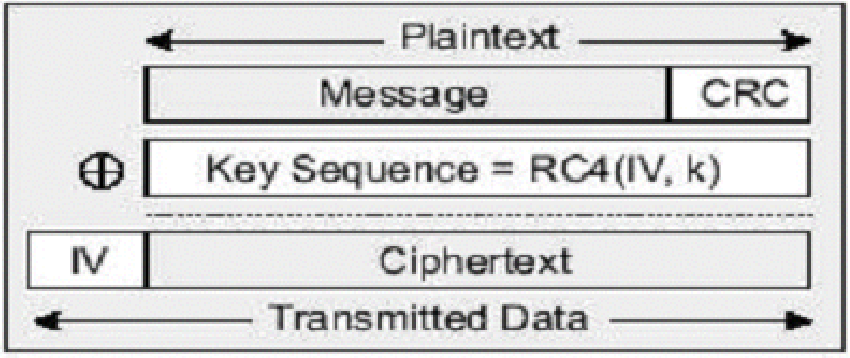
The Wired Equivalent Privacy (WEP) algorithm is used to protect wireless communication from eavesdropping, because wireless transmissions are easier to intercept than transmissions over wired networks, and wireless is a shared medium, everything that is transmitted or received over a wireless network can be intercepted.

WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packages are not modified during the transition. The standard does not discuss how the shared key is established. In practice, most installations use a single key that is shared between all mobile stations and access points APs.

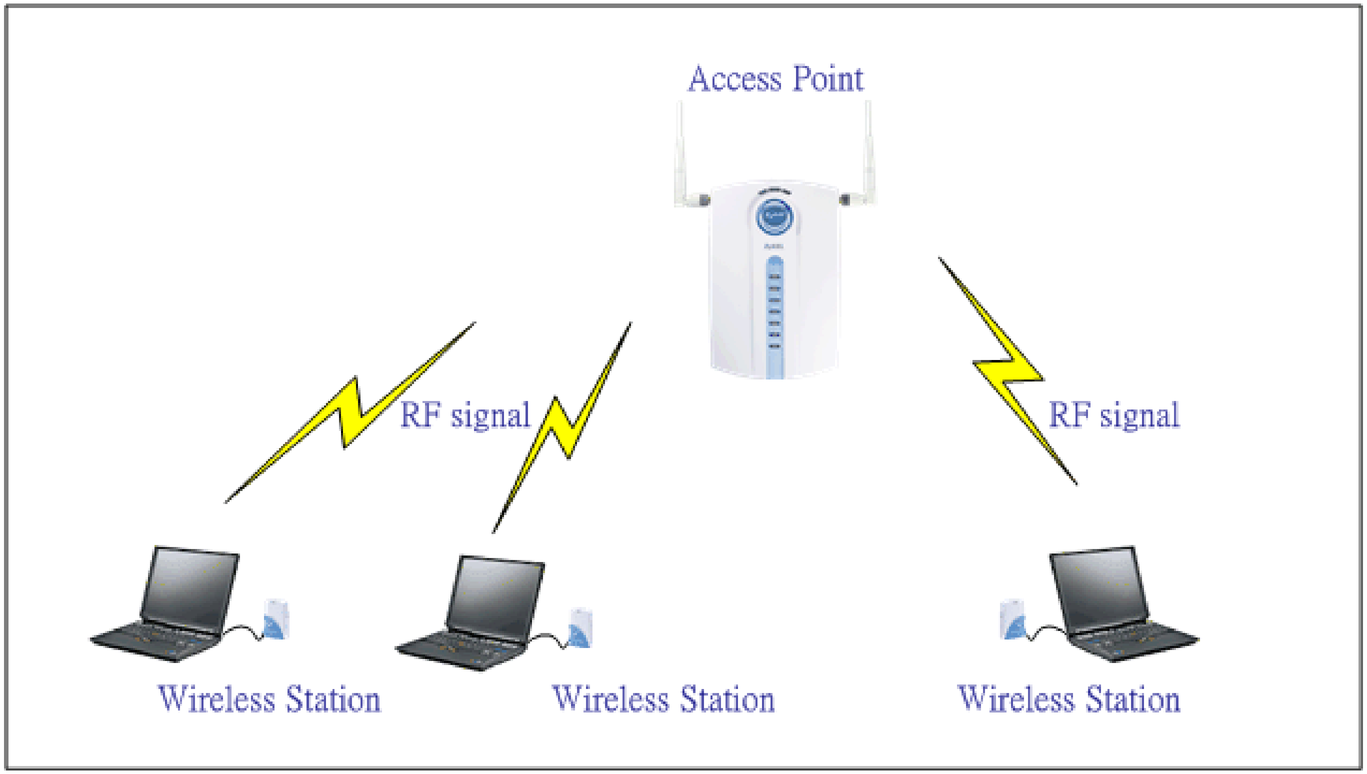
WEP employs the key encryption algorithm, Ron's Code 4 Pseudo Random Number Generator (RC4 PRNG). The same key is used to encrypt and decrypt the data.



WEP has defences against this attack. To avoid encrypting two cipher texts with the same key stream, an Initialisation Vector (IV) is used to augment the shared WEP key (secret key) and produce a different RC4 key for each packet, the IV is also included in the package. WEP key (secret key) are available in two types, 64-bits and 128-bits. Many times you will see them referenced as 40-bits and 104-bits instead. The reson for this misnomer is that the WEP key (40/104 bits) is concatenated with the initialisation vector (24 bits) resulting in a 64/128 bit total key size.



Setting up the Access Point



Most access points and clients have the ability to hold up to 4 WEP keys simultaneously. You need to specify one of the 4 keys as default Key for data encryption. To set up the Access Point, you will need to set the one of the following parameters:

- 64-bit WEP key (secret key) with 5 characters
- 64-bit WEP key (secret key) with 10 hexadecimal digits
- 128-bit WEP key (secret key) with 13 characters
- 128-bit WEP key (secret key) with 26 hexadecimal digits

You can set up the Access Point by SMT or Web configurator

- Setting up the Access Point from SMT Menu 3.5

The ZyAIR hold up to 4 WEP Keys. You have to specify one of the 4 keys as default Key which be used to encrypt wireless data transmission. For example,

```
                       Menu 3.5 - Wireless LAN Setup

     Operaing Mode= Access Point       Edit MAC Address Filter= No
     ESSID= Wireless                     Edit Roaming Configuration= No
     Hide ESSID= No                      Edit Multiple ESS Configuration= N/A
     Channel ID= CH06 2412MHz          Edit Bridge Link Configuration= N/A
     RTS Threshold= 2432                Block Intra-BSS Traffic= No
     Frag. Threshold= 2432             Number of Associated Stations= 32
     WEP Encryption= 64-bit WEP         Breathing LED= Yes

       Default Key= 3                   Output Power= 17dBm
       Key1= lkasd
       Key2= oueww
       Key3= wopek
       Key4= woppe
       Authen. Method= N/A

                    Press ENTER to Confirm or ESC to Cancel:
```

Key settings

Hexadecimal digits have to preceded by '**0x**',

WEP Key type	Example

64-bit WEP with 5 characters	Key1= 2e3f4
	Key2= 5y7js
	Key3= 24fg7
	Key4= 98jui

64-bit WEP with 10 hexadecimal digits ('0-9', 'A-F')	Key1= **0x**123456789A
	Key2= **0x**23456789AB
	Key3= **0x**3456789ABC
	Key4= **0x**456789ABCD

128-bit WEP with 13 characters	Key1= 2e3f4w345ytre
	Key2= 5y7jse8r4i038
	Key3= 24fg70okx3fr7
	Key4= 98jui2wss35u4

128-bit WEP with 26 hexadecimal digits ('0-9', 'A-F')	Key1= **0x**112233445566778899AABBCDEF
	Key2= **0x**2233445566778899AABBCCDDEE
	Key3= **0x**3344556677889900AABBCCDDFF
	Key4= **0x**44556677889900AABBCCDDEEFF

Select one of the WEP key as default Key to encrypt wireless data transmission.
The receiver will use the corresponding key to decrypt the data.

For example, if access point use Key 3 to encrypt data, then station will use Key 3 to decrypt data.
So, the Key 3 of station has to equal to the Key 3 of access point.
Though access point use Key 3 as default key, but the station can use the other Key as its default key to encrypt wireless data transmission.

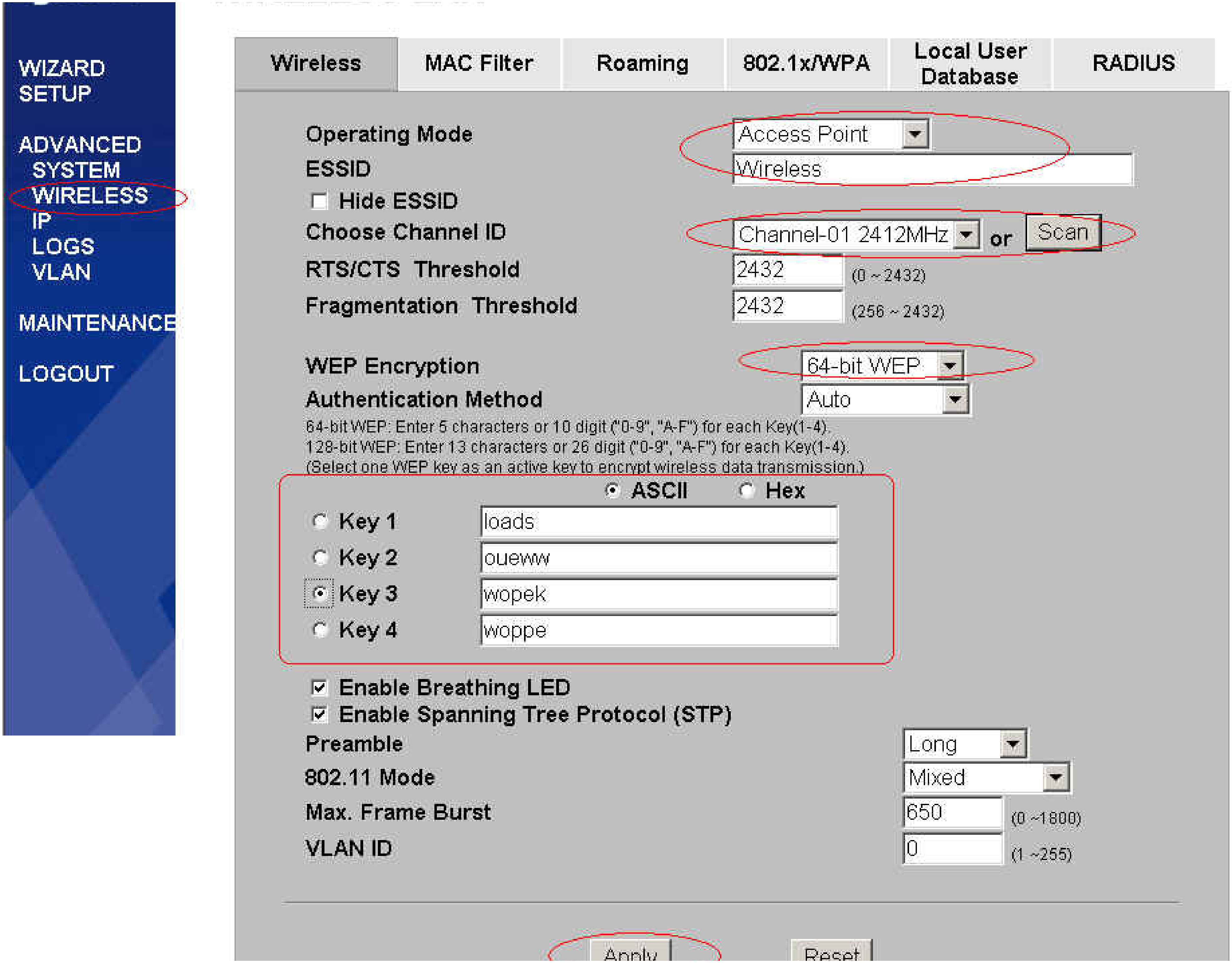
Access Point (encrypt data by Key 3) --------> Station (decrypt data by Key 3)

Access Point (decrypt data by Key 2) <-------- Station (encrypt data by Key 2)

In this case, access point transmits data to station which encrypt data by Key 3 of access point. The station will decrypt the data by its Key 3.

At the same time, when the station transmits data to access point which encrypt data by Key 2.
The access point will decrypt the data by its Key 2.

- Setting up the Access Point with Web configurator



Operating Mode: Access Point

ESSID: Wireless

□ Hide ESSID

Choose Channel ID: Channel-01 2412MHz or Scan

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

WEP Encryption: 64-bit WEP

Authentication Method: Auto

64-bit WEP: Enter 5 characters or 10 digit ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 characters or 26 digit ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

● ASCII ○ Hex

○ Key 1: loads
○ Key 2: oueww
● Key 3: wopek
○ Key 4: woppe

☑ Enable Breathing LED

☑ Enable Spanning Tree Protocol (STP)

Preamble: Long

802.11 Mode: Mixed

Max. Frame Burst: 650 (0 ~1800)

VLAN ID: 0 (1 ~255)

Key settings

Select one WEP key as default key to encrypt wireless data transmission.

Setting up the Station

1. Double click on the utility icon in your windows task bar or right click the utility icon then select 'Show Config Utility'.

The utility will pop up on your windows screen.

Note: If the utility icon doesn't exist in your task bar, click Start -> Programs -> IEEE802.11b WLAN Card -> IEEE802.11b WLAN Card.

2. Select the 'Encryption' tab.
   Select encryption type correspond with access point.
   Set up 4 Keys which correspond with the WEP Keys of access point.
   And select on WEP key as default key to encrypt wireless data transmission.

Key settings

The WEP Encryption type of station has to equal to the access point.
Check 'ASCII' field for characters WEP key or **uncheck 'ASCII'** field for Hexadecimal digits WEP key.
Hexadecimal digits don't need to preceded by '0x'.
For example,

64-bits with characters WEP key :
Key1= loads
Key2= oueww
Key3= wopek
Key4= woppe

64-bits with hexadecimal digits WEP key :
Key1= 123456789A
Key2= 23456789AB
Key3= 3456789ABC

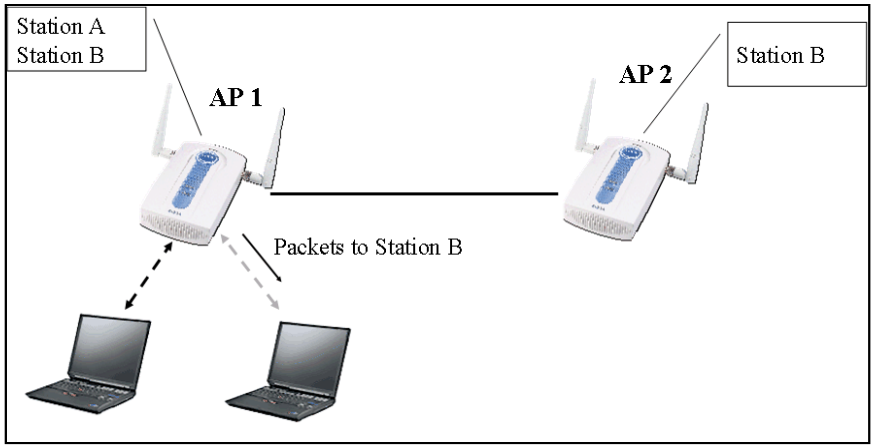
Key4= 456789ABCD

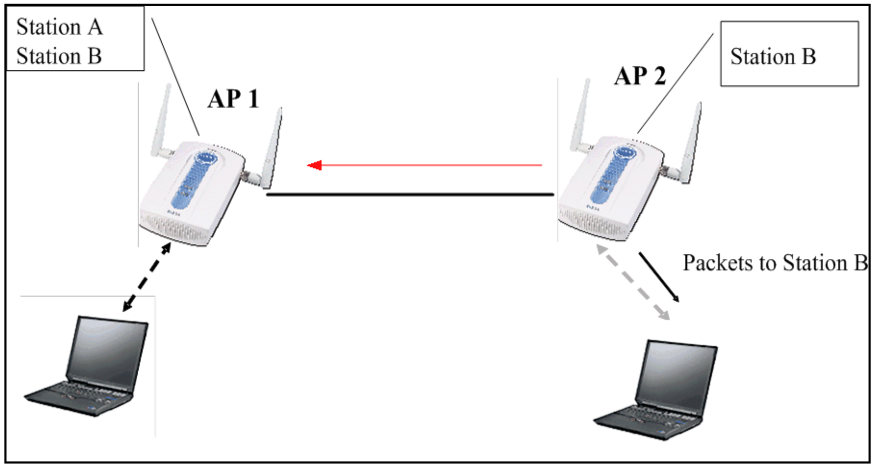
Configure Access Point for Roaming

- Introduction

What is Roaming?

In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. During this period, the wireless station maintains uninterrupted connection to the network. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending on the signal strength, network utilization or other factors.





- Configuration AP1 for Roaming using SMT

To Enable the roaming feature if you have two or more ZyAIRs on the same subnet. Follow the steps below to allow roaming on your ZyAIR.

1. From the SMT main menu, enter 3 to display Menu 3 – LAN Setup.

2. Enter 5 to display Menu 3.5 – Wireless LAN Setup.

```
                Menu 3.5 - Wireless LAN Setup

    Operaing Mode= Access Point       Edit MAC Address Filter= No
    ESSID= Wireless                     Edit Roaming Configuration= Yes
    Hide ESSID= No                      Edit Multiple ESS Configuration= N/A
    Channel ID= CH06 2412MHz          Edit Bridge Link Configuration= N/A
    RTS Threshold= 2432                Block Intra-BSS Traffic= No
    Frag. Threshold= 2432             Number of Associated Stations= 32
    WEP Encryption= Disable           Breathing LED= Yes

      Default Key= N/A                  Output Power= 17dBm
      Key1= N/A
      Key2= N/A
      Key3= N/A
      Key4= N/A
      Authen. Method= N/A

                   Press ENTER to Confirm or ESC to Cancel:
```

3. Move the cursor to the Edit Roaming Configuration field. Press [SPACE BAR] to select Yes and then press [ENTER]. Menu 3.5.2 Roaming Configuration displays as shown next.

```
     Menu 3.5.2 - Roaming Configuration

             Active= Yes
             Port #= 3517


   Press ENTER to Confirm or ESC to Cancel:
```

- Configuration AP2 for Roaming using SMT

To Enable the roaming feature if you have two or more ZyAIRs on the same subnet. Follow the steps below to allow roaming on your ZyAIR.

1. From the SMT main menu, enter 3 to display Menu 3 – LAN Setup.

2. Enter 5 to display Menu 3.5 – Wireless LAN Setup.

```
                     Menu 3.5 - Wireless LAN Setup

     Operaing Mode= Access Point       Edit MAC Address Filter= No
     ESSID= Wireless                     Edit Roaming Configuration= Yes
     Hide ESSID= No                      Edit Multiple ESS Configuration= N/A
     Channel ID= CH06 2412MHz          Edit Bridge Link Configuration= N/A
     RTS Threshold= 2432                Block Intra-BSS Traffic= No
     Frag. Threshold= 2432             Number of Associated Stations= 32
     WEP Encryption= Disable           Breathing LED= Yes

       Default Key= N/A                  Output Power= 17dBm
       Key1= N/A
       Key2= N/A
       Key3= N/A
       Key4= N/A
       Authen. Method= N/A

                    Press ENTER to Confirm or ESC to Cancel:
```

3. Move the cursor to the Edit Roaming Configuration field. Press [SPACE BAR] to select Yes and then press [ENTER]. Menu 3.5.2 Roaming Configuration displays as shown next.

```
     Menu 3.5.2 - Roaming Configuration

             Active= Yes
             Port #= 3517


   Press ENTER to Confirm or ESC to Cancel:
```

field	description
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to enable roaming on the ZyAIR if you have two or more ZyAIRs on the same subnet.
Port #	Enter the port number to communicate roaming information between access points. The port number must be the same on all access points. The default is **3517**. Make sure this port is not used by other services.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

4. Requirements for Roaming

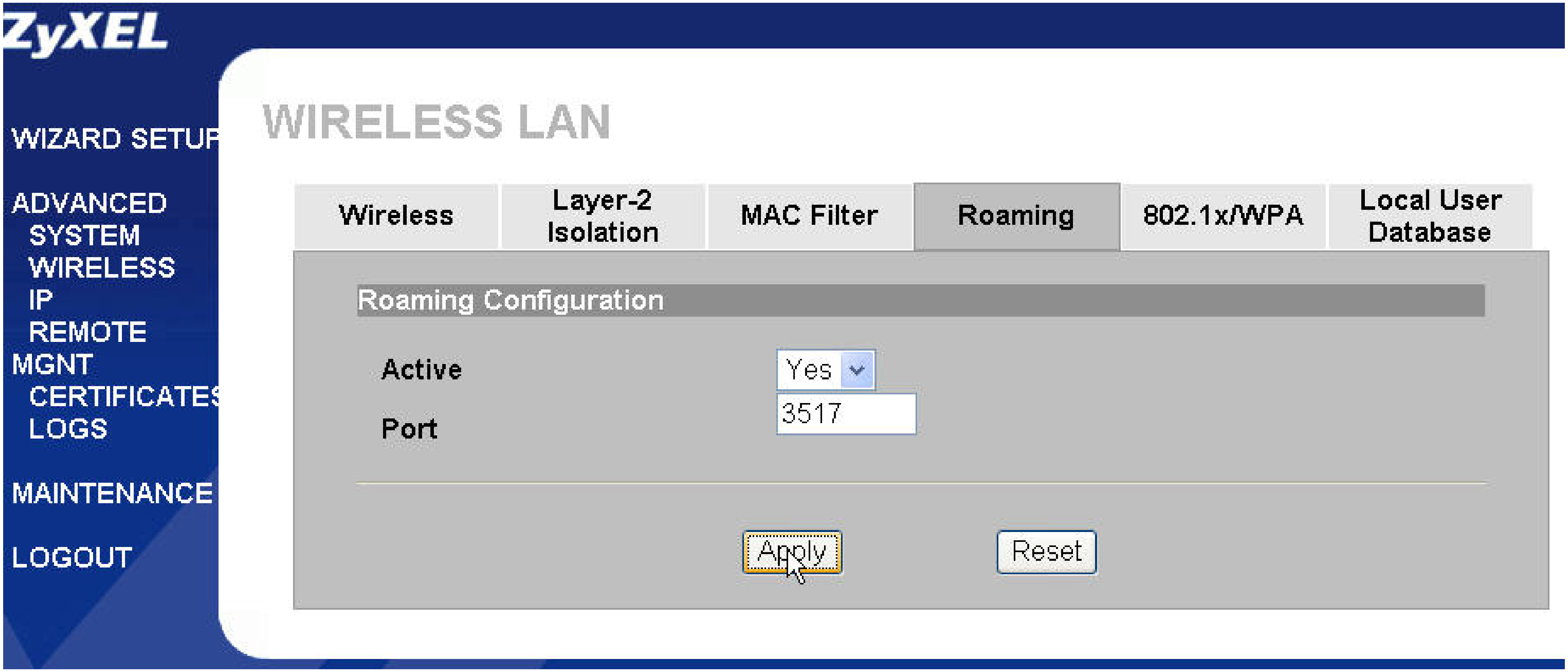
The following requirements must be met in order for wireless stations to roam between the coverage areas.

1. All the access points and wireless stations must be on the same subnet, configured with the same ESSID and security settings such as WEP.
2. If IEEE 802.1X user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.
3. The adjacent access points should use different radio channels when their coverage areas overlap to provide seamless roaming.
4. All access points must use the same port number to relay roaming information.

- Configuration AP1 for Roaming using Web configurator

To Enable the roaming feature if you have two or more ZyAIRs on the same subnet. Follow the steps below to allow roaming on your ZyAIR.

1. From the Web configurator main menu, Click Advanced->wireless than select roaming tab in wireless page.



Roaming Configuration

Active: Yes

Port: 3517

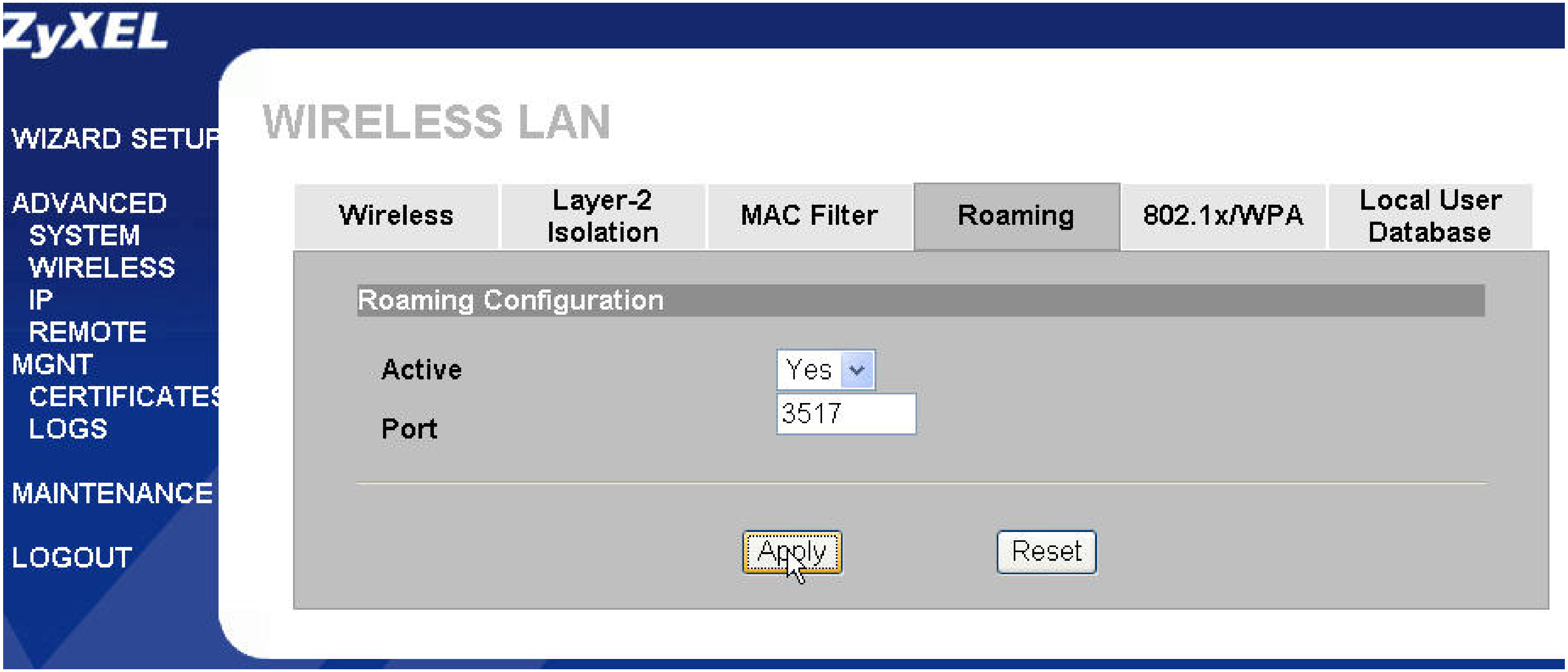
2. Select 'Yes' from the pull down menu under Roaming configuration and specify the roaming port.

3. Upon completion click Apply to make configuration take effect.

- Configuration AP2 for Roaming using Web configurator

To Enable the roaming feature if you have two or more ZyAIRs on the same subnet. Follow the steps below to allow roaming on your ZyAIR.

1. From the Web configurator main menu, Click Advanced->wireless than select roaming tab in wireless page.



Active: Yes

Port: 3517

2. Select 'Yes' from the pull down menu under Roaming configuration and specify the roaming port.

3. Upon completion click Apply to make configuration take effect.

field	description
Active	Use the pull down menu to select **Yes** to enable roaming on the ZyAIR if you have two or more ZyAIRs on the same subnet.
Port #	Enter the port number to communicate roaming information between access points. The port number must be the same on all access points. The default is **3517**. Make sure this port is not used by other services.
When you have completed this menu, press [Apply] on the bottom of the page for the configuration to take effect.	

4. Requirements for Roaming

The following requirements must be met in order for wireless stations to roam between the coverage areas.

1. All the access points and wireless stations must be on the same subnet, configured with the same ESSID and security settings such as WEP.
2. If IEEE 802.1X user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.
3. The adjacent access points should use different radio channels when their coverage areas overlap to provide seamless roaming.
4. All access points must use the same port number to relay roaming information.

Site Survey

- ***Introduction***

What is Site Survey?

An RF site survey is a MAP to RF contour of RF coverage in a particular facility. With wireless system it is very difficult to predict the propagation of radio waves and detect the presence of interfering signals. Walls, doors, elevator shafts, and other obstacles offer different degree of attenuation. This will cause the RF coverage pattern be irregular and hard to predict.

Site survey can help us overcome these problem and even provide us a map of RF coverage of the facility.

Preparation

Below are the step to complete a simple site survey with simple tools.

1. First you will need to Obtain a facility diagram, such as a blueprints. This is for you to mark and take record on.

2. Visually inspect the facility, walk through the facility to verify the accuracy of the diagram and mark down any large obstacle you see that may effect the RF signal such as metal shelf, metal desk, etc on the diagram.

3. Identify user's area, when doing so ask a question where is wireless coverage needed and where does not, and note and take note on the diagram this is information is needed to determine the number of AP required.

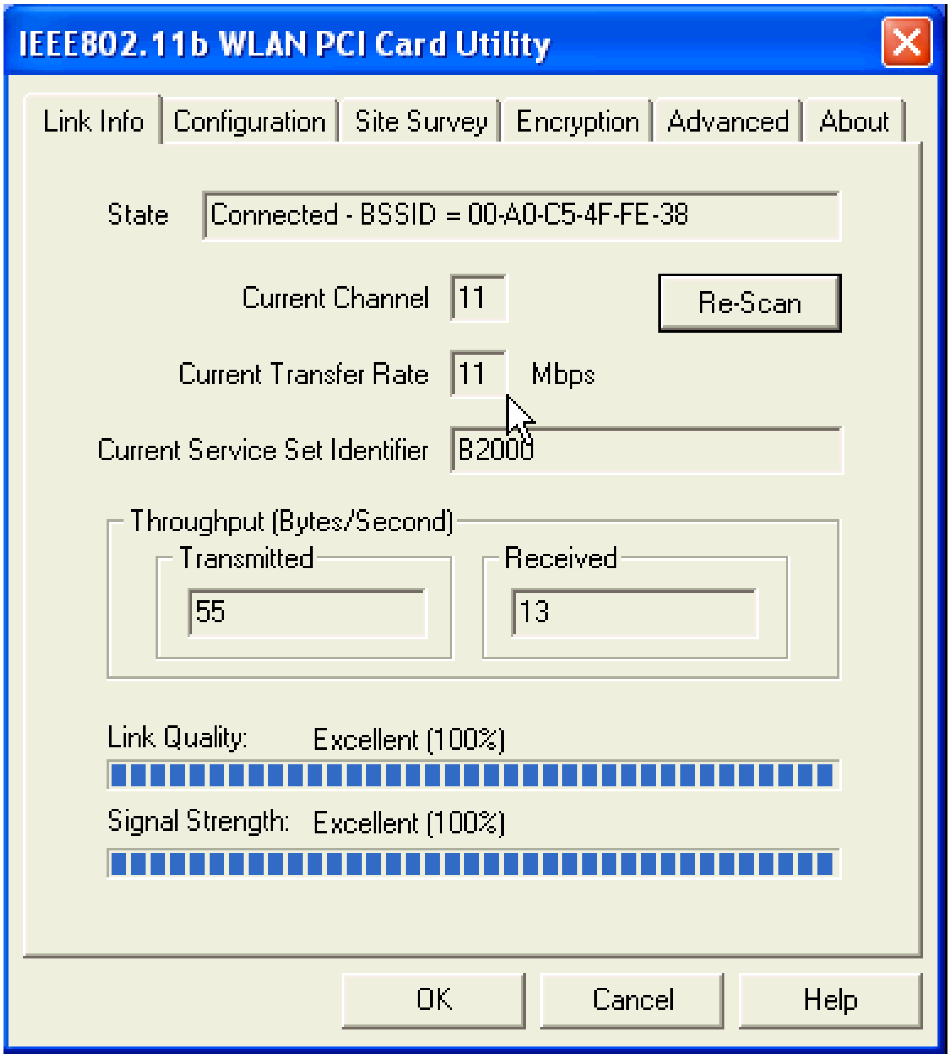
4. Determine the preliminary access point location on the facility diagram base on the service area needed, obstacles, power wall jack considerations.

Survey on Site

1. With the diagram with all information you gathered in the preparation phase. Now you are ready to make the survey.

2. Install an access point at the preliminary location.

3. User a notebook with wireless client installed and run it's utility. An utility will provide information such as connection speed, current used channel, associated rate, link quality, signal strength and etc information as shown in utility below.



IEEE802.11b WLAN PCI Card Utility

State: Connected - BSSID = 00-A0-C5-4F-FE-38

Current Channel: 11

Current Transfer Rate: 11 Mbps

Current Service Set Identifier: B2000

Throughput (Bytes/Second)

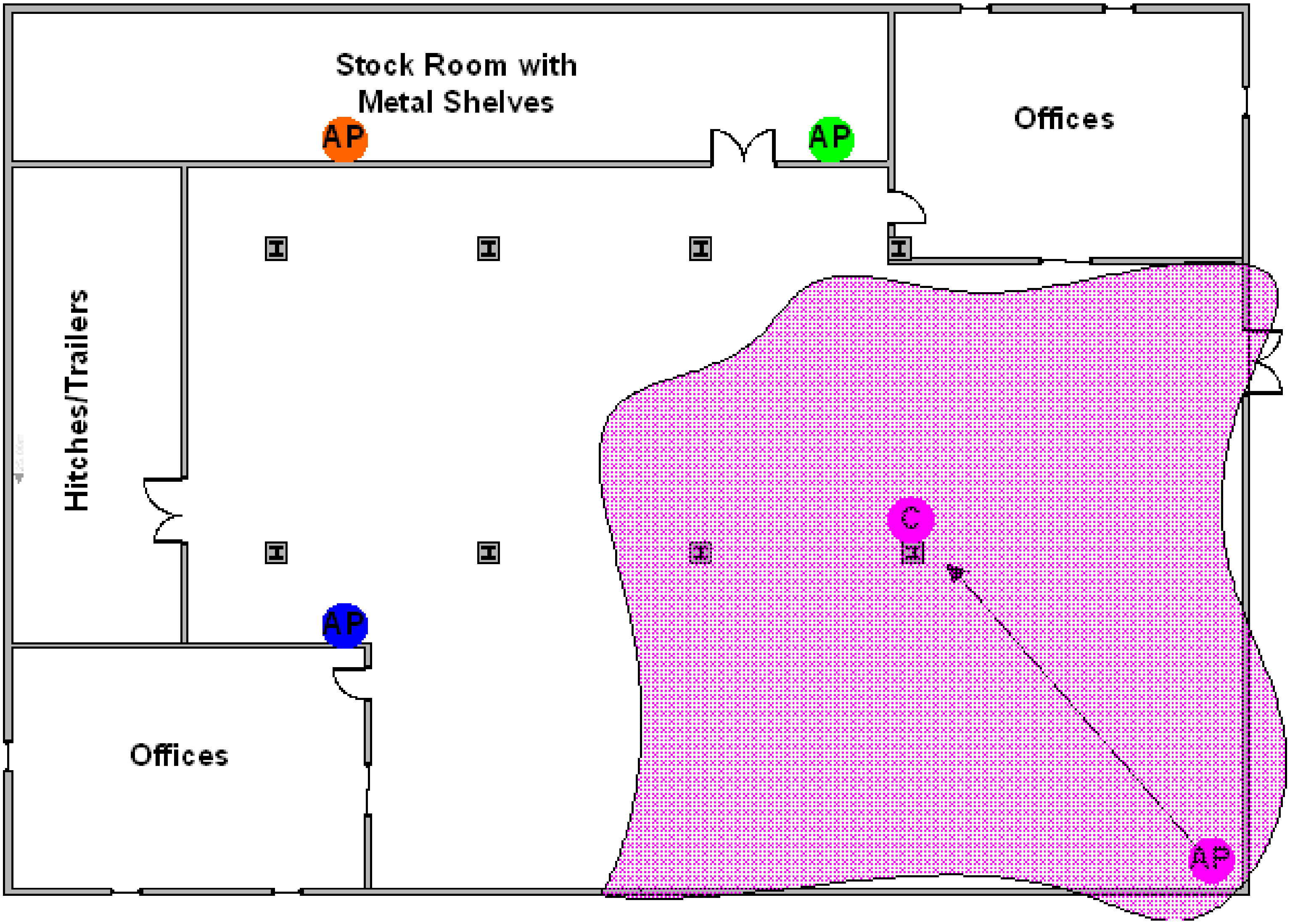
Transmitted: 55

Received: 13

Link Quality: Excellent (100%)

Signal Strength: Excellent (100%)

4. It's always a good idea to start with putting the access point at the corner of the room and walk away from the access point in a systematic manner. Record down the changes at point where transfer rate drop and the link quality and signal strength information on the diagram as you go alone.

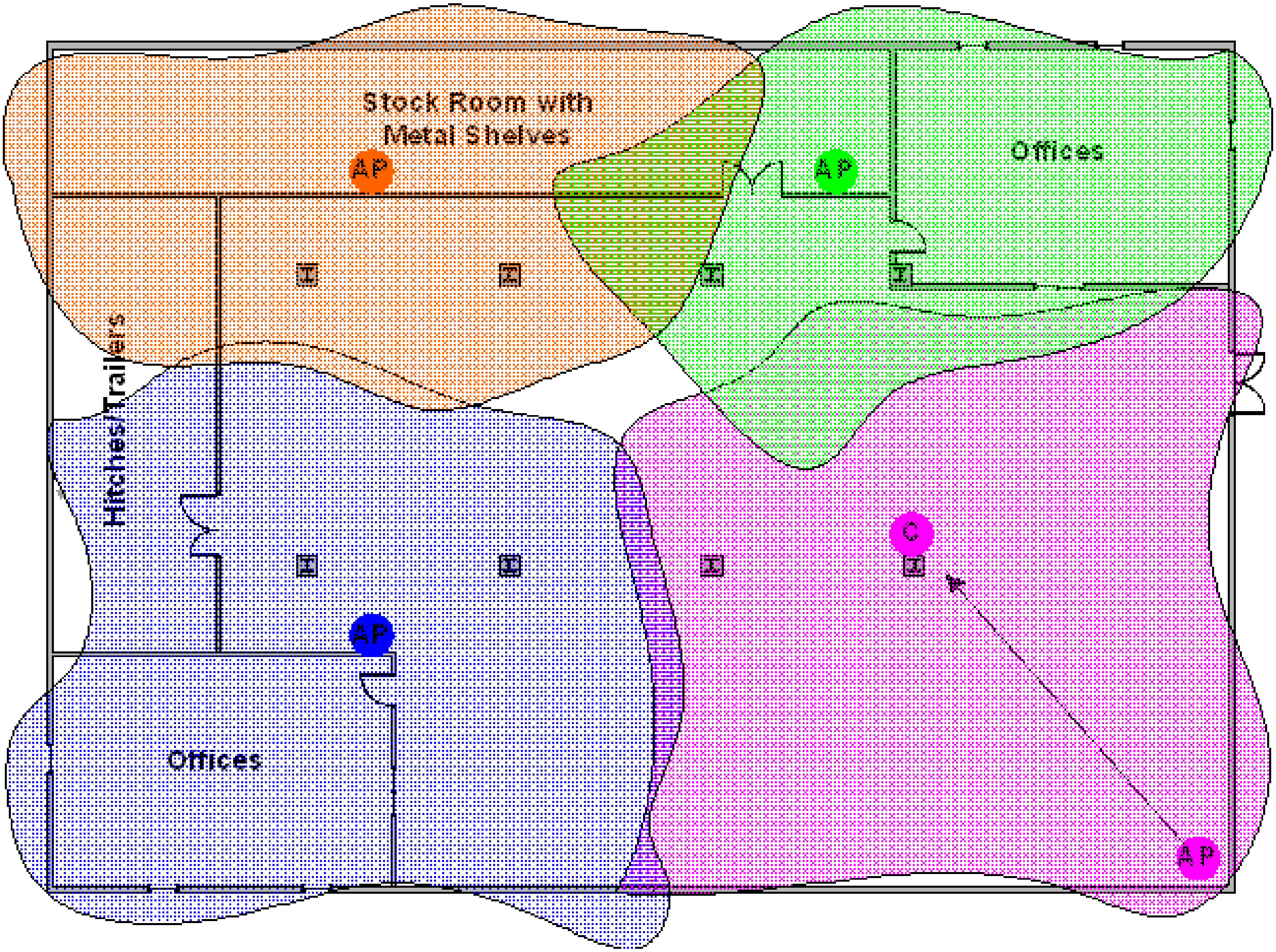


5. When you reach the farthest point of connection mark the spot. Now you move the access point to this new spot as have already determine the farthest point of the access point installation spot if wireless service is required from corner of the room.

6. Repeat step 1~5 and now you should be able to mark an RF coverage area as illustrated in above picutre.

7. You may need more than one access point is the RF coverage area have not cover all the wireless service area you needed.

8. Repeat step 1~6 of survey on site as necessary, upon completion you will have an diagram and information of site survey. As illustrated below.



Note: If there are more than one access point is needed be sure to make the adjacent access point service area over lap one another. So the wireless station are able to roam. For more information please refer to roaming at

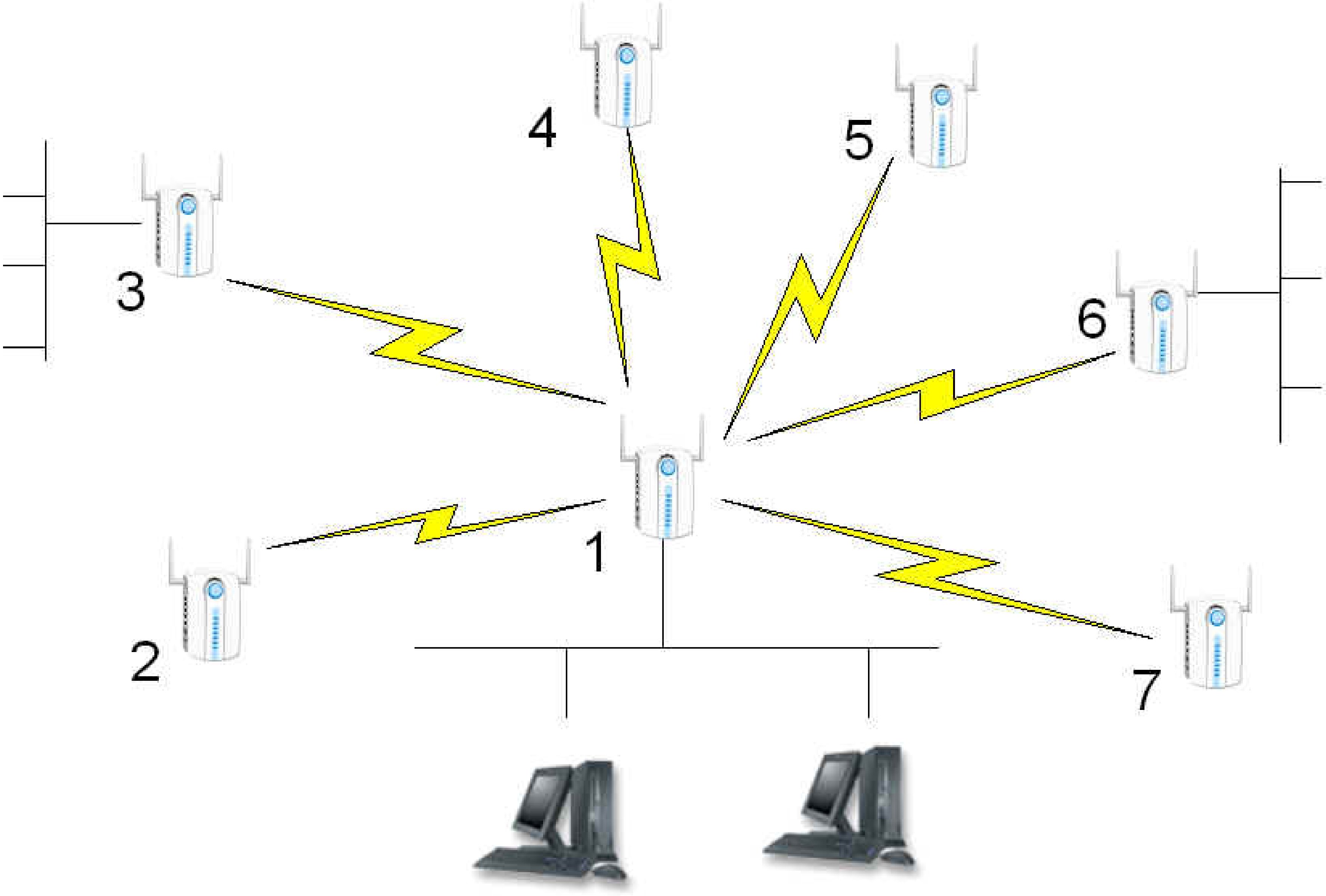
Configure Access Point as a Multiple WDS(Wireless Distribution System) bridge/repeater mode

- ***Introduction***

What is multiple WDS bridge Functionality?

A multiple Distribution System(DS) is a wired connection between two or more APs. While a Wireless Distribution System(WDS) is a wireless connection. The ZyAIR support multiple WDS, providing a cost-effective solution for wireless network expansion.

The ZyAIR can function as a wireless network bridge and establish up to six wireless links with other APs.



- ***Configuration for Wireless Station 1***

The ZyAIR can function as wireless network bridge allowing you to wirelessly connect up to 6 wired network segments. You need to know the MAC address of the peer device, which also must be in bridge/repeater mode.

The repeater mode is the bridge mode without the Ethernet connection. When the ZyAIR is in the bridge/repeater mode, you need to enable STP to prevent bridge loops.

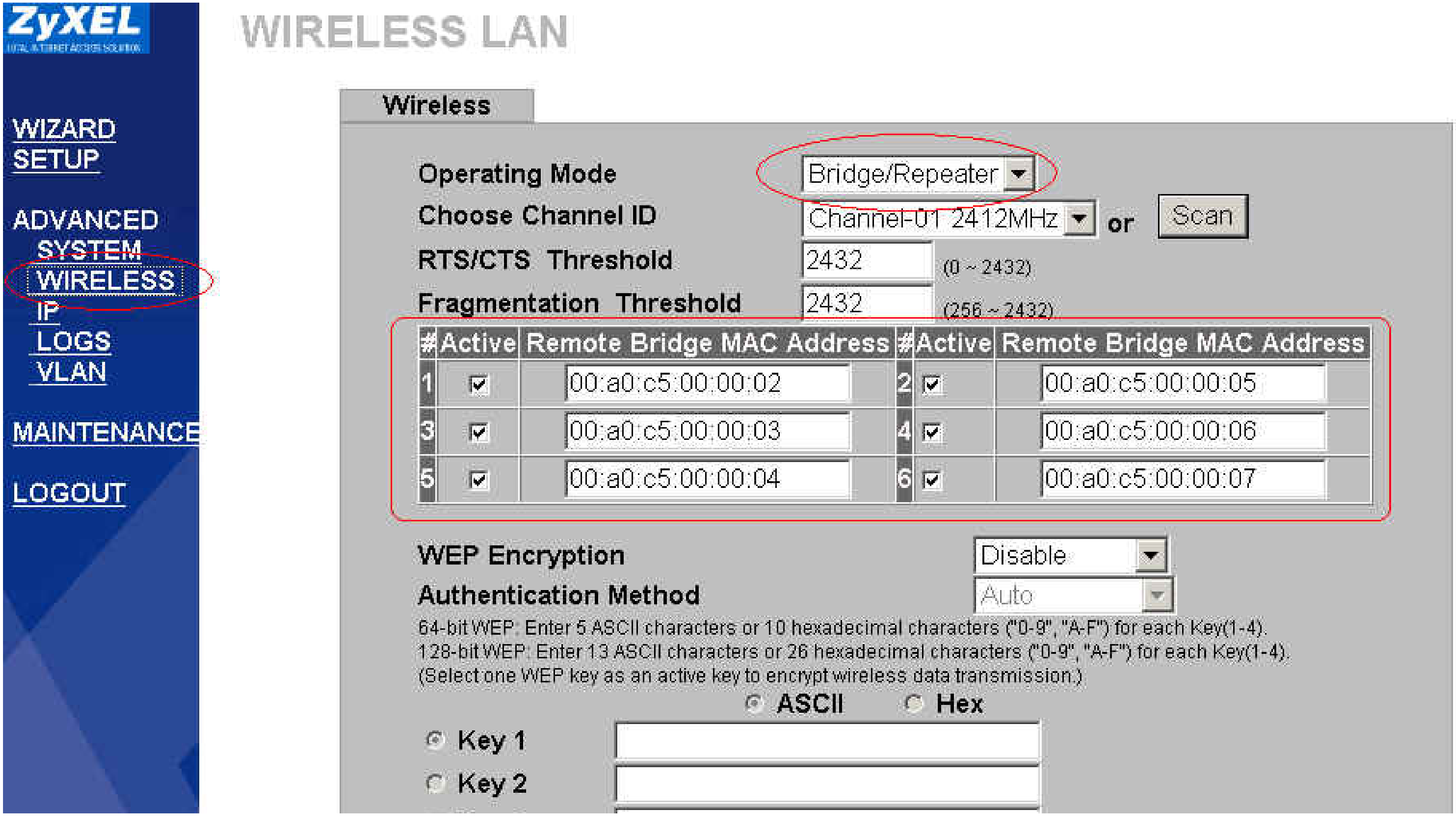
1. Click **Advanced** and **Wireless**.

2. Select **Bridge/Repeater** in the **Operation Mode** drop-down list box to display the screen as down.

3. Type the MAC address of peer device in the **Remote Bridge MAC Address** field, that is, six hexadecimal character pairs.

4. Check '**Enable Spanning Tree Protocol (STP)**'.

5. Click **Apply** to finish.



Operating Mode: Bridge/Repeater
Choose Channel ID: Channel-01 2412MHz or Scan
RTS/CTS Threshold: 2432 (0 ~ 2432)
Fragmentation Threshold: 2432 (256 ~ 2432)

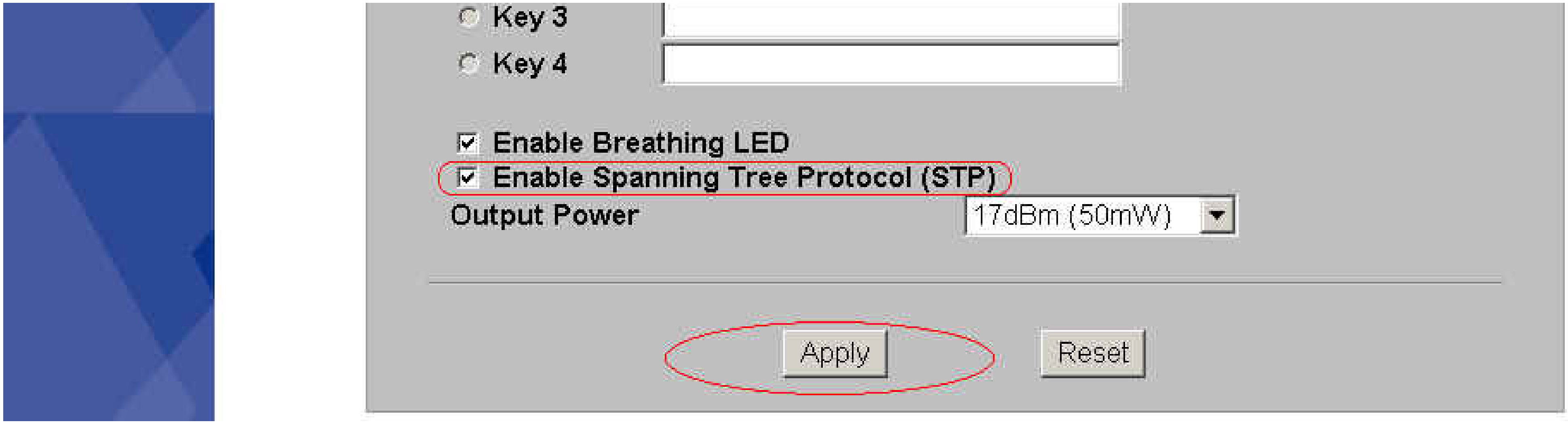
#	Active	Remote Bridge MAC Address	#	Active	Remote Bridge MAC Address
1	☑	00:a0:c5:00:00:02	2	☑	00:a0:c5:00:00:05
3	☑	00:a0:c5:00:00:03	4	☑	00:a0:c5:00:00:06
5	☑	00:a0:c5:00:00:04	6	☑	00:a0:c5:00:00:07

WEP Encryption: Disable
Authentication Method: Auto

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

● ASCII ○ Hex

● Key 1
○ Key 2



○ Key 3

○ Key 4

☑ Enable Breathing LED

☑ Enable Spanning Tree Protocol (STP)

Output Power: 17dBm (50mW)

- ***Configuration for Wireless Station 2***

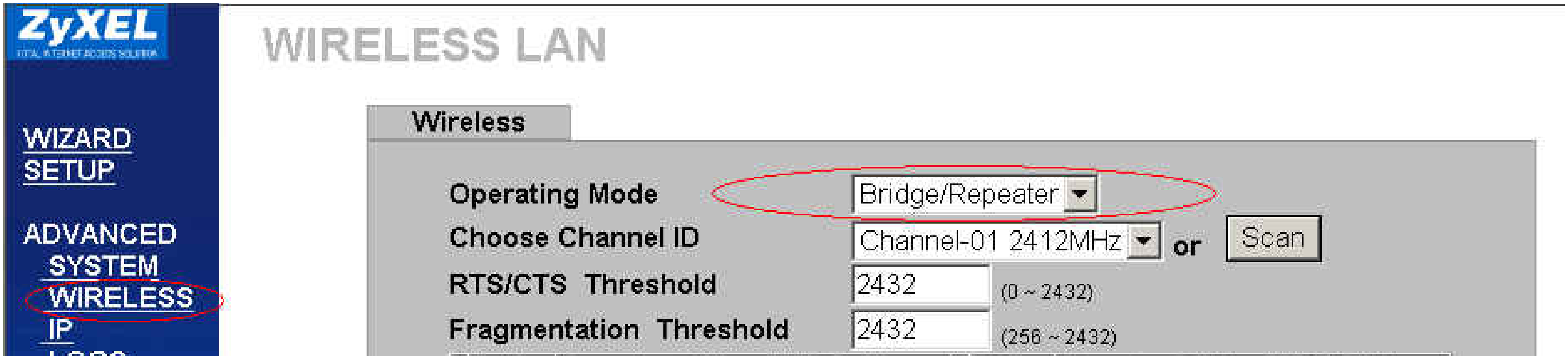
1. Click **Advanced** and **Wireless**.

2. Select **Bridge/Repeater** in the **Operation Mode** drop-down list box to display the screen as down.

3. Type the MAC address of peer device in the **Remote Bridge MAC Address** field, that is, six hexadecimal character pairs.

4. Check '**Enable Spanning Tree Protocol(STP)**'.

5. Click **Apply** to finish.

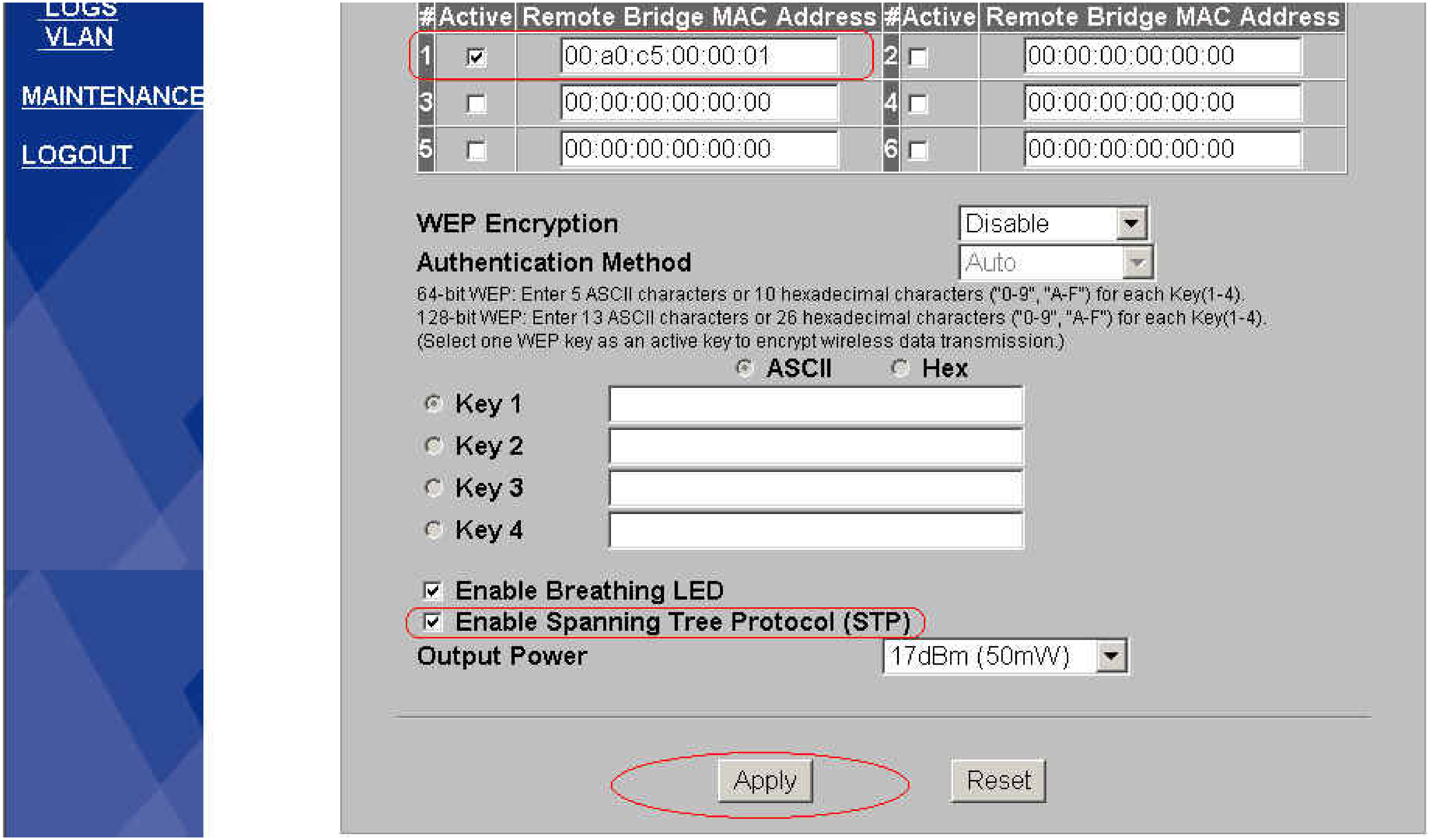


Operating Mode: Bridge/Repeater

Choose Channel ID: Channel-01 2412MHz or

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)



#	Active	Remote Bridge MAC Address	#	Active	Remote Bridge MAC Address
1	☑	00:a0:c5:00:00:01	2	□	00:00:00:00:00:00
3	□	00:00:00:00:00:00	4	□	00:00:00:00:00:00
5	□	00:00:00:00:00:00	6	□	00:00:00:00:00:00

WEP Encryption: Disable

Authentication Method: Auto

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

● ASCII ○ Hex

● Key 1
○ Key 2
○ Key 3
○ Key 4

☑ Enable Breathing LED

☑ Enable Spanning Tree Protocol (STP)

Output Power: 17dBm (50mW)

- ***Configuration for Wireless Station 3***

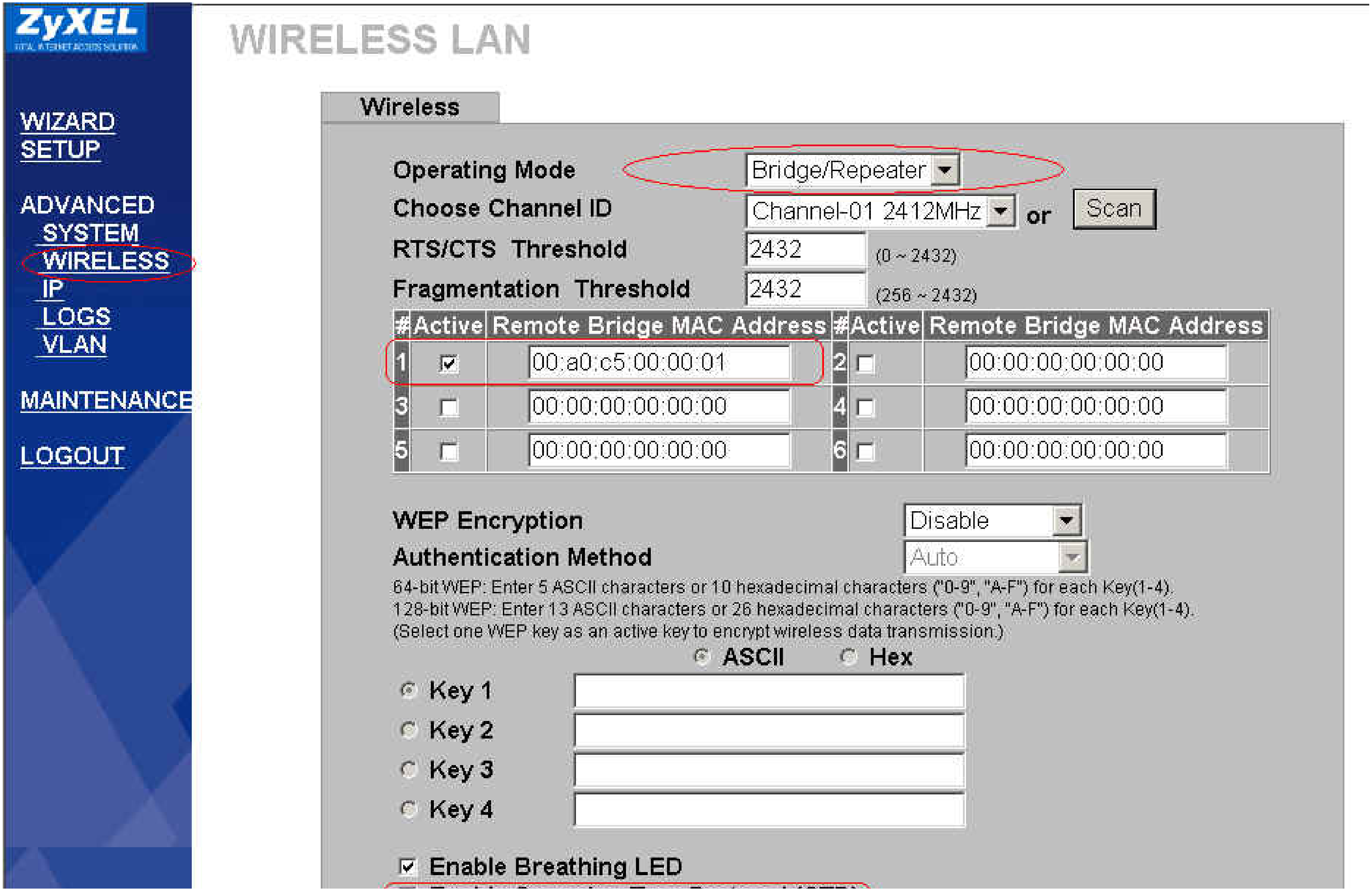
1. Click **Advanced** and **Wireless**.

2. Select **Bridge/Repeater** in the **Operation Mode** drop-down list box to display the screen as down.

3. Type the MAC address of peer device in the **Remote Bridge MAC Address** field, that is, six hexadecimal character pairs.

4. Check '**Enable Spanning Tree Protocol(STP)**'.

5. Click **Apply** to finish.



Operating Mode: Bridge/Repeater

Choose Channel ID: Channel-01 2412MHz or Scan

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

#	Active	Remote Bridge MAC Address	#	Active	Remote Bridge MAC Address
1	☑	00:a0:c5:00:00:01	2	□	00:00:00:00:00:00
3	□	00:00:00:00:00:00	4	□	00:00:00:00:00:00
5	□	00:00:00:00:00:00	6	□	00:00:00:00:00:00

WEP Encryption: Disable

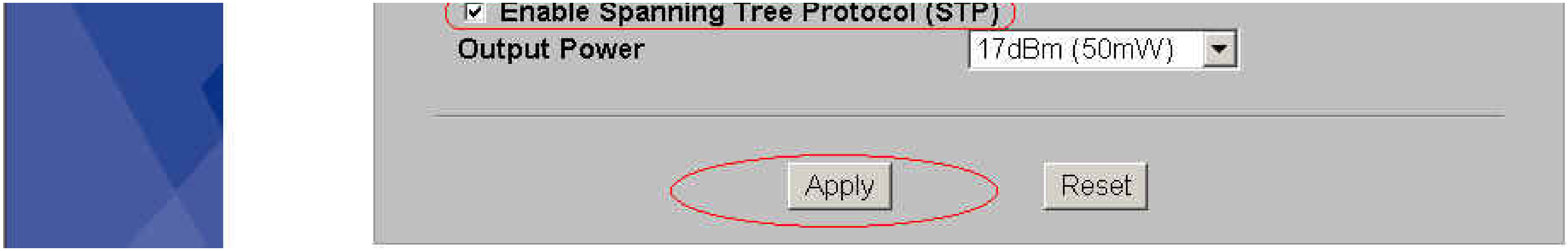
Authentication Method: Auto

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

● ASCII ○ Hex

● Key 1
○ Key 2
○ Key 3
○ Key 4

☑ Enable Breathing LED



☑ Enable Spanning Tree Protocol (STP)

Output Power 17dBm (50mW)

- ***Configuration for Wireless Station 4***

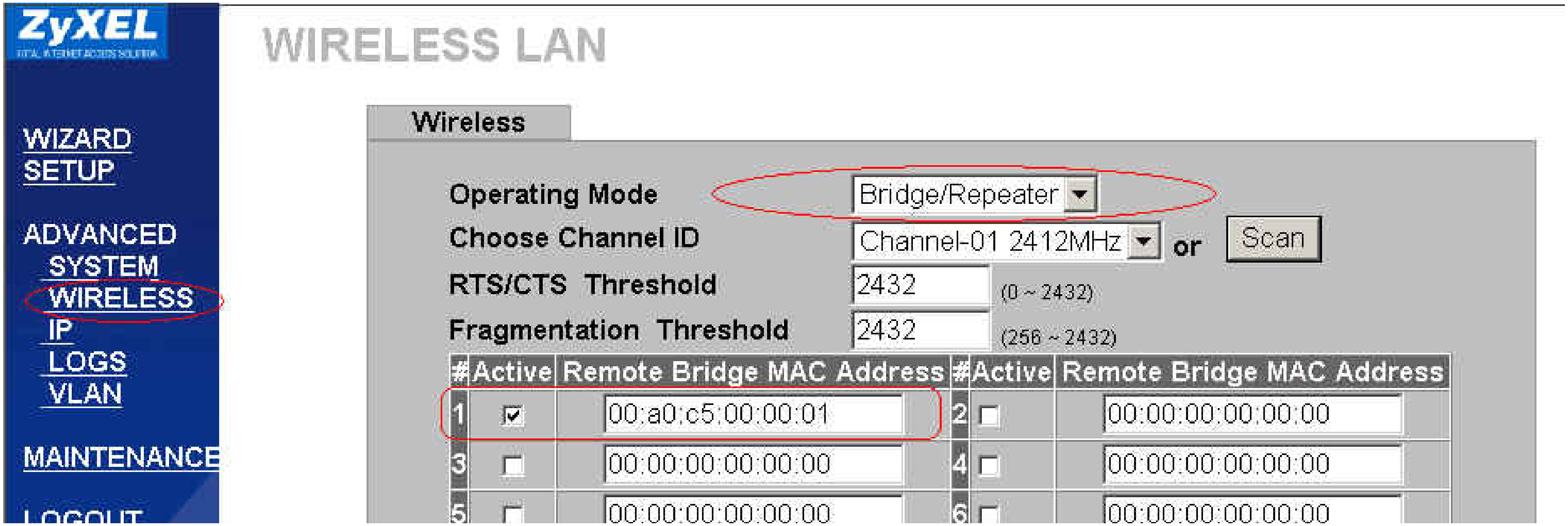
1. Click **Advanced** and **Wireless**.

2. Select **Bridge/Repeater** in the **Operation Mode** drop-down list box to display the screen as down.

3. Type the MAC address of peer device in the **Remote Bridge MAC Address** field, that is, six hexadecimal character pairs.

4. Check '**Enable Spanning Tree Protocol(STP)**'.

5. Click **Apply** to finish.



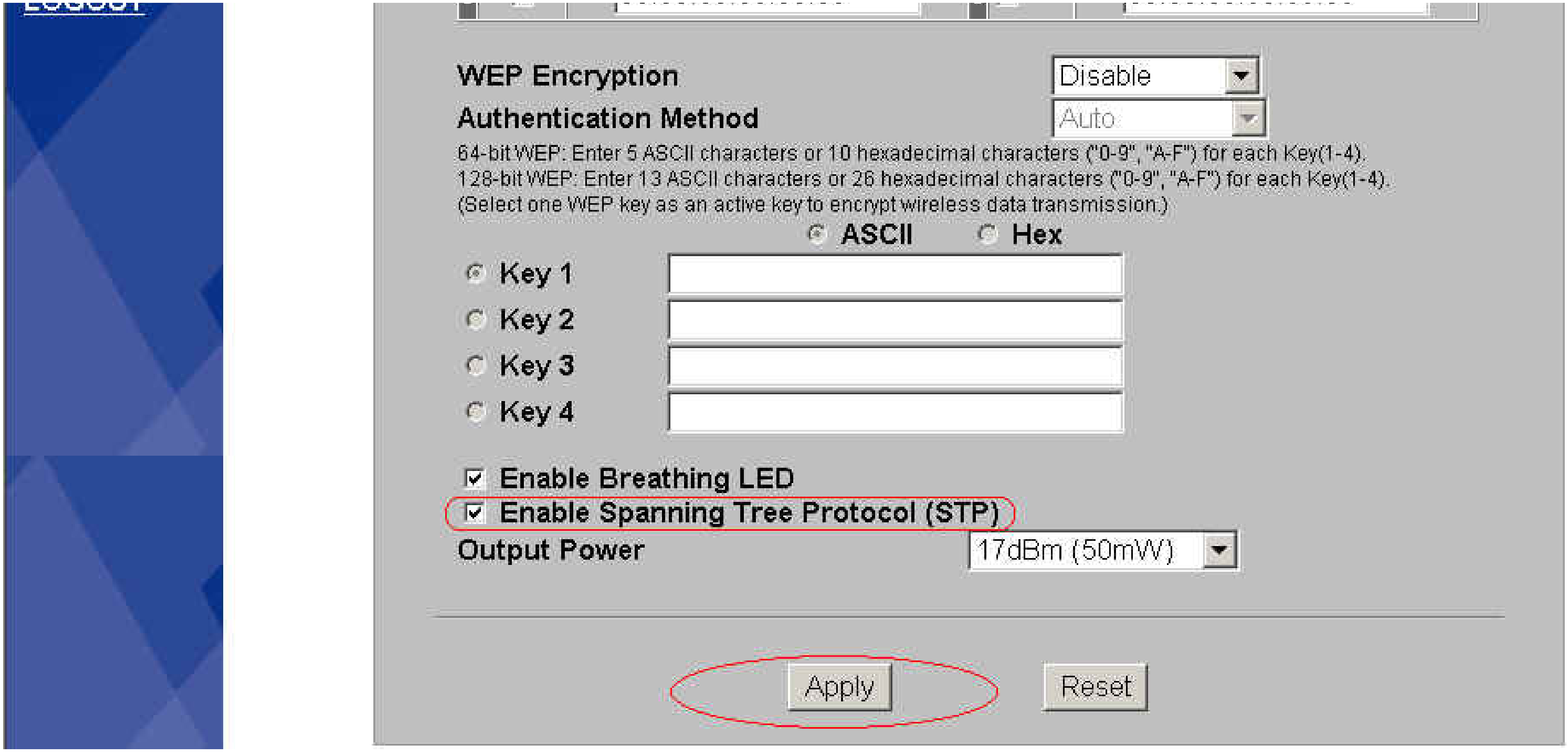
Operating Mode Bridge/Repeater

Choose Channel ID Channel-01 2412MHz or

RTS/CTS Threshold 2432 (0 ~ 2432)

Fragmentation Threshold 2432 (256 ~ 2432)

#	Active	Remote Bridge MAC Address	#	Active	Remote Bridge MAC Address
1	☑	00:a0:c5:00:00:01	2	□	00:00:00:00:00:00
3	□	00:00:00:00:00:00	4	□	00:00:00:00:00:00
5	□	00:00:00:00:00:00	6	□	00:00:00:00:00:00



WEP Encryption: Disable

Authentication Method: Auto

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

● ASCII ○ Hex

● Key 1
○ Key 2
○ Key 3
○ Key 4

☑ Enable Breathing LED
☑ Enable Spanning Tree Protocol (STP)

Output Power: 17dBm (50mW)

- ***Configuration for Wireless Station 5***

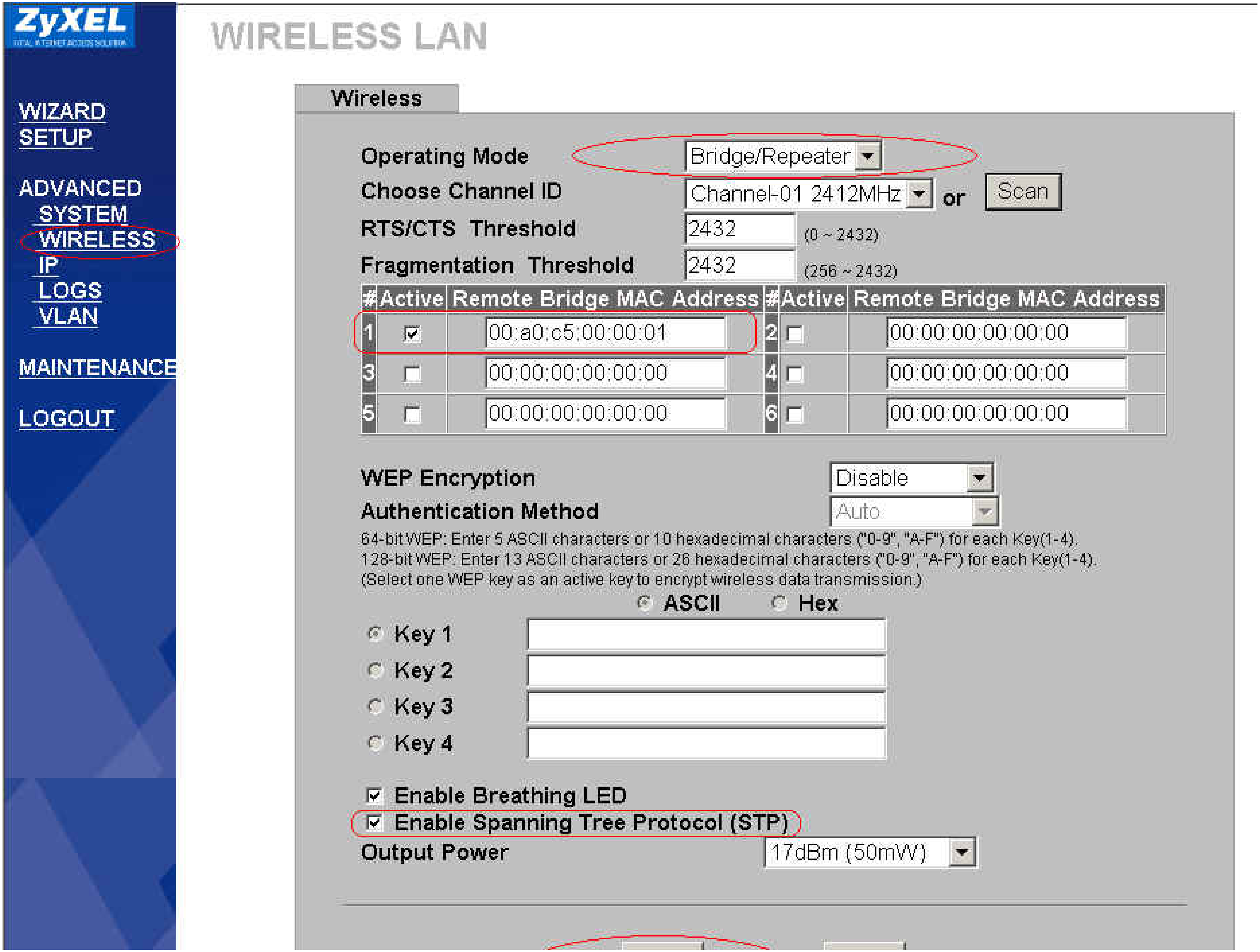
1. Click **Advanced** and **Wireless**.

2. Select **Bridge/Repeater** in the **Operation Mode** drop-down list box to display the screen as down.

3. Type the MAC address of peer device in the **Remote Bridge MAC Address** field, that is, six hexadecimal character pairs.

4. Check '**Enable Spanning Tree Protocol(STP)**'.

5. Click **Apply** to finish.



WIRELESS LAN

Wireless

Operating Mode: Bridge/Repeater

Choose Channel ID: Channel-01 2412MHz or Scan

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

#	Active	Remote Bridge MAC Address	#	Active	Remote Bridge MAC Address
1	☑	00:a0:c5:00:00:01	2	□	00:00:00:00:00:00
3	□	00:00:00:00:00:00	4	□	00:00:00:00:00:00
5	□	00:00:00:00:00:00	6	□	00:00:00:00:00:00

WEP Encryption: Disable

Authentication Method: Auto

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

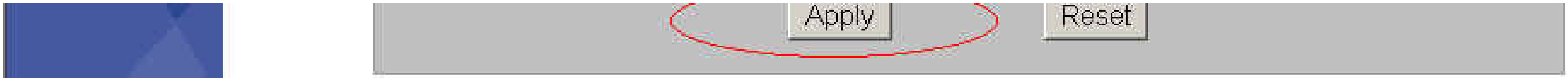
● ASCII ○ Hex

● Key 1
○ Key 2
○ Key 3
○ Key 4

☑ Enable Breathing LED

☑ Enable Spanning Tree Protocol (STP)

Output Power: 17dBm (50mW)



- ***Configuration for Wireless Station 6***

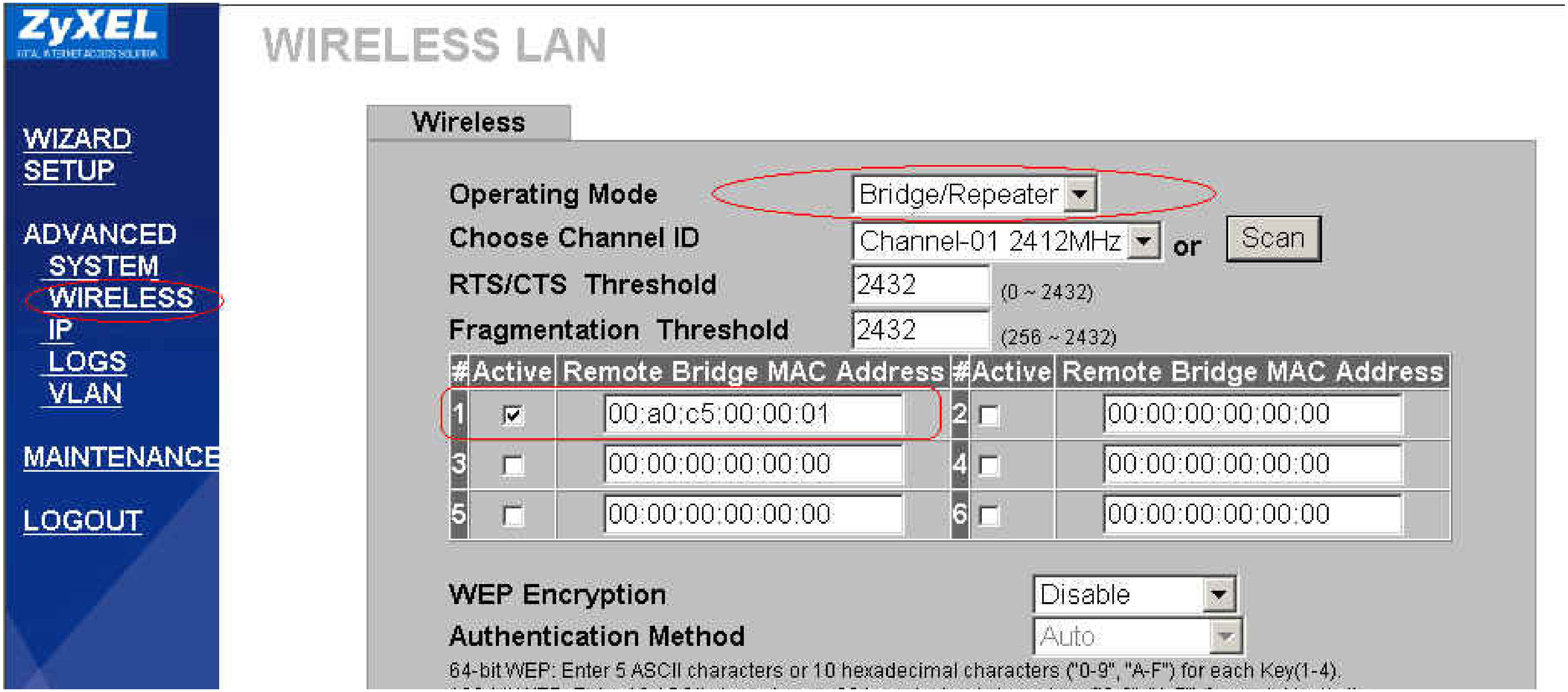
1. Click **Advanced** and **Wireless**.

2. Select **Bridge/Repeater** in the **Operation Mode** drop-down list box to display the screen as down.

3. Type the MAC address of peer device in the **Remote Bridge MAC Address** field, that is, six hexadecimal character pairs.

4. Check '**Enable Spanning Tree Protocol(STP)**'.

5. Click **Apply** to finish.



Operating Mode: Bridge/Repeater

Choose Channel ID: Channel-01 2412MHz or Scan

RTS/CTS Threshold: 2432 (0 ~ 2432)

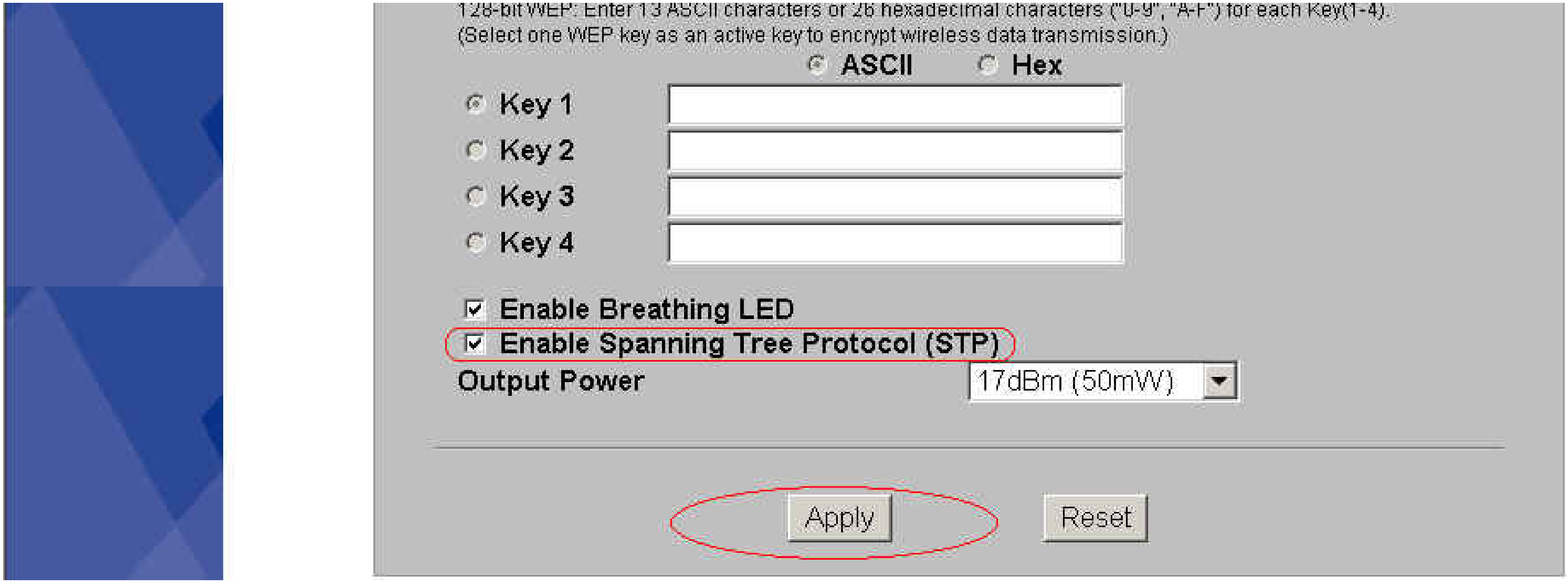
Fragmentation Threshold: 2432 (256 ~ 2432)

#	Active	Remote Bridge MAC Address	#	Active	Remote Bridge MAC Address
1	☑	00:a0:c5:00:00:01	2	□	00:00:00:00:00:00
3	□	00:00:00:00:00:00	4	□	00:00:00:00:00:00
5	□	00:00:00:00:00:00	6	□	00:00:00:00:00:00

WEP Encryption: Disable

Authentication Method: Auto

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key(1-4).



128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

● ASCII ○ Hex

● Key 1

○ Key 2

○ Key 3

○ Key 4

☑ Enable Breathing LED

☑ Enable Spanning Tree Protocol (STP)

Output Power: 17dBm (50mW)

- ***Configuration for Wireless Station 7***

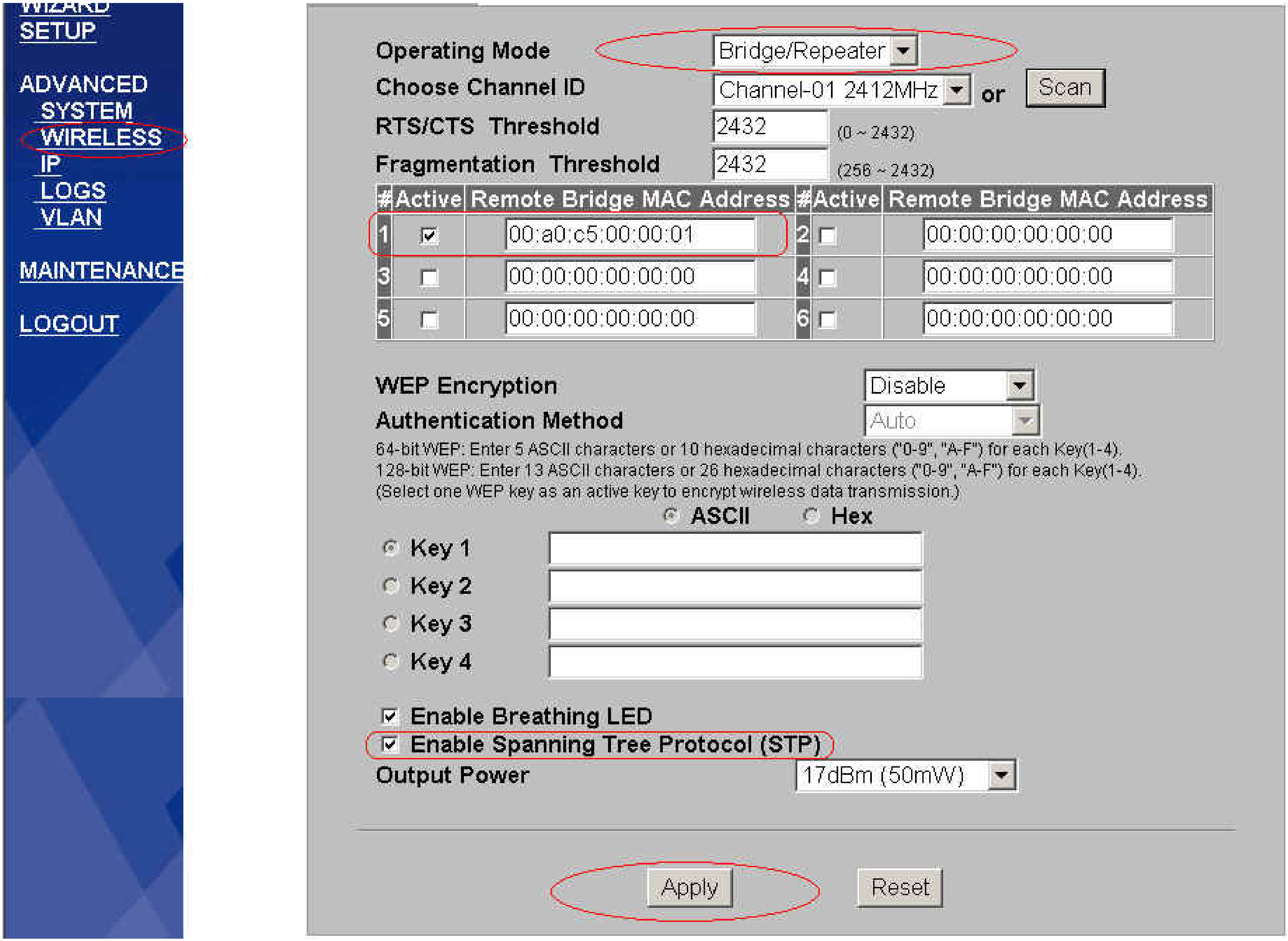
1. Click **Advanced** and **Wireless**.

2. Select **Bridge/Repeater** in the **Operation Mode** drop-down list box to display the screen as down.

3. Type the MAC address of peer device in the **Remote Bridge MAC Address** field, that is, six hexadecimal character pairs.

4. Check '**Enable Spanning Tree Protocol(STP)**'.

5. Click **Apply** to finish.



Operating Mode: Bridge/Repeater

Choose Channel ID: Channel-01 2412MHz or Scan

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

#	Active	Remote Bridge MAC Address	#	Active	Remote Bridge MAC Address
1	☑	00:a0:c5:00:00:01	2	□	00:00:00:00:00:00
3	□	00:00:00:00:00:00	4	□	00:00:00:00:00:00
5	□	00:00:00:00:00:00	6	□	00:00:00:00:00:00

WEP Encryption: Disable

Authentication Method: Auto

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

● ASCII ○ Hex

● Key 1

○ Key 2

○ Key 3

○ Key 4

☑ Enable Breathing LED

☑ Enable Spanning Tree Protocol (STP)

Output Power: 17dBm (50mW)

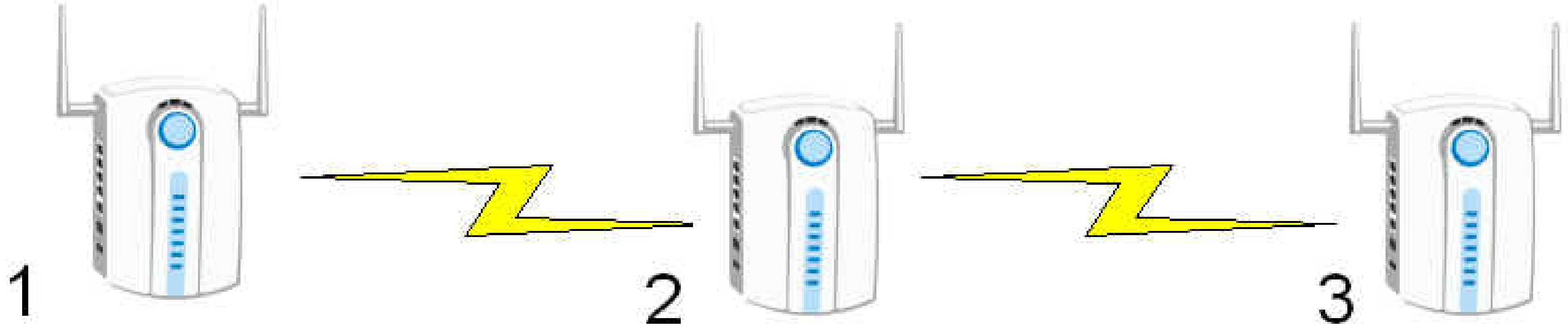
Configure Access Point as a Repeater mode

- ***Introduction***

What is Repeater Functionality?

A multiple Distribution System(DS) is a wired connection between two or more bridge/repeater devices. While a Wireless Distribution System(WDS) is a wireless connection. The ZyAIR support Repeater, providing a like repeater solution for wireless network expansion. Basically, it's still a bridge device that all of traffic is transparent through the device.

The ZyAIR can function as a wireless network bridge/repeater links with other bridge/repeater.



- ***Configuration for Wireless Station 1***

The ZyAIR can function as wireless network bridge/repeater. You need to know the MAC address of the peer device, which also must be in bridge/repeater mode.

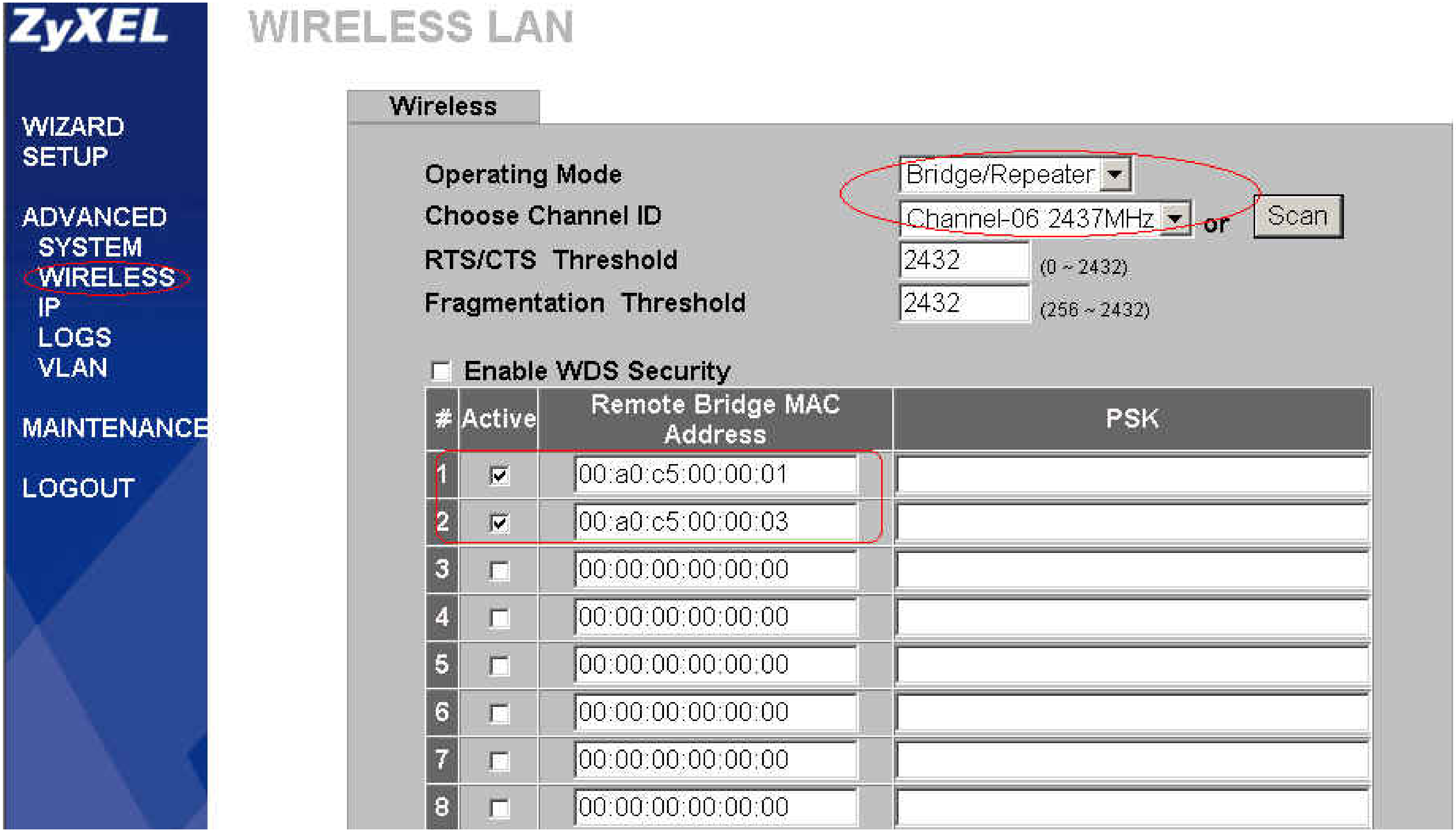
The repeater mode is the bridge mode without the Ethernet connection. When the ZyAIR is in the bridge/repeater mode, you need to enable STP to prevent bridge loops.

1. Click **Advanced** and **Wireless**.

2. Select **Bridge/Repeater** in the **Operation Mode** drop-down list box to display the screen as down.

3. Type the MAC address of peer device in the **Remote Bridge MAC Address** field, that is, six hexadecimal character pairs.

4. Click **Apply** to finish.



WIRELESS LAN

Operating Mode: Bridge/Repeater

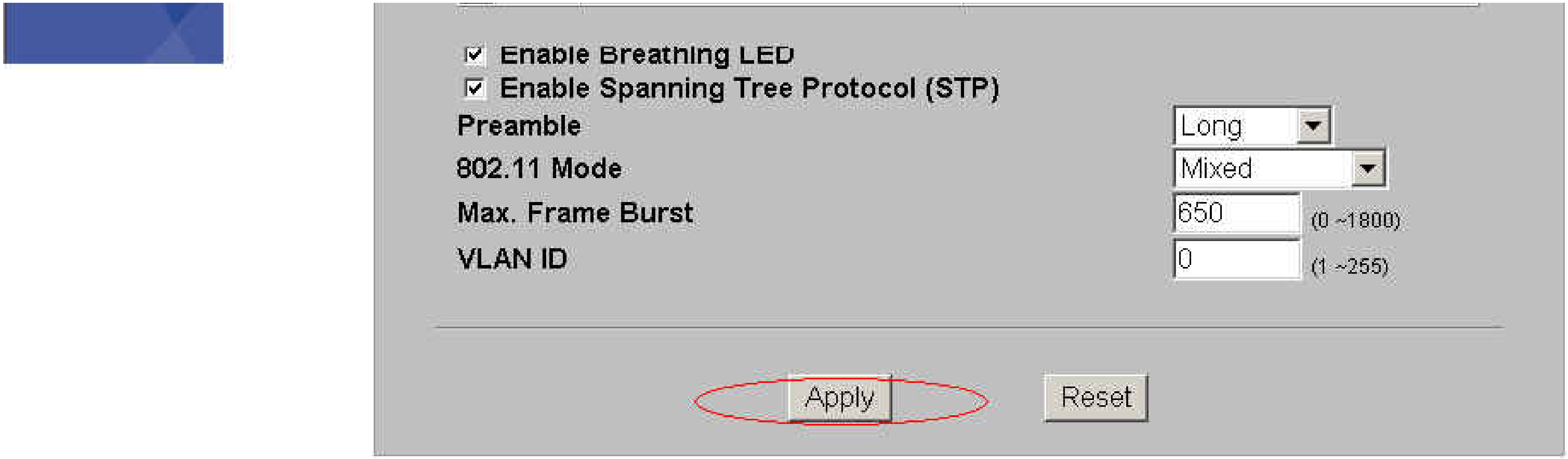
Choose Channel ID: Channel-06 2437MHz or Scan

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

□ Enable WDS Security

#	Active	Remote Bridge MAC Address	PSK
1	☑	00:a0:c5:00:00:01	
2	☑	00:a0:c5:00:00:03	
3	□	00:00:00:00:00:00	
4	□	00:00:00:00:00:00	
5	□	00:00:00:00:00:00	
6	□	00:00:00:00:00:00	
7	□	00:00:00:00:00:00	
8	□	00:00:00:00:00:00	



☑ Enable Breathing LED

☑ Enable Spanning Tree Protocol (STP)

Preamble: Long

802.11 Mode: Mixed

Max. Frame Burst: 650 (0 ~1800)

VLAN ID: 0 (1 ~255)

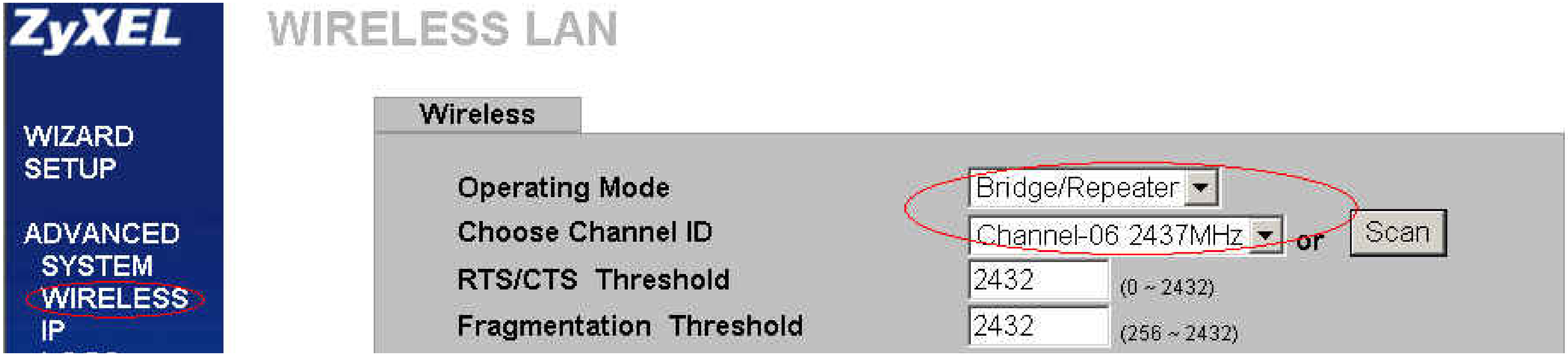
- ***Configuration for Wireless Station 2***

1. Click **Advanced** and **Wireless**.

2. Select **Bridge/Repeater** in the **Operation Mode** drop-down list box to display the screen as down.

3. Type the MAC address of peer device in the **Remote Bridge MAC Address** field, that is, six hexadecimal character pairs.

4. Click **Apply** to finish.

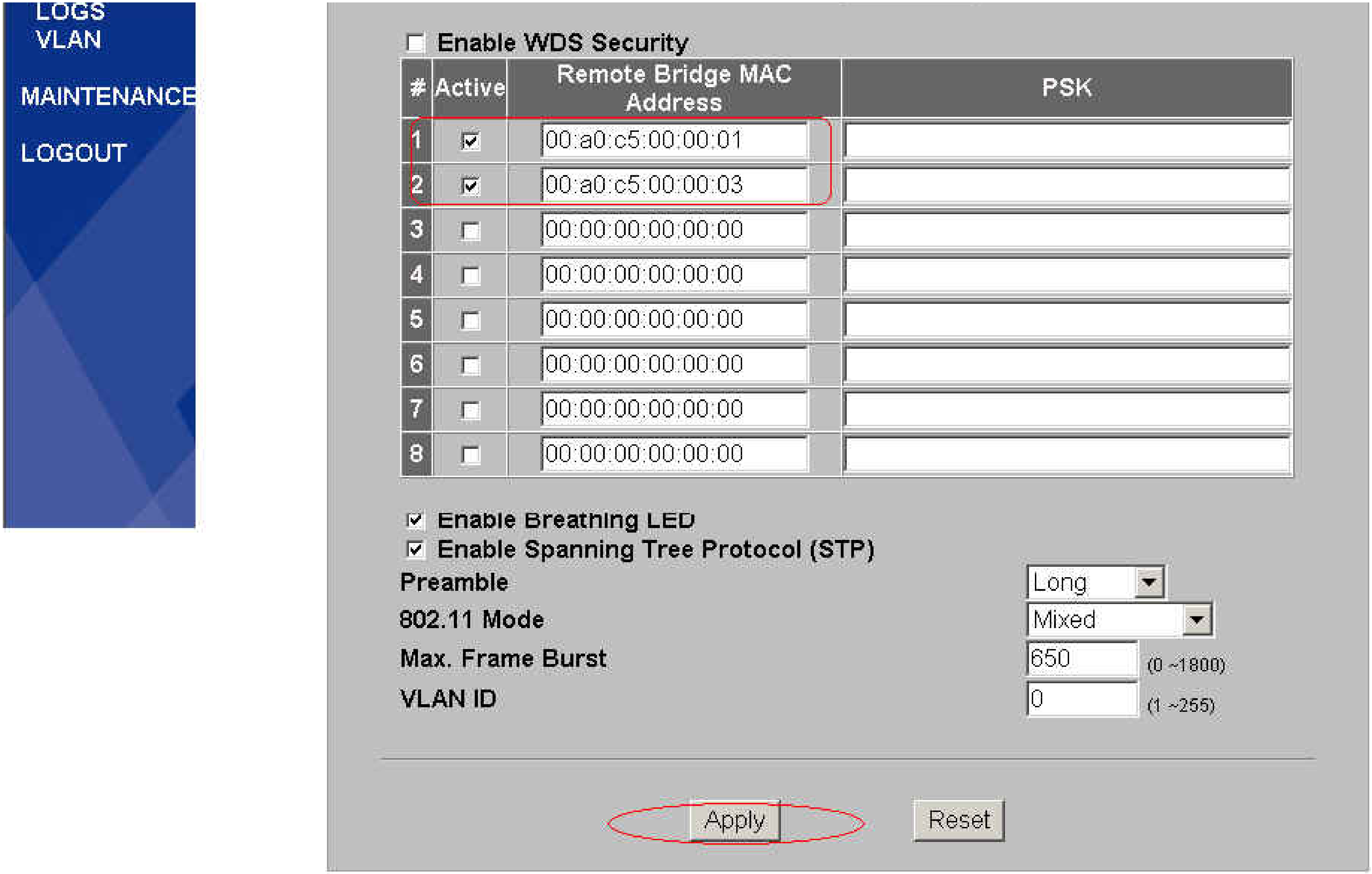


Operating Mode: Bridge/Repeater

Choose Channel ID: Channel-06 2437MHz or Scan

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)



□ Enable WDS Security

#	Active	Remote Bridge MAC Address	PSK
1	☑	00:a0:c5:00:00:01	
2	☑	00:a0:c5:00:00:03	
3	□	00:00:00:00:00:00	
4	□	00:00:00:00:00:00	
5	□	00:00:00:00:00:00	
6	□	00:00:00:00:00:00	
7	□	00:00:00:00:00:00	
8	□	00:00:00:00:00:00	

☑ Enable Breathing LED
☑ Enable Spanning Tree Protocol (STP)

Preamble	Long	
802.11 Mode	Mixed	
Max. Frame Burst	650	(0 ~1800)
VLAN ID	0	(1 ~255)

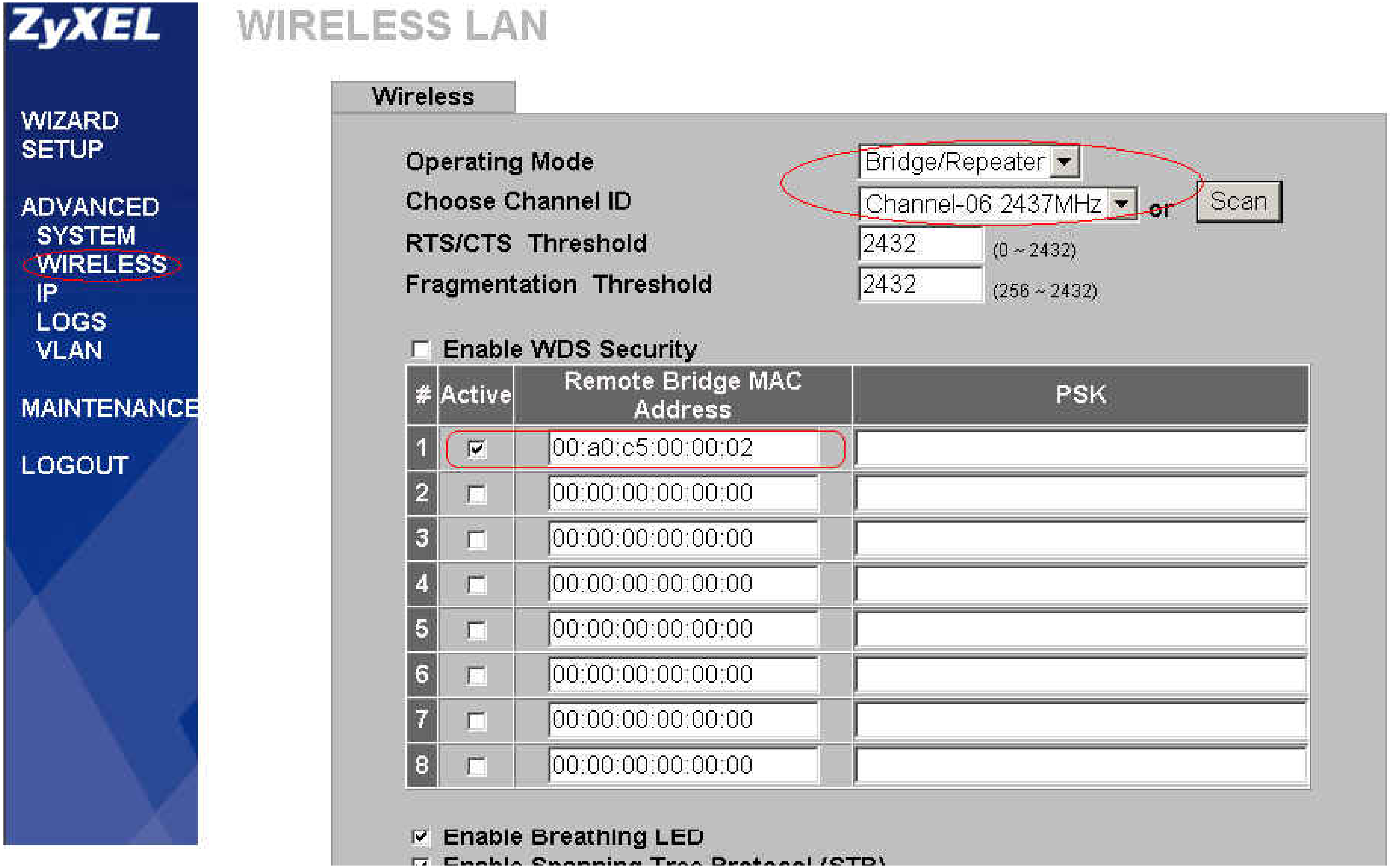
- ***Configuration for Wireless Station 3***

1. Click **Advanced** and **Wireless**.

2. Select **Bridge/Repeater** in the **Operation Mode** drop-down list box to display the screen as down.

3. Type the MAC address of peer device in the **Remote Bridge MAC Address** field, that is, six hexadecimal character pairs.

4. Click **Apply** to finish.



Operating Mode: Bridge/Repeater

Choose Channel ID: Channel-06 2437MHz or Scan

RTS/CTS Threshold: 2432 (0 ~ 2432)

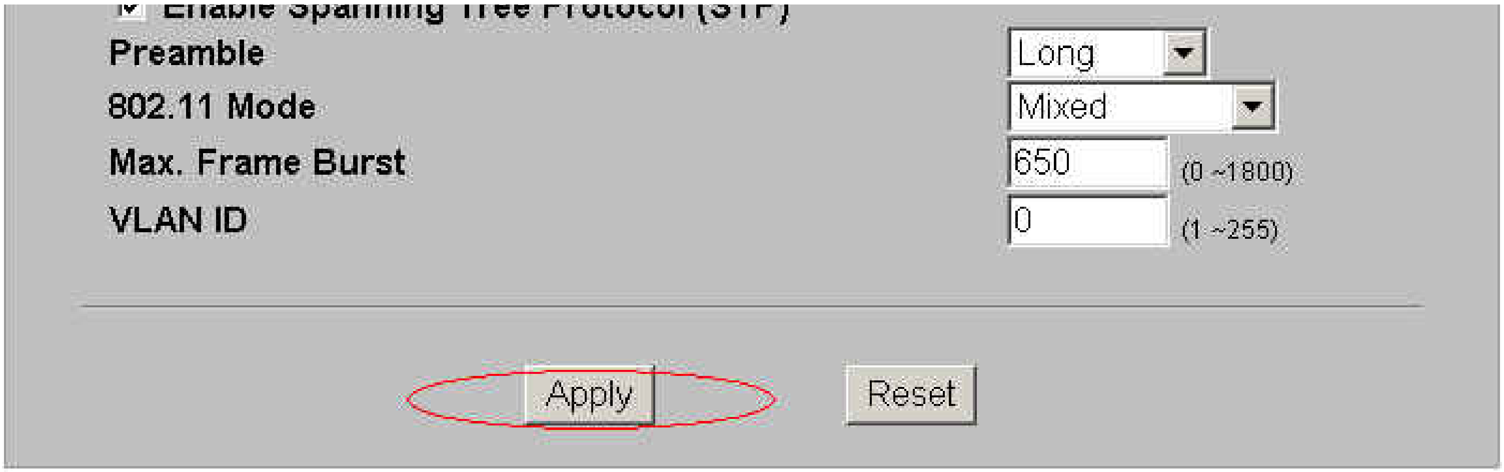
Fragmentation Threshold: 2432 (256 ~ 2432)

□ Enable WDS Security

#	Active	Remote Bridge MAC Address	PSK
1	☑	00:a0:c5:00:00:02	
2	□	00:00:00:00:00:00	
3	□	00:00:00:00:00:00	
4	□	00:00:00:00:00:00	
5	□	00:00:00:00:00:00	
6	□	00:00:00:00:00:00	
7	□	00:00:00:00:00:00	
8	□	00:00:00:00:00:00	

☑ Enable Breathing LED

☑ Enable Spanning Tree Protocol (STP)



☑ Enable Spanning Tree Protocol (STP)

Preamble: Long

802.11 Mode: Mixed

Max. Frame Burst: 650 (0 ~1800)

VLAN ID: 0 (1 ~255)

Configure Access Point as a AP + bridge/repeater mode

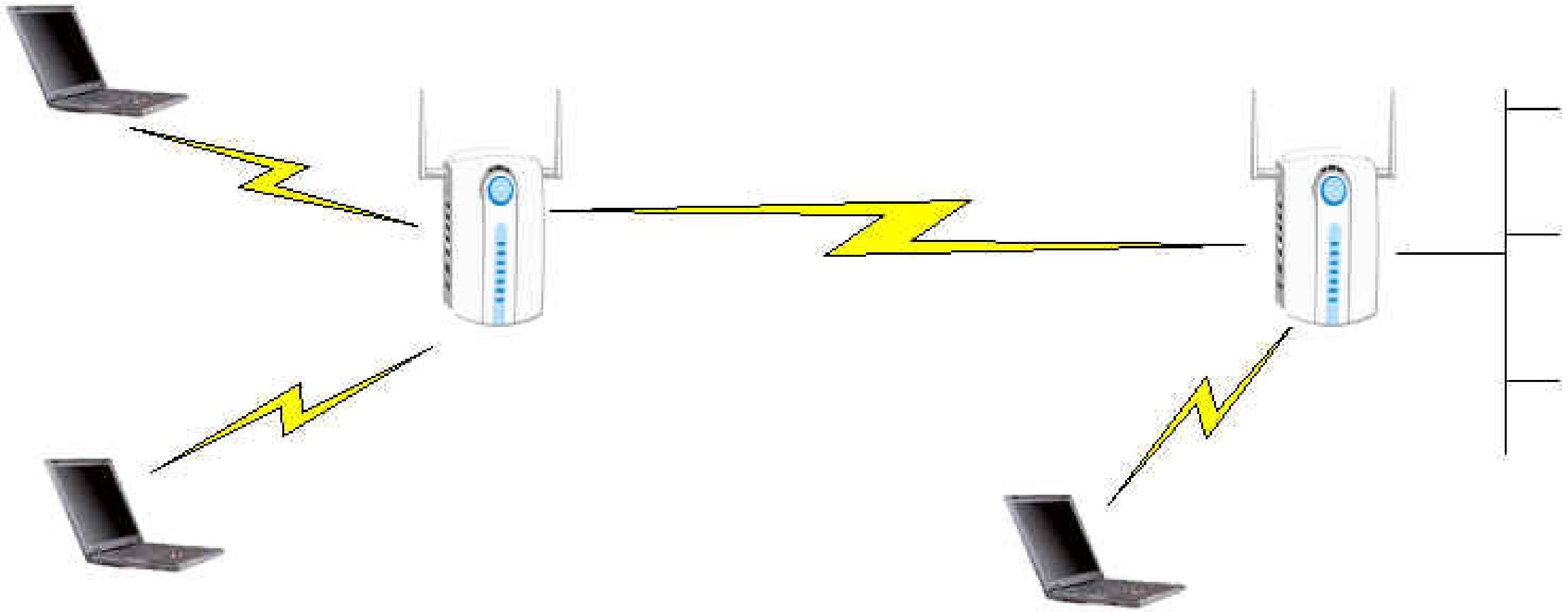
- ***Introduction***

What is AP+Bridge mode Functionality?

Wireless station can only associated with device in access point mode. If a device is configured in bridge/repeater mode it means the other peer is another bridge/ repeater not a wireless station. ZyXEL implement a new feature letting the Access point & bridge/repeater function mixed in the same device.

In AP+Bridge mode, the ZyAIR support both AP(the wireless station can connect to the wired network through AP) and bridge(two APs can communicate with one another) connection at the same time.

Note: When the ZyAIR is in AP+Bridge mode, the traffic between ZyAIRs(WDS) is not encrypted. The security settings on the ZyAIR refer to the traffic between the wireless station and the ZyAIR.



- ***Configuration for Wireless Station A***

1. Click **Advanced** and **Wireless**.

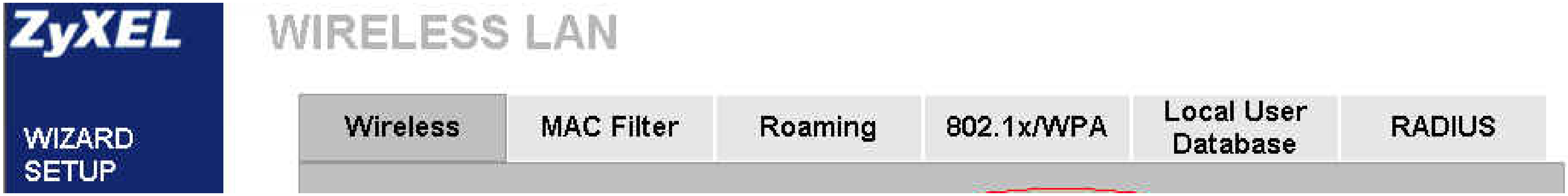
2. Select **AP+Bridge** in the **Operation Mode** drop-down list box to display the screen as down.

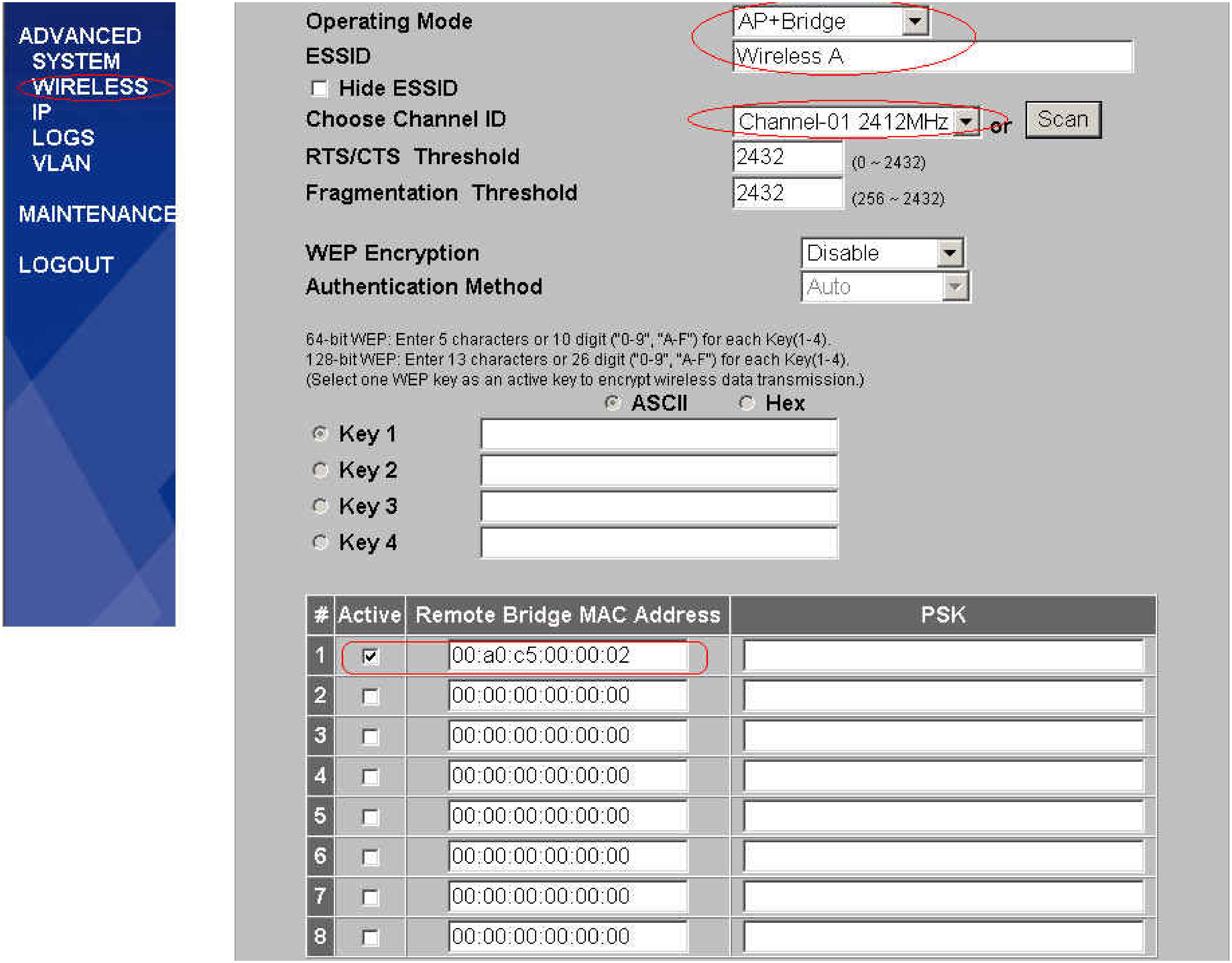
3. Type a name to identify the ZyAIR in the wireless LAN(up to 32 characters) as the **ESSID**.

4. Select the **Channel** in the **Choose Channel ID** field.

5. Type the MAC address of peer device in the **Remote Bridge MAC Address** field, that is, six hexadecimal character pairs.

6. Click **Apply** to finish.





Operating Mode: AP+Bridge

ESSID: Wireless A

□ Hide ESSID

Choose Channel ID: Channel-01 2412MHz or Scan

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

WEP Encryption: Disable

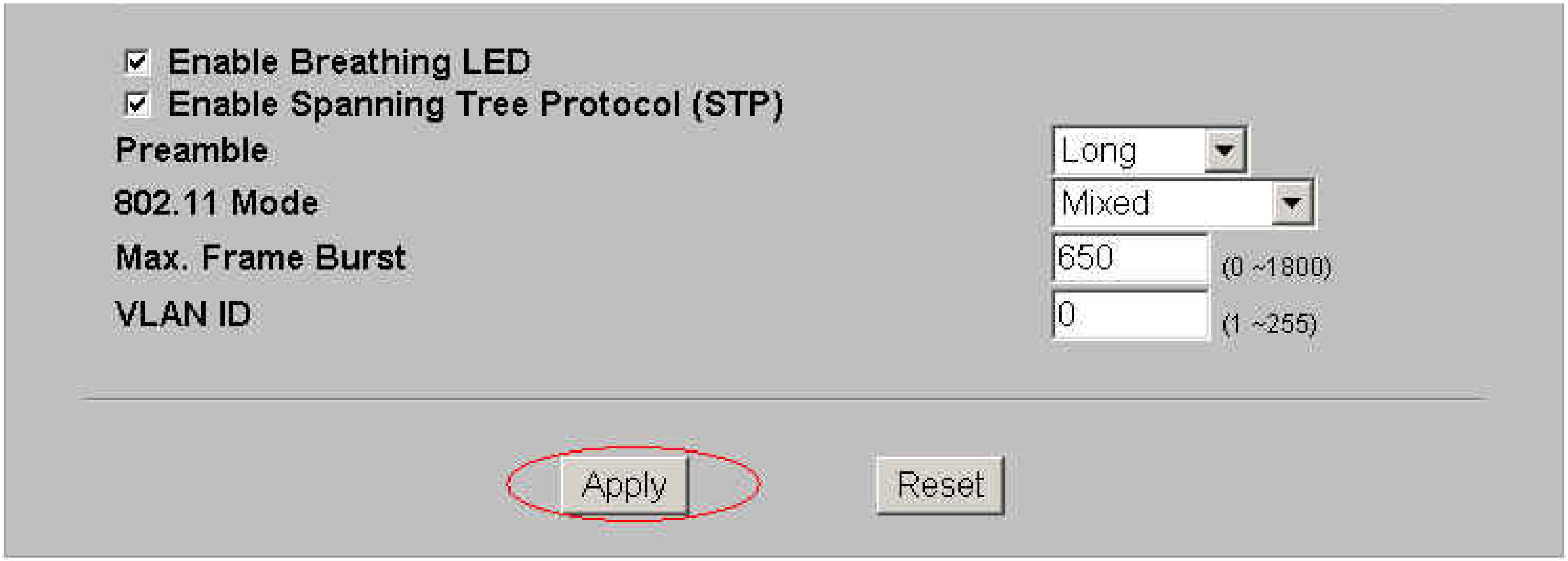
Authentication Method: Auto

64-bit WEP: Enter 5 characters or 10 digit ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 characters or 26 digit ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

● ASCII ○ Hex

● Key 1
○ Key 2
○ Key 3
○ Key 4

#	Active	Remote Bridge MAC Address	PSK
1	☑	00:a0:c5:00:00:02	
2	□	00:00:00:00:00:00	
3	□	00:00:00:00:00:00	
4	□	00:00:00:00:00:00	
5	□	00:00:00:00:00:00	
6	□	00:00:00:00:00:00	
7	□	00:00:00:00:00:00	
8	□	00:00:00:00:00:00	



☑ Enable Breathing LED

☑ Enable Spanning Tree Protocol (STP)

Preamble: Long

802.11 Mode: Mixed

Max. Frame Burst: 650 (0 ~1800)

VLAN ID: 0 (1 ~255)

- ***Configuration for Wireless Station B***

1. Click **Advanced** and **Wireless**.

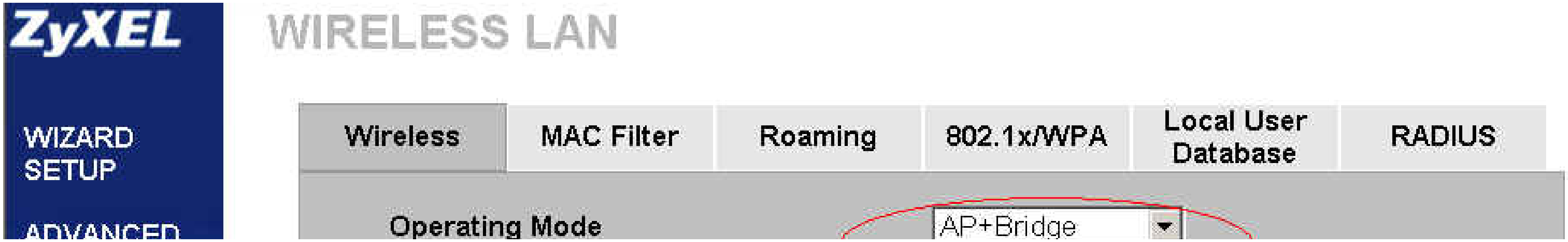
2. Select **AP+Bridge** in the **Operation Mode** drop-down list box to display the screen as down.

3. Type a name to identify the ZyAIR in the wireless LAN(up to 32 characters) as the **ESSID**.

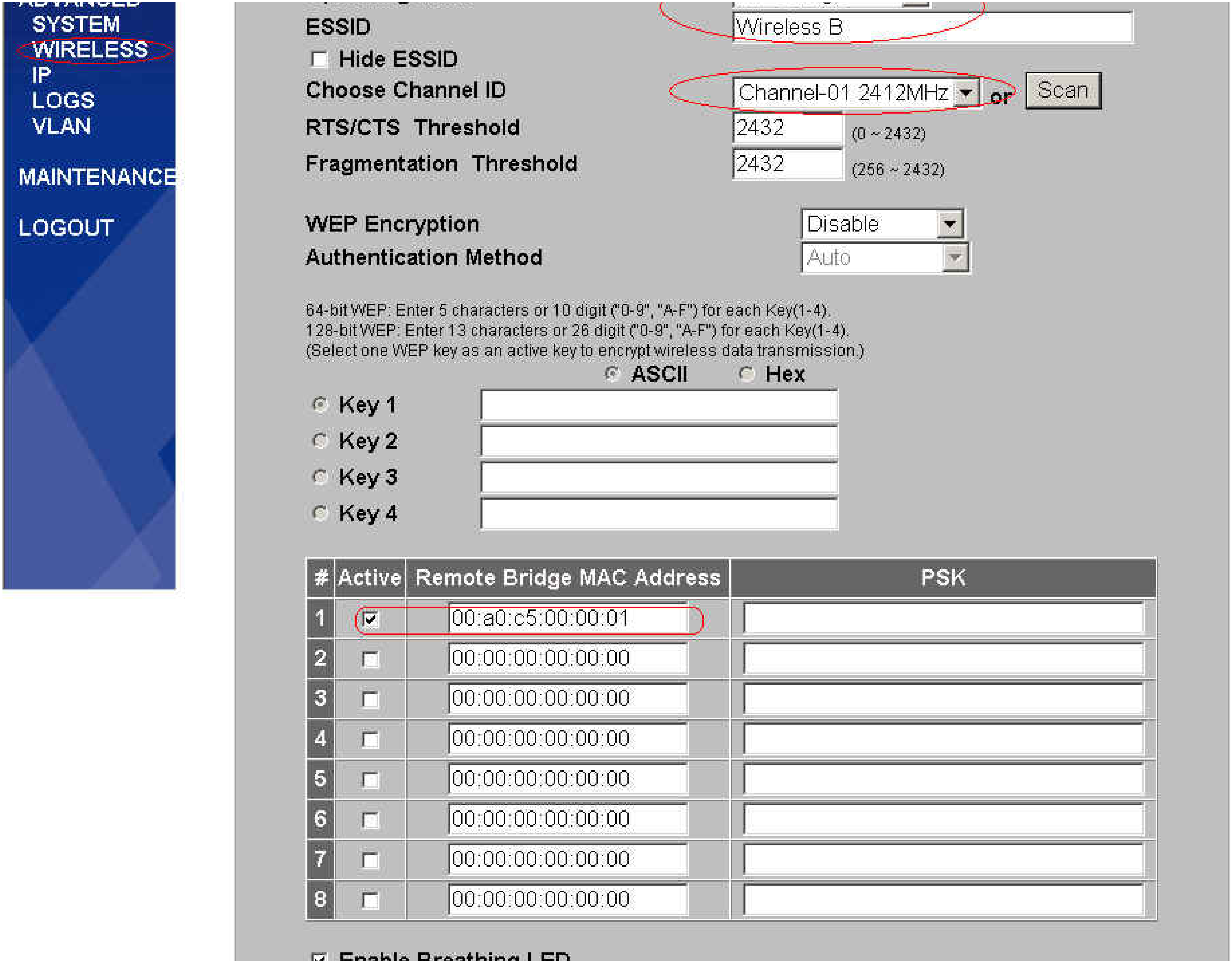
4. Select the **Channel** in the **Choose Channel ID** field.

5. Type the MAC address of peer device in the **Remote Bridge MAC Address** field, that is, six hexadecimal character pairs.

6. Click **Apply** to finish.



Operating Mode: AP+Bridge



SYSTEM
WIRELESS
IP
LOGS
VLAN

MAINTENANCE

LOGOUT

ESSID: Wireless B

□ Hide ESSID

Choose Channel ID: Channel-01 2412MHz or Scan

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

WEP Encryption: Disable

Authentication Method: Auto

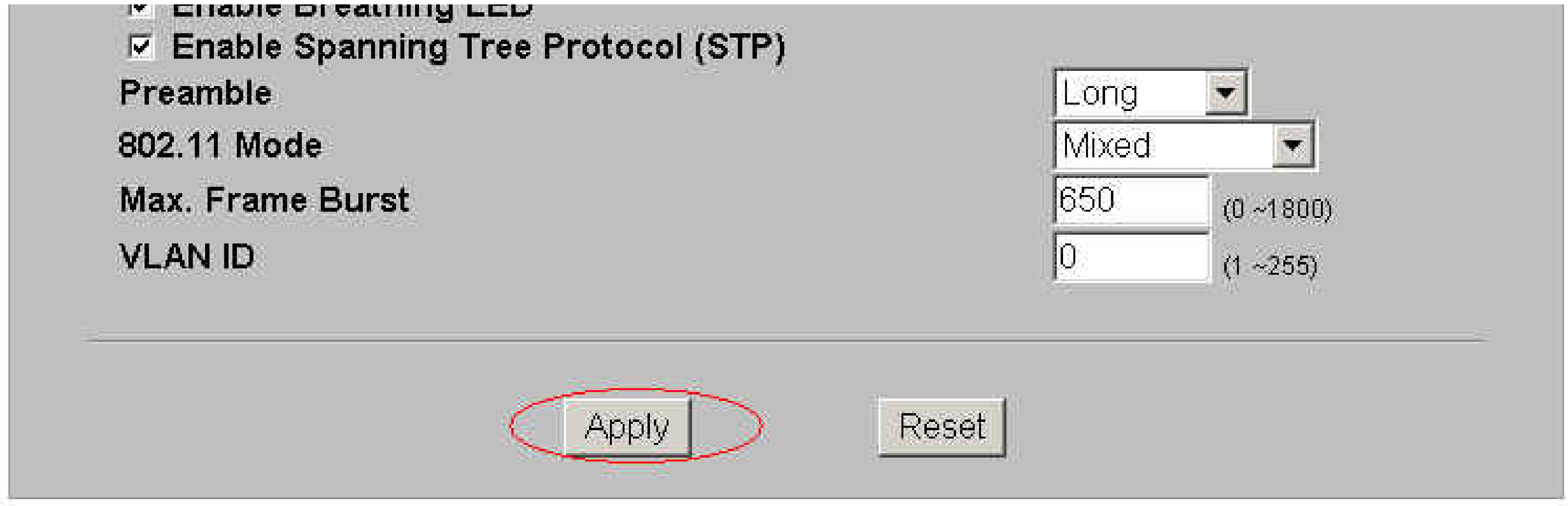
64-bit WEP: Enter 5 characters or 10 digit ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 characters or 26 digit ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

● ASCII ○ Hex

● Key 1
○ Key 2
○ Key 3
○ Key 4

#	Active	Remote Bridge MAC Address	PSK
1	☑	00:a0:c5:00:00:01	
2	□	00:00:00:00:00:00	
3	□	00:00:00:00:00:00	
4	□	00:00:00:00:00:00	
5	□	00:00:00:00:00:00	
6	□	00:00:00:00:00:00	
7	□	00:00:00:00:00:00	
8	□	00:00:00:00:00:00	

☑ Enable Breathing LED



☑ Enable Breathing LED

☑ Enable Spanning Tree Protocol (STP)

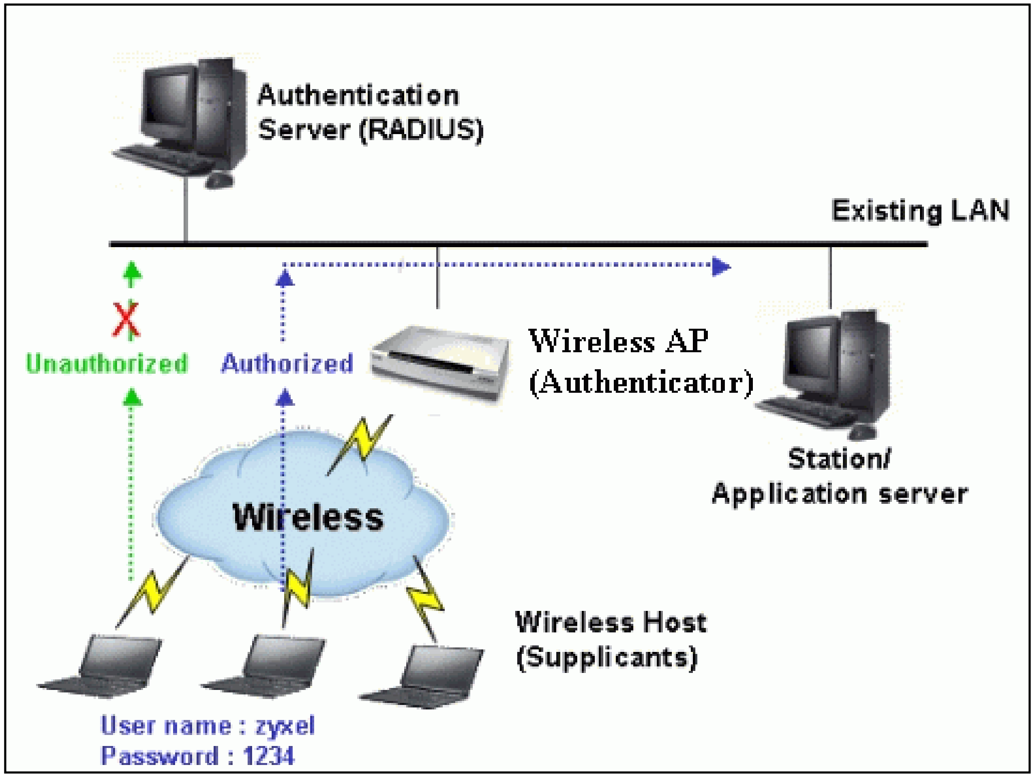
Preamble	Long	
802.11 Mode	Mixed	
Max. Frame Burst	650	(0 ~1800)
VLAN ID	0	(1 ~255)

Setup IEEE 802.1x Access Control (Authentication and Accounting)

Configure 802.1x and WPA

- ***IEEE 802.1x Introduction***

IEEE 802.1x port-based authentication is desired to prevent unauthorized devices (clients) from gaining access to the network. As LANs extend to hotels, airports, and corporate lobbies, insecure environments could be created. 802.1x port-based network access control makes use of the physical access characteristics of **IEEE 802 LAN infrastructures**, such as 802.3 Ethernet, 802.11 Wireless LAN and VDSL LRE (Long Reach Ethernet), 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 the authentication process fails.


Authentication Server (RADIUS)
Existing LAN
X
Unauthorized
Authorized
Wireless AP (Authenticator)
Station/ Application server
Wireless
Wireless Host (Supplicants)
User name : zyxel
Password : 1234

IEEE 802.1x authentication is a client-server architecture delivered with EAPOL (Extensible Authentication Protocol over LAN). The authentication server authenticates each client connected to a Access Point (For Wireless LAN) or switch port (for Ethernet) before accessing any services offered by the Wireless AP. 802.1x contains tree major components :

1. Authenticator :

The device (i.e. Wireless AP) facilitates authentication for the supplicant (Wireless client) attached on the Wireless network. Authenticator controls the physical access to the network based on the authentication status of the client. The authenticator acts as an intermediary (proxy) between the client and the authentication server (i.e. RADIUS server), requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client.

2. Supplicant :

The station (i.e. Wireless client) is being authenticated by an authenticator attached on the Wireless network. The supplicant requests access to the LAN services and responds to the requests from the authenticator. The station must be running 802.1x-compliant client software such as that offered in the Microsoft Windows XP operating system, Meeting House AEGIS 802.1x client and Odyssey 802.1x client.

3. Authentication Server :

The device (i.e. RADIUS server) provides an authentication service to an authenticator. This service determines, from the credentials provided by the supplicant, whether the supplicant is authorized to access the services provided by the authenticator. The authentication server performs the actual authentication of the client. It validates the identity of the supplicant. Because the authenticator acts as the proxy, the authentication service is transparent to the supplicant.

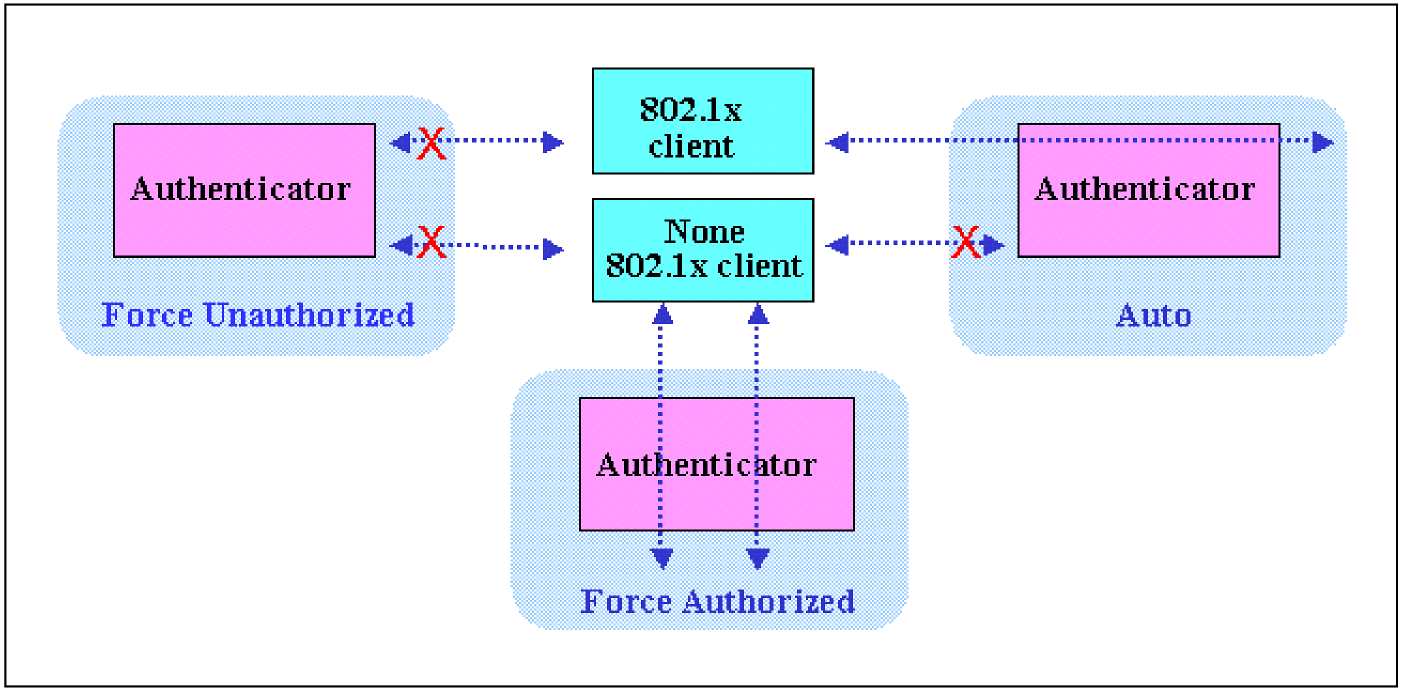
Some Wireless AP (i.e. ZyXEL Wireless AP) have built-in authentication server, external RADIUS authentication server is not needed. In this case, Wireless AP is acted as both authenticator and authentication server.

- ***Authentication Port State and Authentication Control***

The port state determines whether or not the supplicant (Wireless Client) is granted access to the network behind Wireless AP. There are two authentication port state on the AP, **authorized state** and **unauthorized state**.

By default, the port starts in the unauthorized state. While in this state, the port disallows all incoming and outgoing data traffic except for 802.1x packets. When a supplicant is successfully authenticated, the port transitions to the authorized state, allowing all traffic for the client to flow normally. If a client that does not support 802.1x is connected to an unauthorized 802.1x port, the authenticator requests the client’s identity. In this situation, the client does not respond to the 802.1x request, the port remains in the unauthorized state, and the client is not granted access to the network.

When 802.1x is enabled, the authenticator controls the port authorization state by using the following control parameters. The following three authentication control parameter are applied in Wireless AP.



1. Force Authorized : Disables 802.1x and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1x-based authentication of the client. This is the default port control setting. While AP is setup as **Force Authorized**, Wireless client (supported 802.1x client or none-802.1x client) can always access the network.

2. Force Unauthorized : Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The authenticator cannot provide authentication services to the supplicants through the port. While AP is setup as **Force Unauthorized**, Wireless clients (supported 802.1x client or none-802.1x client) never have the access for the network.

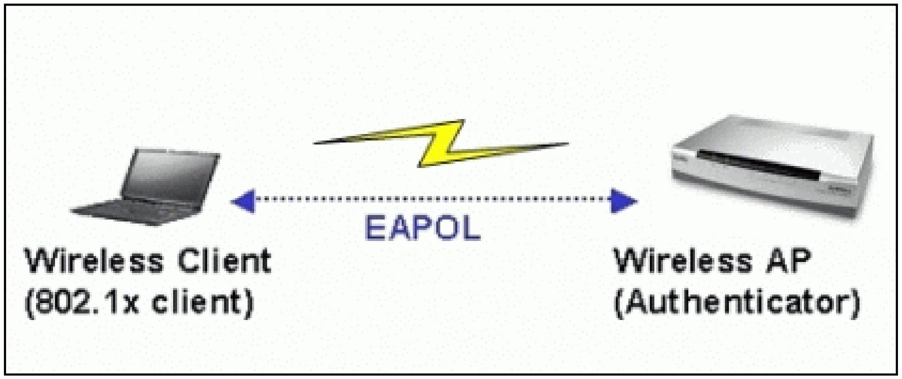
3. Auto : Enables 802.1x and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received requests the identity of the client and begins relaying authentication messages between supplicant and the authentication server. Each supplicant attempting to access the network is uniquely identified by the authenticator by using the client's MAC address. While AP is setup as **Auto**, only Wireless client supported 802.1x client can access the network.

- ***Re-Authentication***

The administrator can enable periodic 802.1x client re-authentication and specify how often it occurs. When re-authentication time out, Authenticator will send EAP-Request/ Identity to reinitiate authentication process.
In ZyXEL Wireless AP 802.1x implementation, if you do not specify a time period before enabling re-authentication, the number of seconds between re-authentication attempts is 1800 seconds (30 minutes).

- ***EAPOL (Extensible Authentication Protocol over LAN)***

Authenticators and supplicants communicate with one another by using the Extensible Authentication Protocol (EAP, RFC-2284). EAP was originally designed to run over PPP and to authenticate dial-in users, but 802.1x defines an encapsulation method for passing EAP packets over Ethernet frames. This method is referred to as **EAP over LANs, or EAPOL**. Ethernet type of EAPOL is **88-8E** , two octets in length. EAPOL encapsulations are described for IEEE 802 compliant environment, such as 802.3 Ethernet, 802.11 Wireless LAN and Token Ring/FDDI.

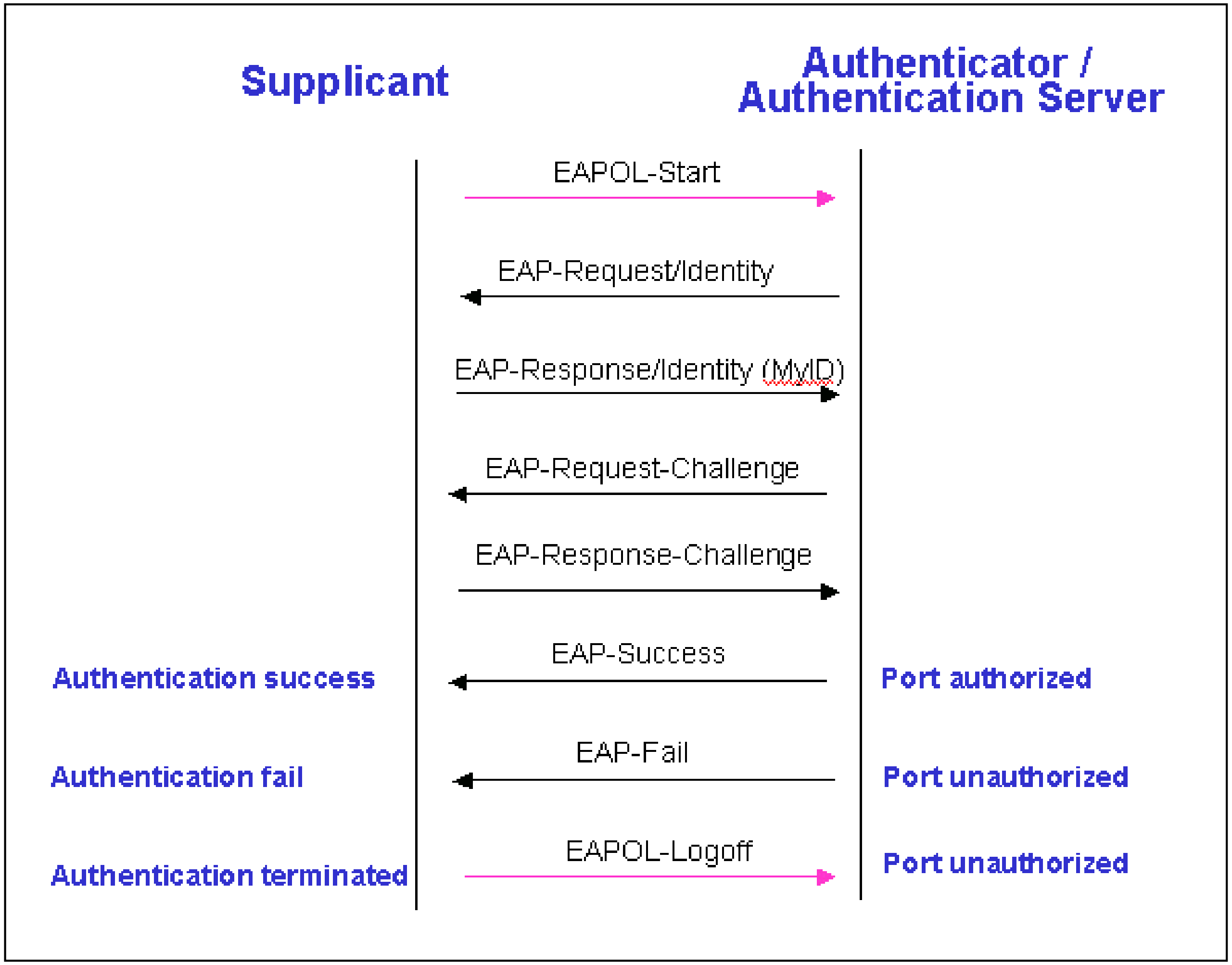


The EAP protocol can support multiple authentication mechanisms, such as MD5-challenge, One-Time Passwords, Generic Token Card, TLS and TTLS etc. Typically, the authenticator will send an initial Identity Request followed by one or more Requests for authentication information. When supplicant receive the EAP request, it will reply associated EAP response. So far, ZyXEL Wireless AP only supports MD-5 challenge authentication mechanism, but will support TLS and TTLS in the future.

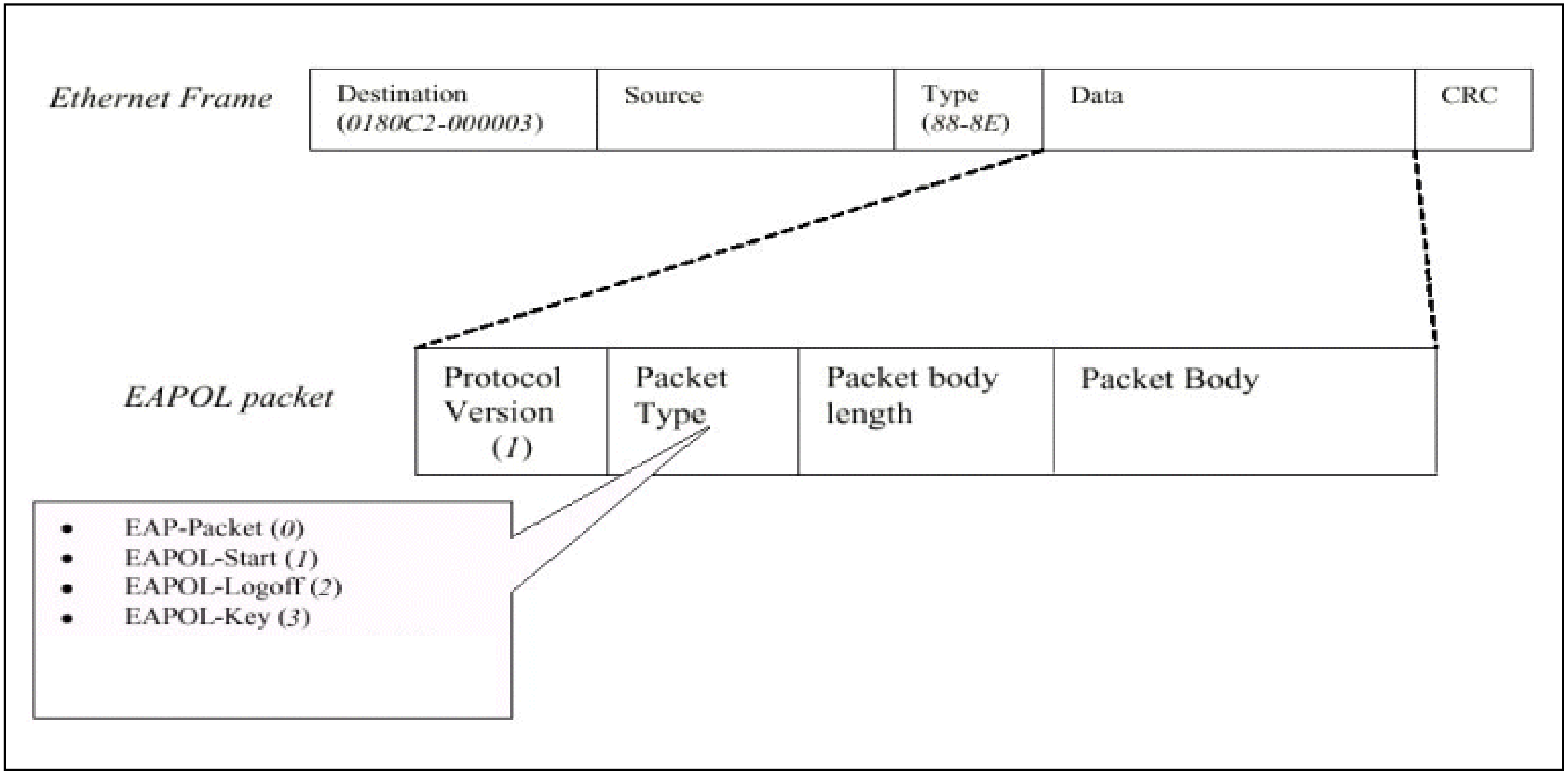
EAPOL Exchange between 802.1x Authenticator and Supplicant

The authenticator or the supplicant can initiate authentication. If you enable 802.1x authentication on the Wireless AP, the authenticator must initiate authentication when it determines that the Wireless link state transitions from down to up. It then sends an EAP-request/identity frame to the 802.1x client to request its identity (typically, the authenticator sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the supplicant responds with an EAP-response/identity frame.

However, if during bootup, the supplicant does not receive an EAP-request/identity frame from the Wireless AP, the client can initiate authentication by sending an **EAPOL-Start** frame, which prompts the switch to request the supplicant's identity. In above case, authenticator co-locate with authentication server. When the supplicant supplies its identity, the authenticator directly exchanges EAPOL to the supplicant until authentication succeeds or fails. If the authentication succeeds, the port becomes authorized. If the authentication fails, the port becomes unauthorized. When the supplicant does not need Wireless access any more, it sends **EAPOL-Logoff** packet to terminate its 802.1x session, the port state will become unauthorized. The following figure shows the EAPOL exchange ping-pong chart.



The EAPOL packet contains the following fields: protocol version, packet type, packet body length and packet body. Most of the fields are obvious. The packet type can have four different values, and these values are described below:



- EAP-Packet : Both the supplicant and the authenticator send this packet when authentication is taking place. This is the packet that contains either the MD5-Challenge or TLS information required for authentication.
- EAPOL-Start : This supplicant sends this packet when it wants to initiate the authentication process.
- EAPOL-Logoff : The supplicant sends this packet when it wants to terminate its 802.1x session.
- EAPOL-Key : This is used for TLS authentication method. The Wireless AP uses this packet to send the calculated WEP key to the supplicant after TLS negotiation has completed between the supplicant and the RADIUS server.

IEEE 802.1x Configuration in ZyXEL Wireless Access Point

- ***Enable 802.1x in AP***

When the IEEE 802.1x authentication is enabled, the wireless client must be authenticated by the ZyXEL AP before it can communicate on your network through ZyXEL AP. By default, the 802.1x function is disabled (Authentication Control= Force Authorized) to allow all wireless client. You can use SMT or Web Configuration to configure it.

Enter SMT Menu 23.4 to setup the 802.1x authentication control.

Menu 23.4 - System Security - IEEE802.1X

Wireless Port Control= **No Access Allowed/No Authentication Required/**

Authentication Required

ReAuthentication Timer (in second)= 1800
Idle Timeout (in second)= 3600

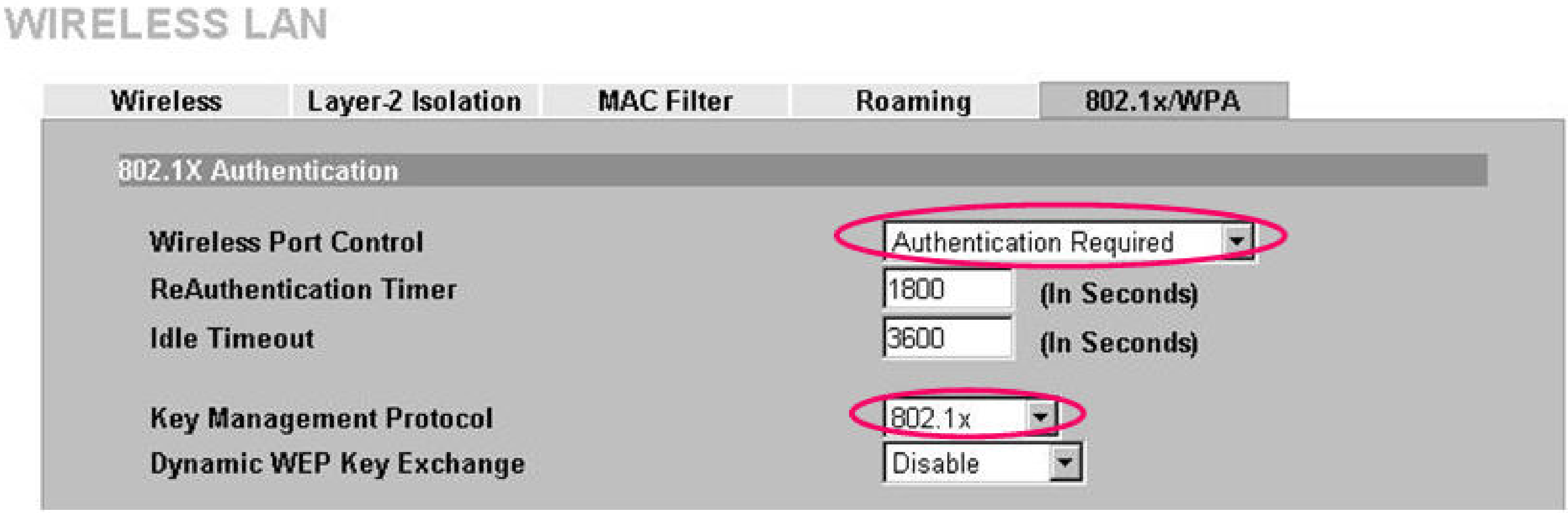
Key Management Protocol= **802.1x/WPA/WPA-PSK**

Key Settings :

Option	Descriptions
Wireless Port Control	To control wireless clients access to the wired network, select a control method from the drop-down list box. Choose from **No Authentication Required**, **Authentication Required** and **No Access Allowed**. **No Authentication Required** allows all wireless stations access to the wired network without entering usernames and passwords. This is the default setting. **Authentication Required** means that all wireless stations have to enter usernames and passwords before access to the wired network is allowed. **No Access Allowed** blocks all wireless stations access to the wired network. Select **Authentication Required** to configure **Key Management Protocol** and other related fields.
Key Management Protocol	Choose **802.1x** from the drop-down list.

If you use WEB Configuration,

1. From the Web Configurator main menu, go to **Main Menu->WIRELESS->802.1x/WPA**.
2. In the Wireless Port Control, select **Authentication Required** option.
3. In the Key Management Protocol, select **802.1x** to enable 802.1x authentication function.
4. Click **Apply** to make your setting work.



802.1X Authentication

Wireless Port Control: Authentication Required

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Key Management Protocol: 802.1x

Dynamic WEP Key Exchange: Disable

After 802.1x authentication function is enabled, you have to setup the authentication server, you may use **internal authentication server** inside ZyXEL wireless AP or **External RADIUS authentication server** or **Internal RADIUS authentication server**.

- ***Using Internal Authentication Server***

ZyXEL Wireless Access Point has an internal authentication server for authenticating the wireless 802.1x client users. It builds total 32-users database and allows up to 32 authorized users to login to the Wireless AP simultaneously. When you use internal authentication server, ZyXEL wireless AP is acted as Authenticator and Authentication Server.

By storing wireless 802.1x client profiles locally, your ZyXEL AP is able to authenticate wireless client without interacting with a extra network RADIUS server. Follow the steps to add user accounts on your ZyXEL AP.

1. From the SMT main menu, enter 14 to display Menu 14 Dial-in User Setup

```
                         Menu 14 - Dial-in User Setup

   1. support        9. ________   17. ________   25. ________
   2. ________      10. ________   18. ________   26. ________
   3. ________      11. ________   19. ________   27. ________
   4. ________      12. ________   20. ________   28. ________
   5. ________      13. ________   21. ________   29. ________
   6. ________      14. ________   22. ________   30. ________
   7. ________      15. ________   23. ________   31. ________
   8. ________      16. ________   24. ________   32. ________

                      Enter Menu Selection Number:
```

2. Type a number and press [Enter] to edit the wireless 802.1x client profile

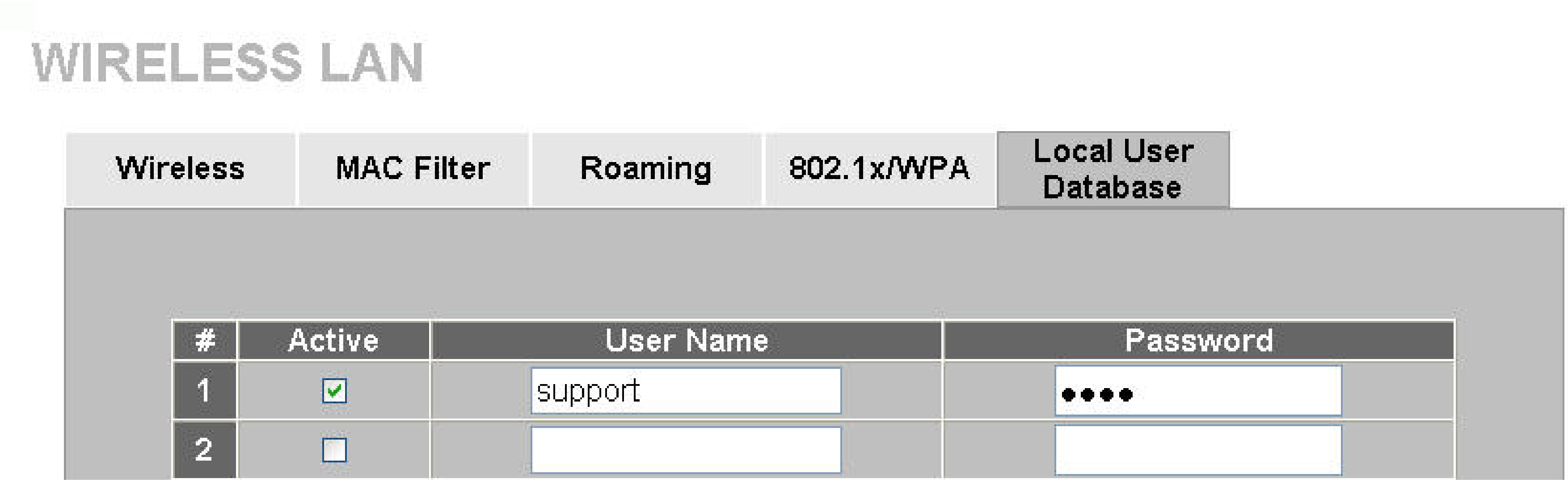
```
                    Menu 14.1 - Edit Dial-in User

                     User Name= support
                     Active= Yes
                     Password= ********

                Press ENTER to Confirm or ESC to Cancel:
```

Key settings :

Option	Descriptions
User Name	Enter a username up to 31 alphanumeric characters long.
Active	Press [SPACE BAR] to select **Yes** and press [Enter] to activate this 802.1x client profile.
Password	Enter a password up to 31 characters long.

If you use WEB Configurator,

1. From the Web Configurator main menu, go to **Main Menu->Wireless->Local User Database**.
2. Select one of the profile and fill in the **User Name** and **Password**, then click **Apply** to make your setting work.

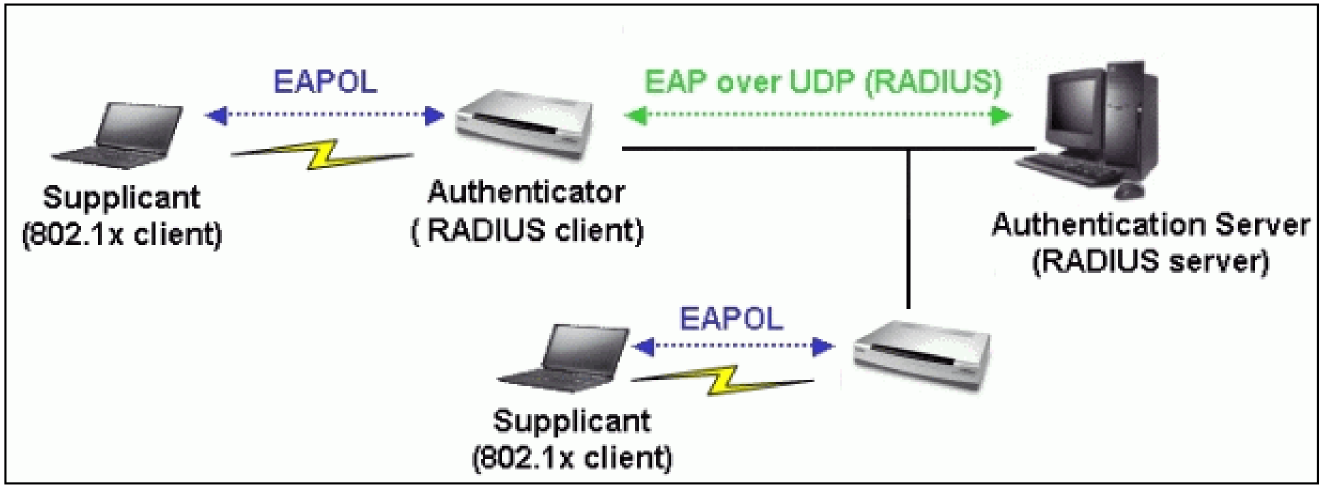


#	Active	User Name	Password
1	☑	support	●●●●
2	□		

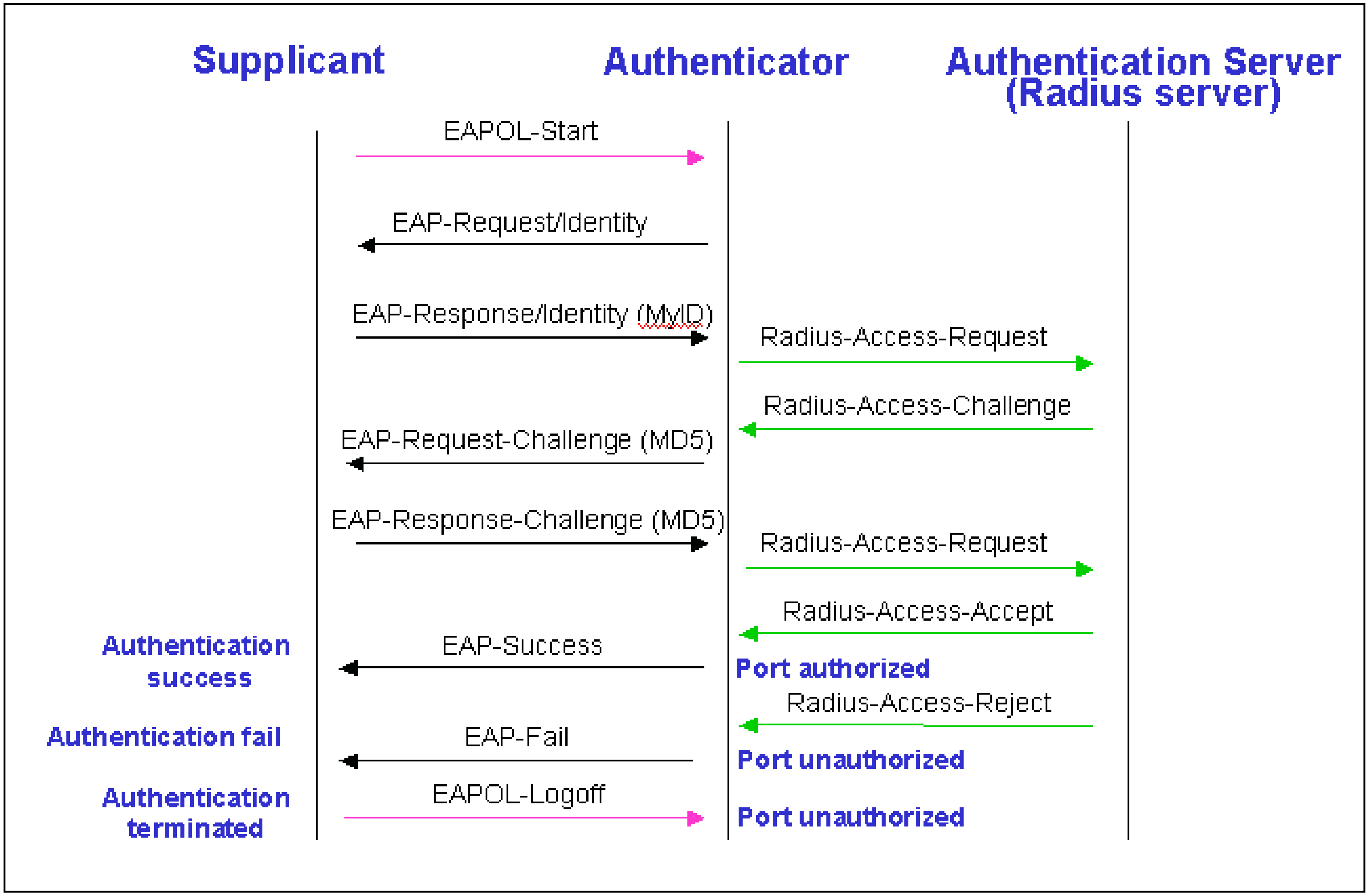
- ***Using External RADIUS Authentication Server***

In addition to the internal authentication server inside ZyXEL AP, you can use external RADIUS authentication server to centrally manage the user account profile. RADIUS is based on a client-server model that supports authentication, authorization and accounting. The wireless AP is the client and the server is the RADIUS server.

The authenticator includes the RADIUS client, which is responsible for encapsulating and decapsulating the Extensible Authentication Protocol (EAP) frames and interacting with the authentication server. When the authenticator receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the authenticator receives frames from the authentication server, the server’s frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the supplicant.



When the client supplies its identity, the authenticator begins its role as the intermediary, passing EAP frames between the supplicant and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized. The specific exchange of EAP frames depends on the authentication method being used. The figure below shows a message exchange initiated by the client using the MD5 Challenge authentication method with a RADIUS server.



1. From the SMT main menu, enter Menu 23.2 to setup System Security - RADIUS Server to setup the External RADIUS authentication server.

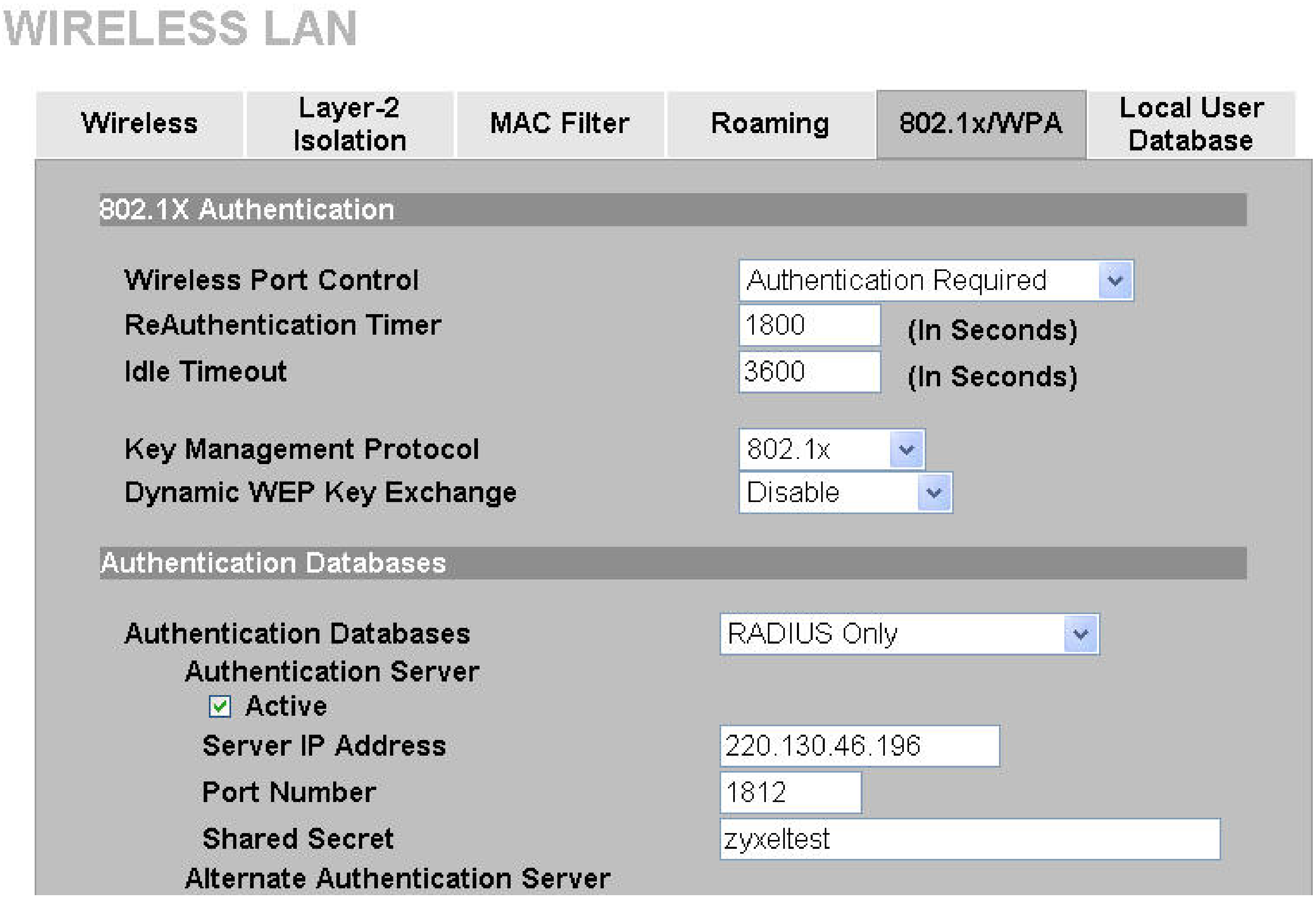
```
          Menu 23.2 - System Security - RADIUS Server

                    Authentication Server:
                       Active= Yes
                       Server Address= 220.130.46.196
                       Port #= 1812
                       Shared Secret= ********

                    Accounting Server:
                       Active= No
                       Server Address= 0.0.0.0
                       Port #= 1813
                       Shared Secret= ******

               Press ENTER to Confirm or ESC to Cancel:
```

Option	Descriptions
Active	Press [SPACE BAR] to select **Yes** and press [Enter] to enable 802.1x user authentication through an external RADIUS authentication server. Select **No** to enable authentication using ZyXEL AP internal authentication server.
Server Address	Enter the IP address of the external RADIUS authentication server.
Port	The default port of RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 31 characters) as the key to be shared between external RADIUS authentication server and ZyXEL AP (RADIUS client). The key is not send to the network. This key must be the same on the external RADIUS authentication server and ZyXEL AP.

2. If accounting is required, you must setup the external RADIUS accounting server. Normally, RADIUS authentication server and RADIUS accounting server are put in the same machine. However, they own separated UDP port and shared secret, you can separate authentication and accounting service in two different RADIUS servers. You can refer to RADIUS authentication configuration.

If you use WEB Configuration,

1. From the Web Configurator main menu, go to **Main Menu->WIRELESS->802.1x/WPA**.
2. On the "**Authentication Databases**" field, choose "**RADIUS Only**" option, and click **Active** check box.
3. After you've done the settings, click **Apply** to make your setting work.



WIRELESS LAN

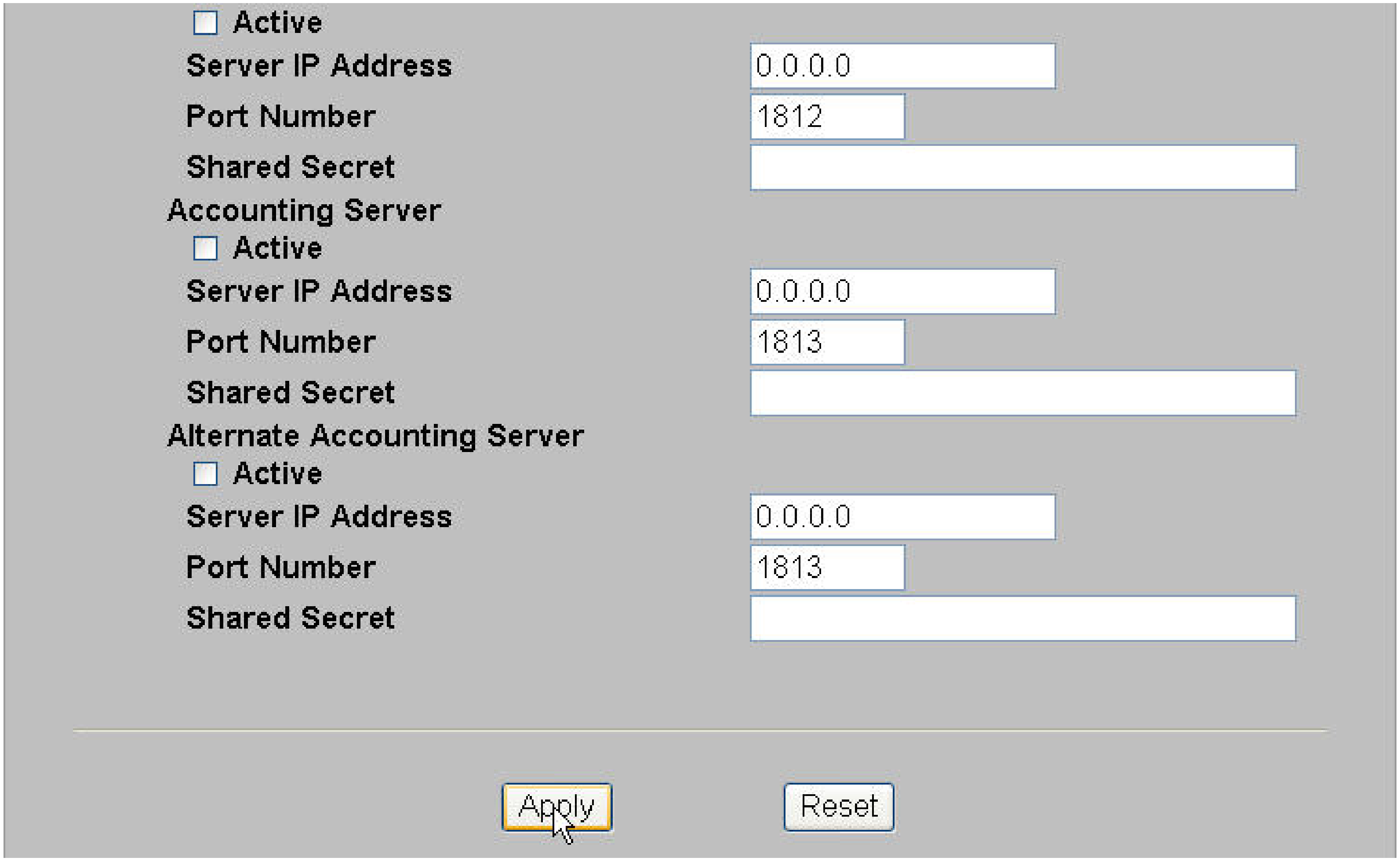
802.1X Authentication

Wireless Port Control: Authentication Required
ReAuthentication Timer: 1800 (In Seconds)
Idle Timeout: 3600 (In Seconds)

Key Management Protocol: 802.1x
Dynamic WEP Key Exchange: Disable

Authentication Databases

Authentication Databases: RADIUS Only
Authentication Server
☑ Active
Server IP Address: 220.130.46.196
Port Number: 1812
Shared Secret: zyxeltest
Alternate Authentication Server



□ Active

Server IP Address 0.0.0.0

Port Number 1812

Shared Secret

Accounting Server

□ Active

Server IP Address 0.0.0.0

Port Number 1813

Shared Secret

Alternate Accounting Server

□ Active

Server IP Address 0.0.0.0

Port Number 1813

Shared Secret

Key settings for External Authentication Server:

Field	Description
External RADIUS Server	Select the radio button to use an External RADIUS Server to authenticate the ZyAIR’s wireless clients.
Authentication Server	
Active	Select the check box to enable user authentication through an external authentication server.
Server IP Address	Type the IP address of the external authentication server in dotted decimal notation.
Port Number	Type the port number of the external authentication server. The default port number is 1812. You need not change this value unless your network administrator instructs you to do so with additional information.

Shared Secret	Type a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyAIR. The key must be the same on the external authentication server and your ZyAIR. The key is not sent over the network.
Alternate Authentication Server	If the ZyAIR cannot authenticate wireless users using the Authentication Server, the Alternate Authentication Server is used. The ZyAIR will attempt to authenticate three times before using the Alternate Authentication Server. Requests can be issued from the client interface to use the alternate authentication server. The length of time for each authentication is decided by the wireless client or based on the configuration of the ReAuthentication Timer field in the 802.1x/WPA screen.

- ***Using Internal RADIUS Authentication Server***

1. From the SMT main menu, enter Menu 23.2 to setup System Security - RADIUS Server to setup the Internal RADIUS authentication server.

```
          Menu 23.2 - System Security - RADIUS Server

                 Authentication Server:
                    Active= Yes
                    Server Address= 127.0.0.1
                    Port #= 1812
                    Shared Secret= *****

                 Accounting Server:
                    Active= Yes
                    Server Address= 192.168.1.100
                    Port #= 1813
                    Shared Secret= ******

              Press ENTER to Confirm or ESC to Cancel:
```

Key settings for authentication server:

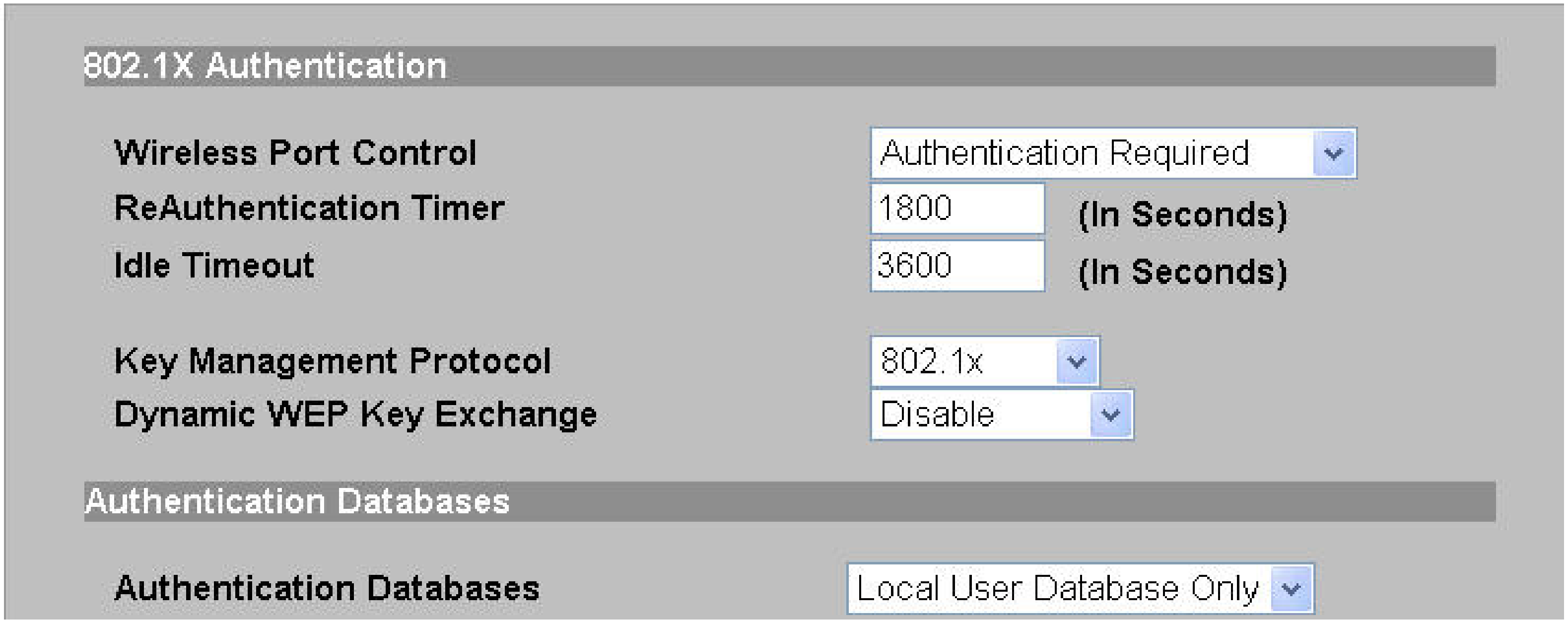
Option	Descriptions

Active	Press [SPACE BAR] to select **Yes** and press [Enter] to enable 802.1x user authentication through an external RADIUS authentication server. Select **No** to enable authentication using ZyXEL AP internal authentication server.
Server Address	You must enter **127.0.0.1** IP address to enable the Internal RADIUS Server option.
Port	If you use Internal RADIUS Server , you should set the default port of the RADIUS server.
Shared Secret	If you use Internal RADIUS Server , keep the default settings in it.

Note : If you use SMT menu to do the settings, you can't choose authentication type and Dynamic WEP Key Exchange settings, you can only use the default settings.

If you use WEB Configuration,

1. From the Web Configurator main menu, go to **Main Menu**->**WIRELESS**->**802.1x**.
2. On the **Authentication Databases field,** choose **Local User Database Only**.
3. After you've done the settings, click **Apply** to make your setting work.



802.1X Authentication

Wireless Port Control: Authentication Required

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Key Management Protocol: 802.1x

Dynamic WEP Key Exchange: Disable

Authentication Databases

Authentication Databases: Local User Database Only

Configure 802.1x and WPA

- ***Introduction***

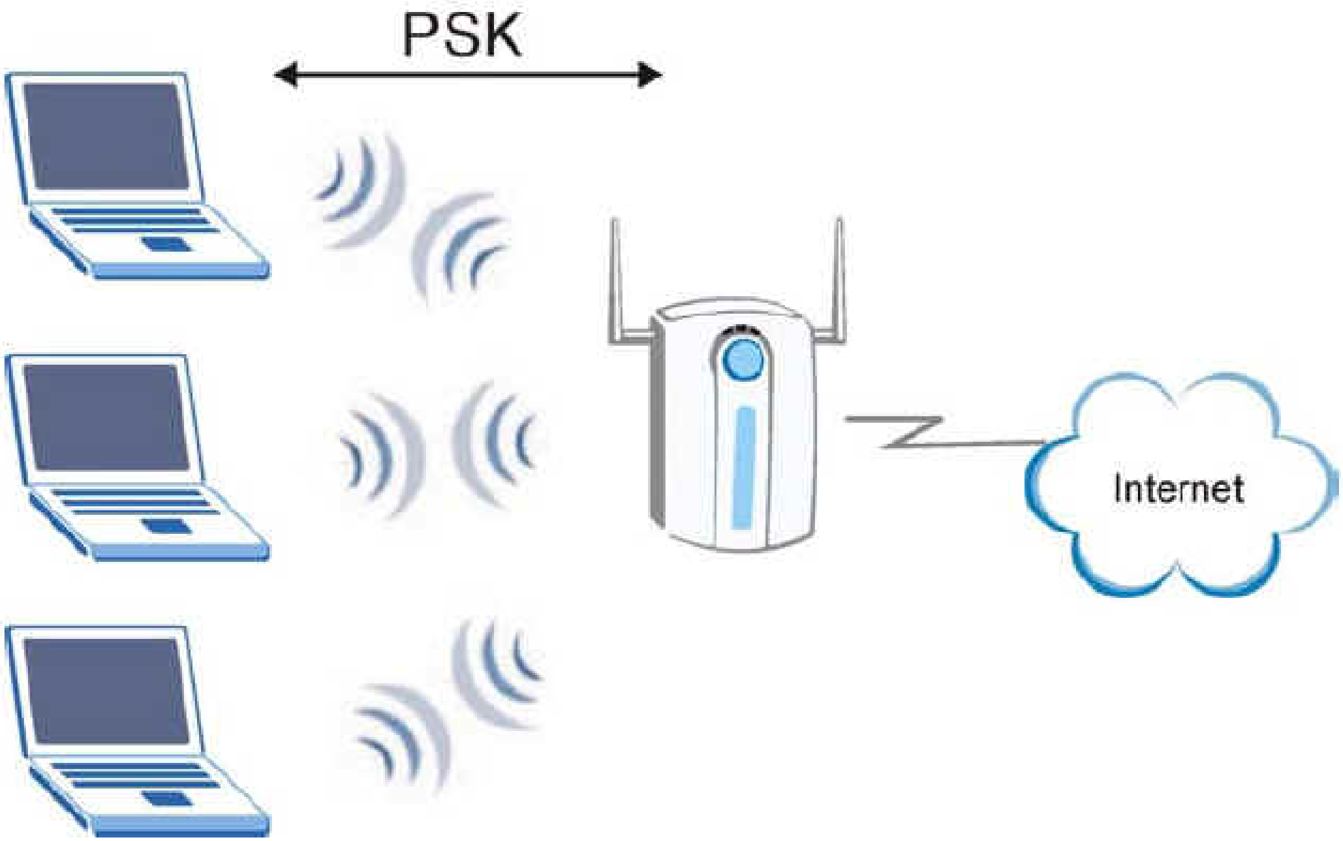
What is WPA Functionality?

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. Key differences between WAP and WEP are user authentication and improved data encryption WAP applies IEEE 802.1x Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. You can not use the ZyAIR's local user database for WPA authentication purpose since the local user database uses MD5 EAP which can not to generate keys.

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check and IEEE 802.1x. Temporal Key Integrity Protocol uses 128-bits keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extend initialization vector (IV) with sequencing rules and a re-keying mechanism.

If you do not have an external RADIUS, server, you should use WPA-PSK (WPA Pre-Share Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the password match, a client will be granted access to a WLAN.

Here comes **WPA-PSK Application example** for your reference.



- ***Configuration for Access point***

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication cabn be done using local user database internal to the ZyAIR (authenticate up to 32 users) or an external RADIUS server for an unlimited number of users.

1. To change your ZyAIR's authentication settings, click the wireless **Wireless** link under Advanced.

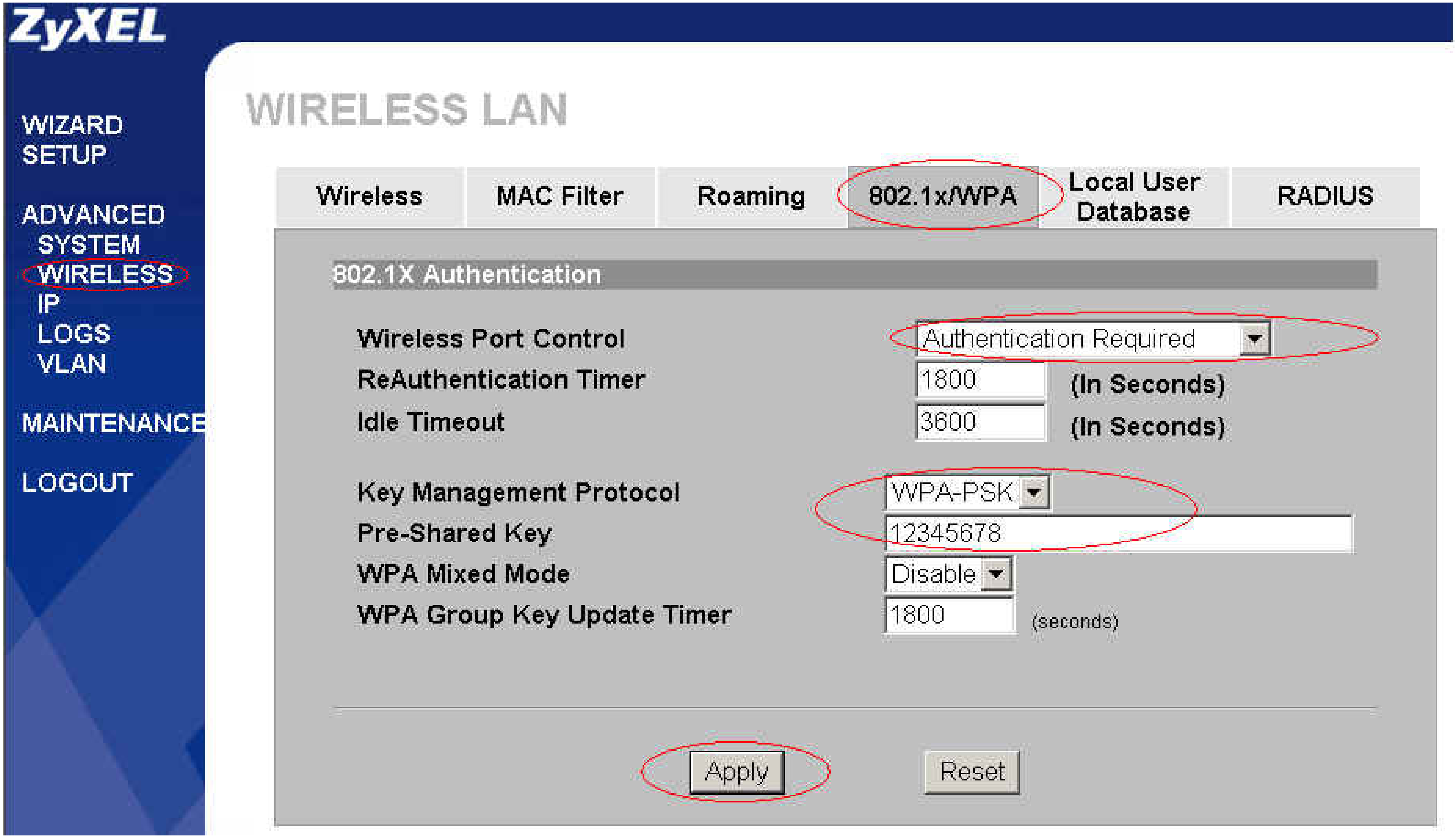
2. Select **802.1x/WPA** tab.

3. choose **Authentication Required** from the **Wireless Port Control.**

4. Select the **WAP-PSK** in the **Key Management Protocol** field.

5. Type the Pre Shared Key in the **Pre-Shared Key** field.

6**.** Click **Apply** to finish.



WIRELESS LAN

802.1X Authentication

Wireless Port Control: Authentication Required

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Key Management Protocol: WPA-PSK

Pre-Shared Key: 12345678

WPA Mixed Mode: Disable

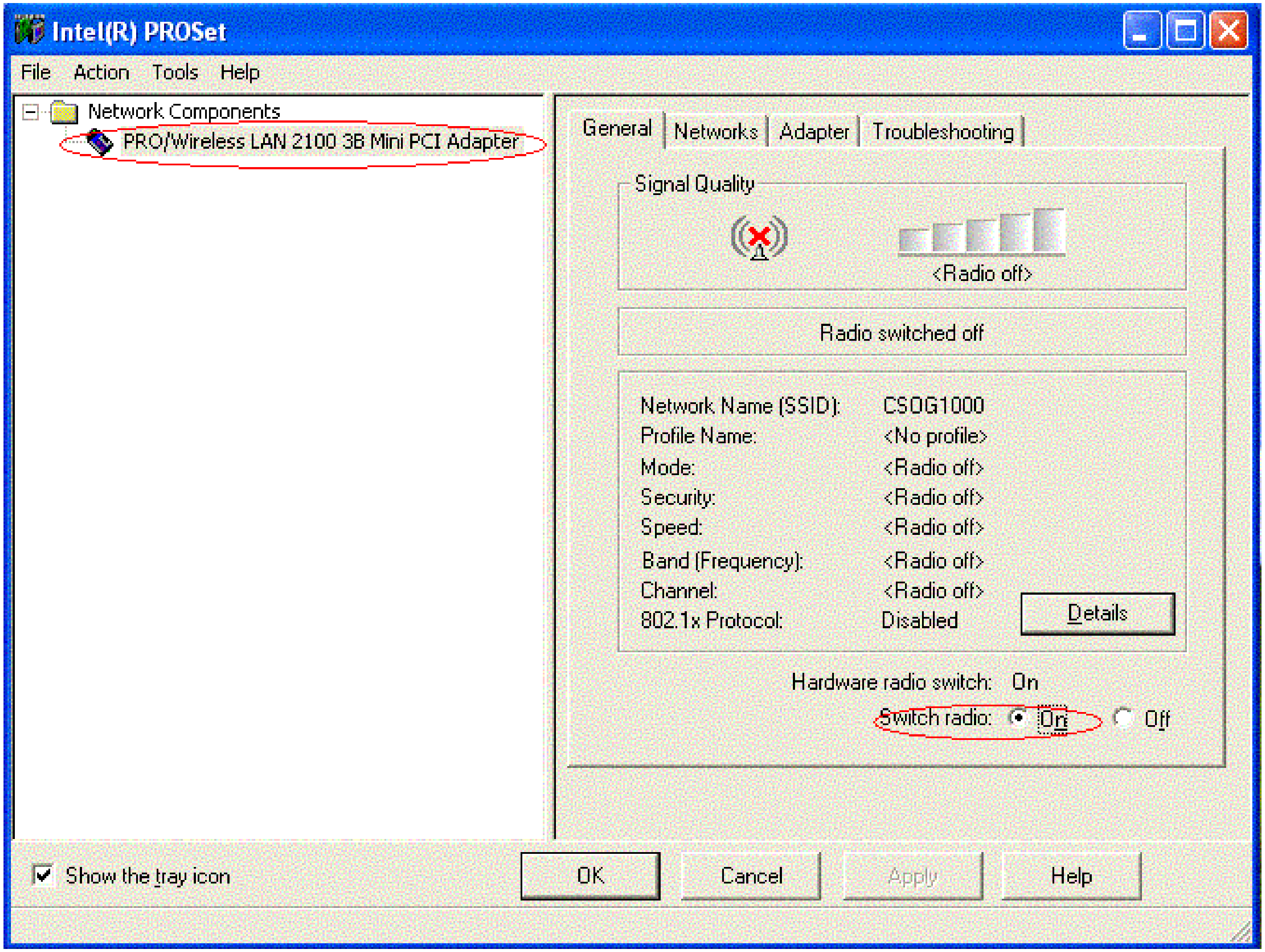
WPA Group Key Update Timer: 1800 (seconds)

- ***Configuration for your PC***

1. Double click on your wireless utility icon(here is the Centrion on Windows XP) in your windows task bar the utility will pop up on your windows screen.

2. Select the **wireless card** that you want to configure.

3. Select **on** from the Switch Radio.



Radio switched off

Network Name (SSID): CSOG1000
Profile Name: <No profile>
Mode: <Radio off>
Security: <Radio off>
Speed: <Radio off>
Band (Frequency): <Radio off>
Channel: <Radio off>
802.1x Protocol: Disabled

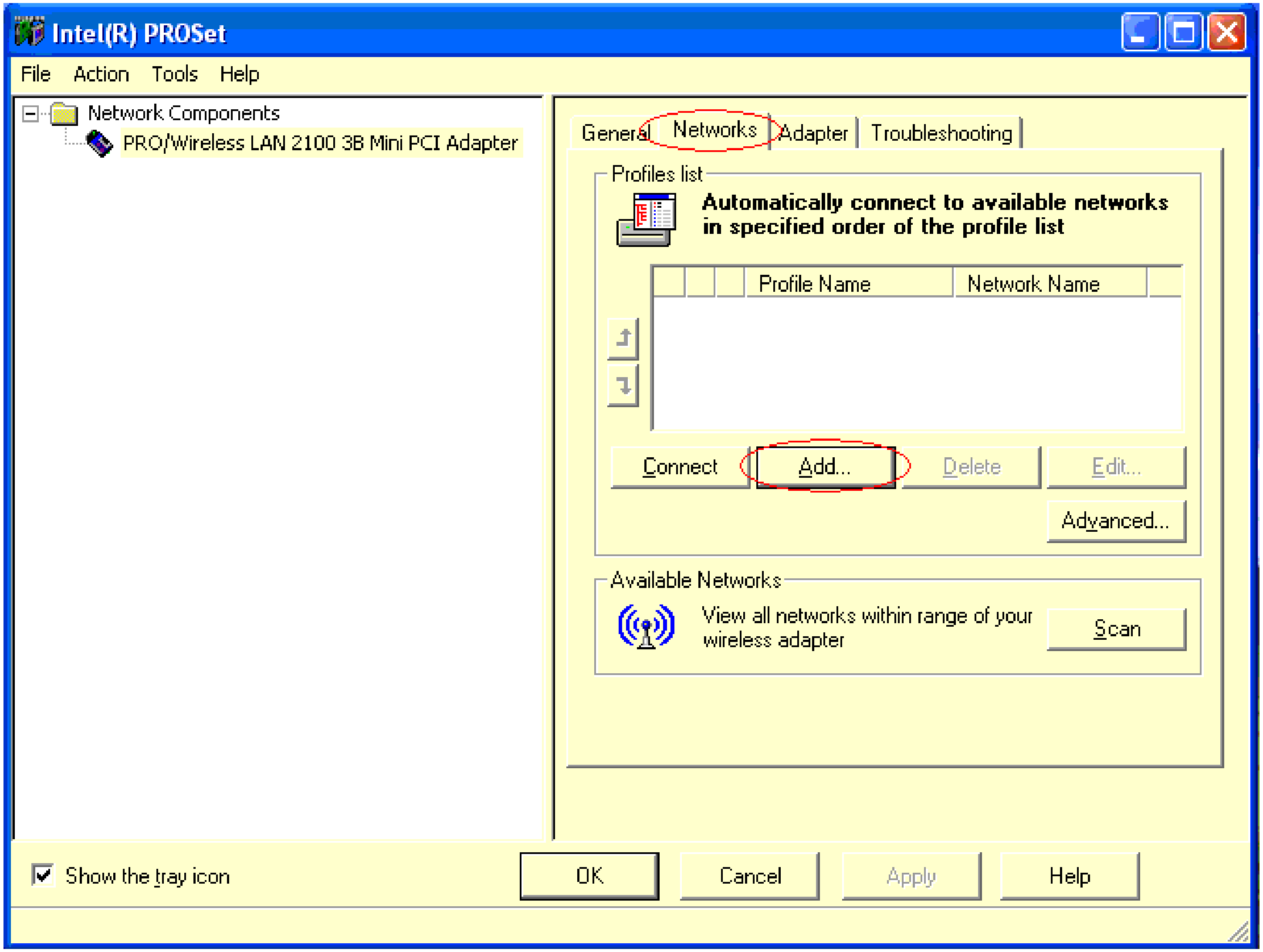
Hardware radio switch: On

Switch radio: ● On ○ Off

☑ Show the tray icon

4. choose **Network** option.

5. **Add** a new wireless profile.



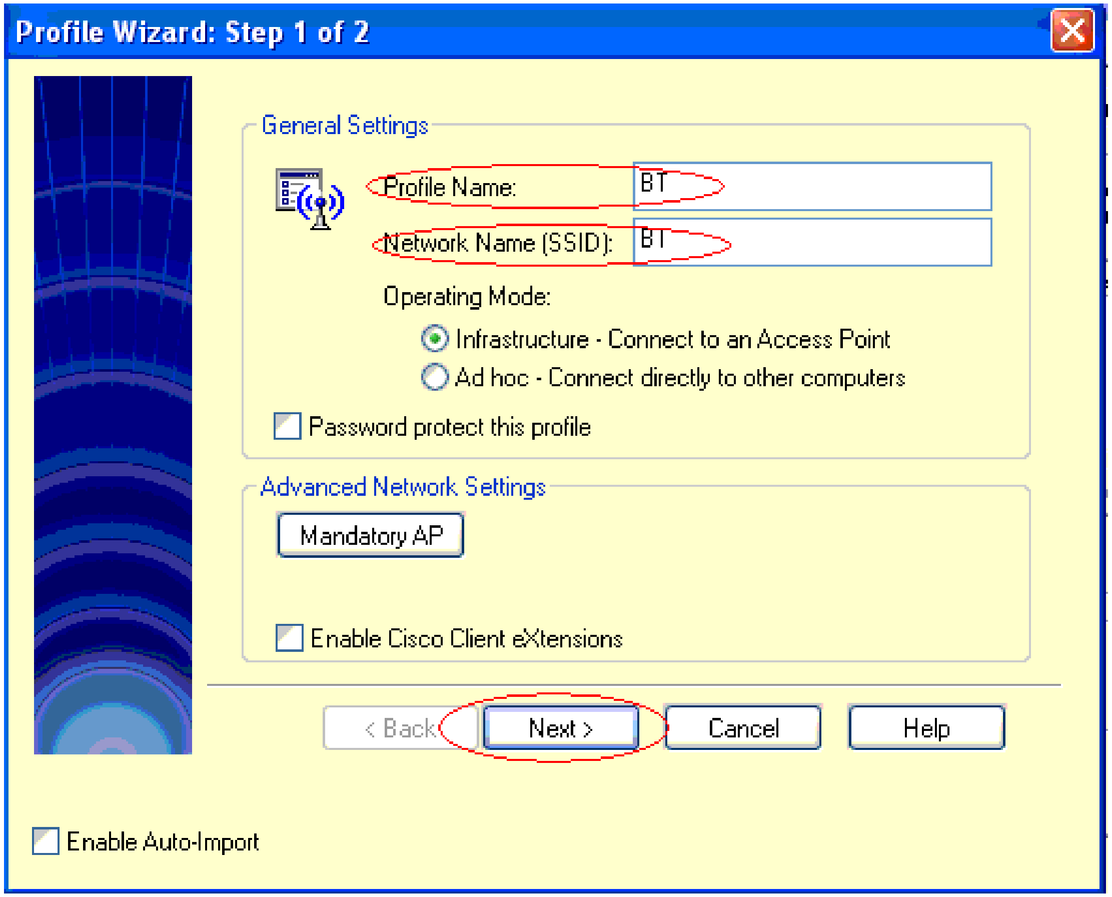
Automatically connect to available networks in specified order of the profile list

View all networks within range of your wireless adapter

☑ Show the tray icon

6. Type the **Profile Name** and **Network Name (SSID)** in the field.

7. Click **Next** button.



Profile Wizard: Step 1 of 2

General Settings

Profile Name: BT

Network Name (SSID): BT

Operating Mode:

● Infrastructure - Connect to an Access Point

○ Ad hoc - Connect directly to other computers

□ Password protect this profile

Advanced Network Settings

□ Enable Cisco Client eXtensions

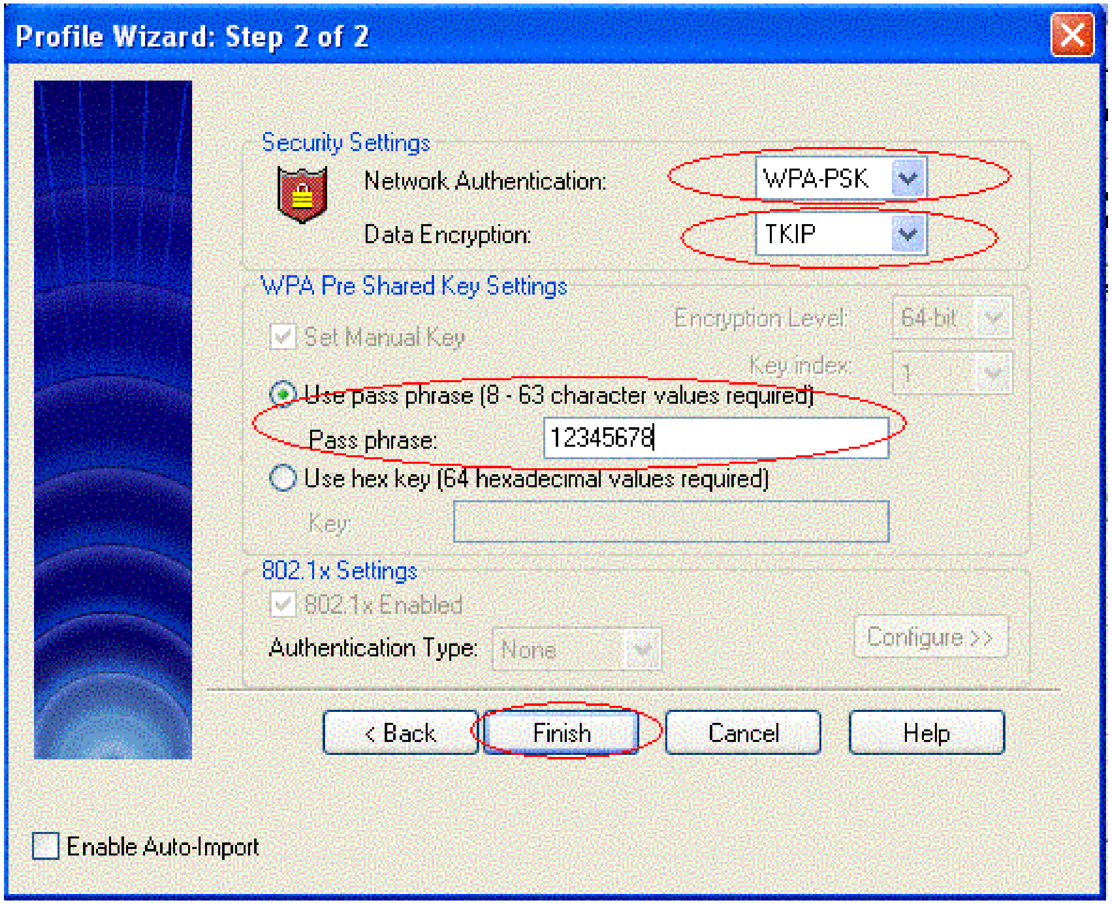
□ Enable Auto-Import

8. Select **WPA-PSK** from the **Network Authentication** field.

9. Select **TKIP** from the **Data Encryption** field.

10. Type the **Pre Share Key** (8-63 character) in the **Pass phrase** field.

11. Click **Finish** to exit the **Profile Wizard** screen.



Profile Wizard: Step 2 of 2

Security Settings

Network Authentication: WPA-PSK

Data Encryption: TKIP

WPA Pre Shared Key Settings

☑ Set Manual Key

Encryption Level: 64-bit

Key index: 1

● Use pass phrase (8 - 63 character values required)

Pass phrase: 12345678

○ Use hex key (64 hexadecimal values required)

Key:

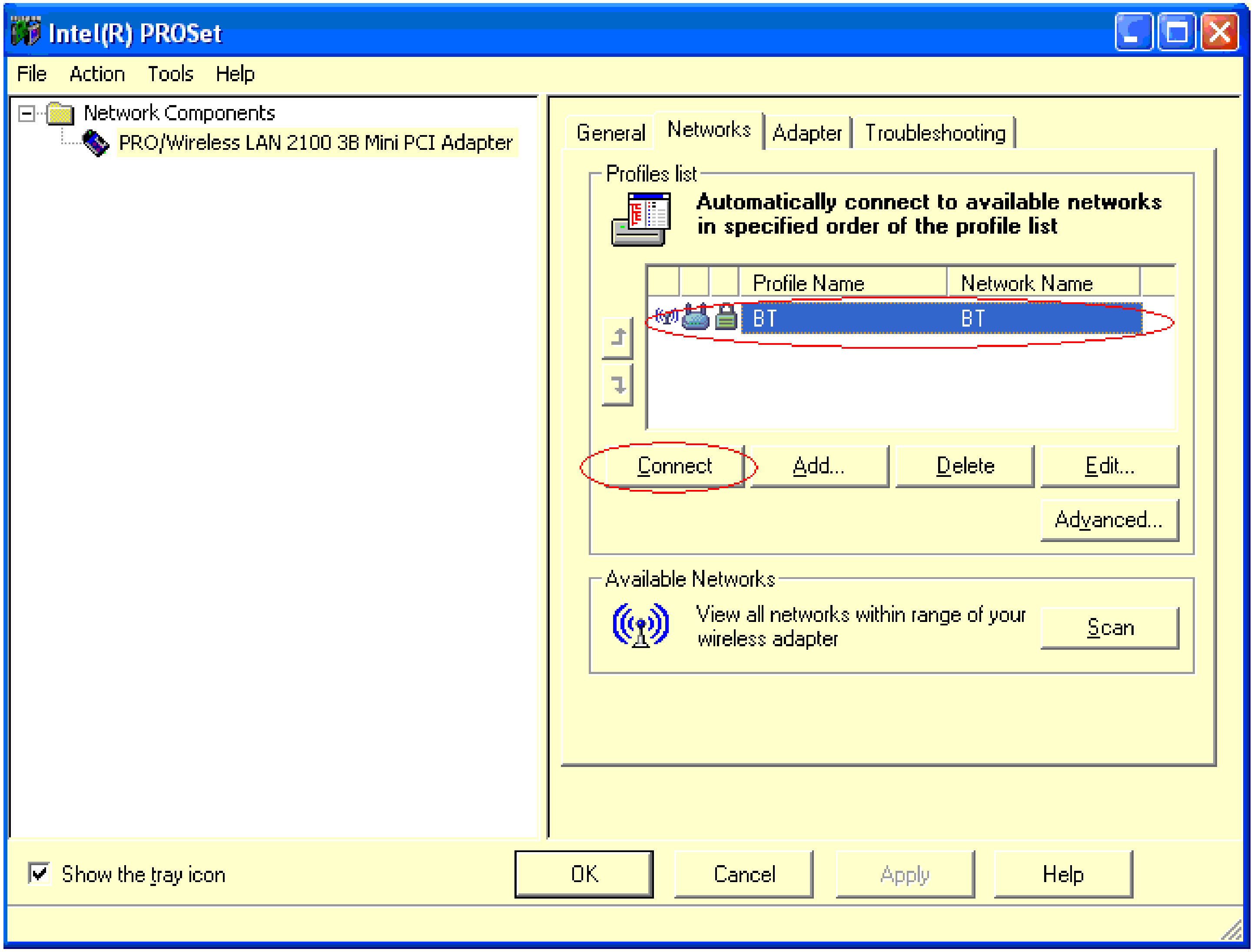
802.1x Settings

☑ 802.1x Enabled

Authentication Type: None

□ Enable Auto-Import

12. After you finished the profile settings, choose the profile you configured. Then, click **Connect** button to associate with the Access Point.



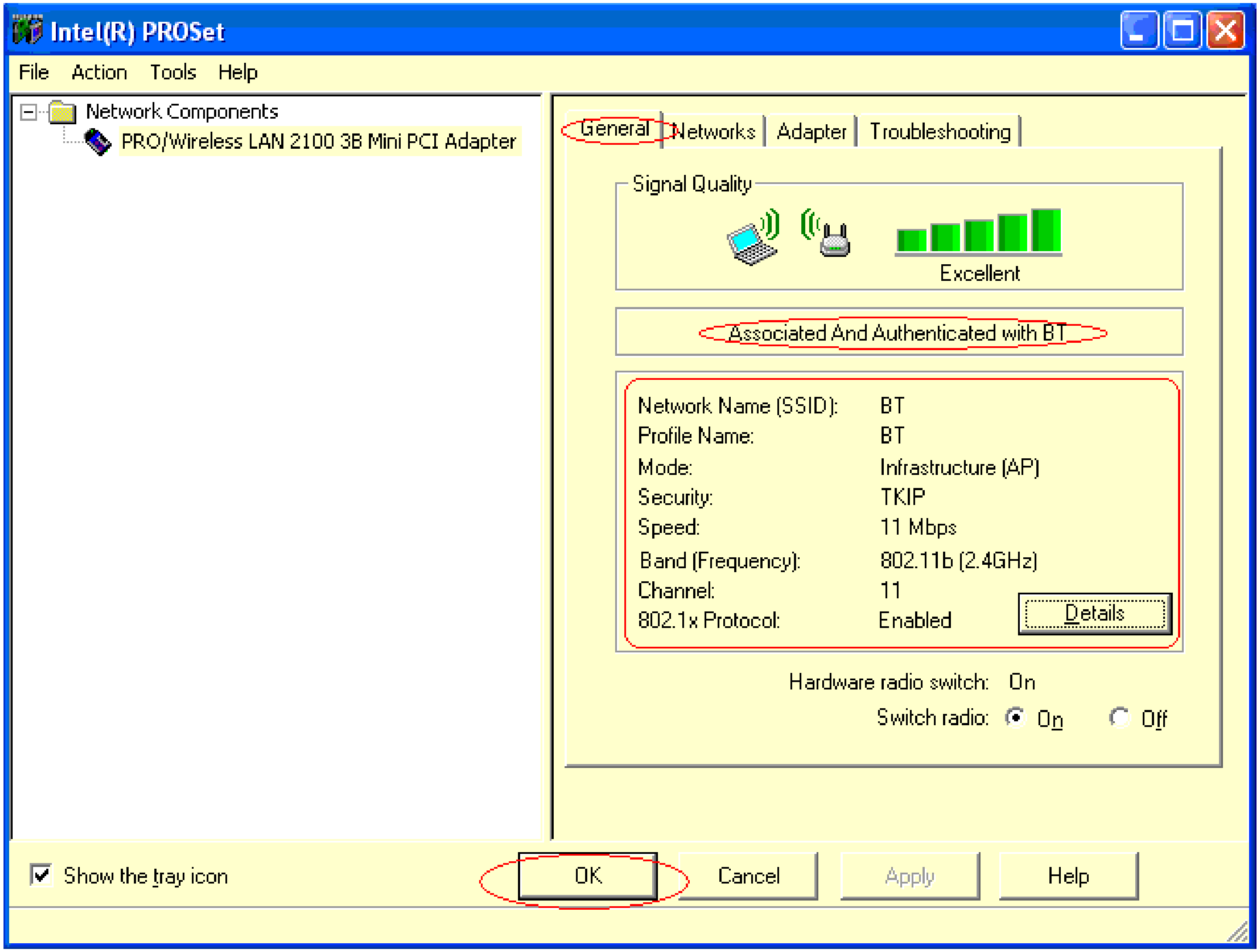
Automatically connect to available networks in specified order of the profile list

Profile Name	Network Name
BT	BT

View all networks within range of your wireless adapter

☑ Show the tray icon

13. Click the General option, we will see the following information, that means the PC associated and authenticated with AP successfully.



Associated And Authenticated with BT

Network Name (SSID):	BT
Profile Name:	BT
Mode:	Infrastructure (AP)
Security:	TKIP
Speed:	11 Mbps
Band (Frequency):	802.11b (2.4GHz)
Channel:	11
802.1x Protocol:	Enabled

Hardware radio switch: On

Switch radio: ● On ○ Off

☑ Show the tray icon

Setup 802.1x client in the station

- ***Setup 802.1x client in the station***

The EAP protocol can support multiple authentication mechanisms, such as MD5-challenge, One-Time Passwords, Generic Token Card, TLS and TTLS etc. So far, ZyXEL Wireless AP only supports MD-5 challenge authentication mechanism, but will support TLS and TTLS in the future. Here we just take MD-5 challenge authentication mechanism as a example.

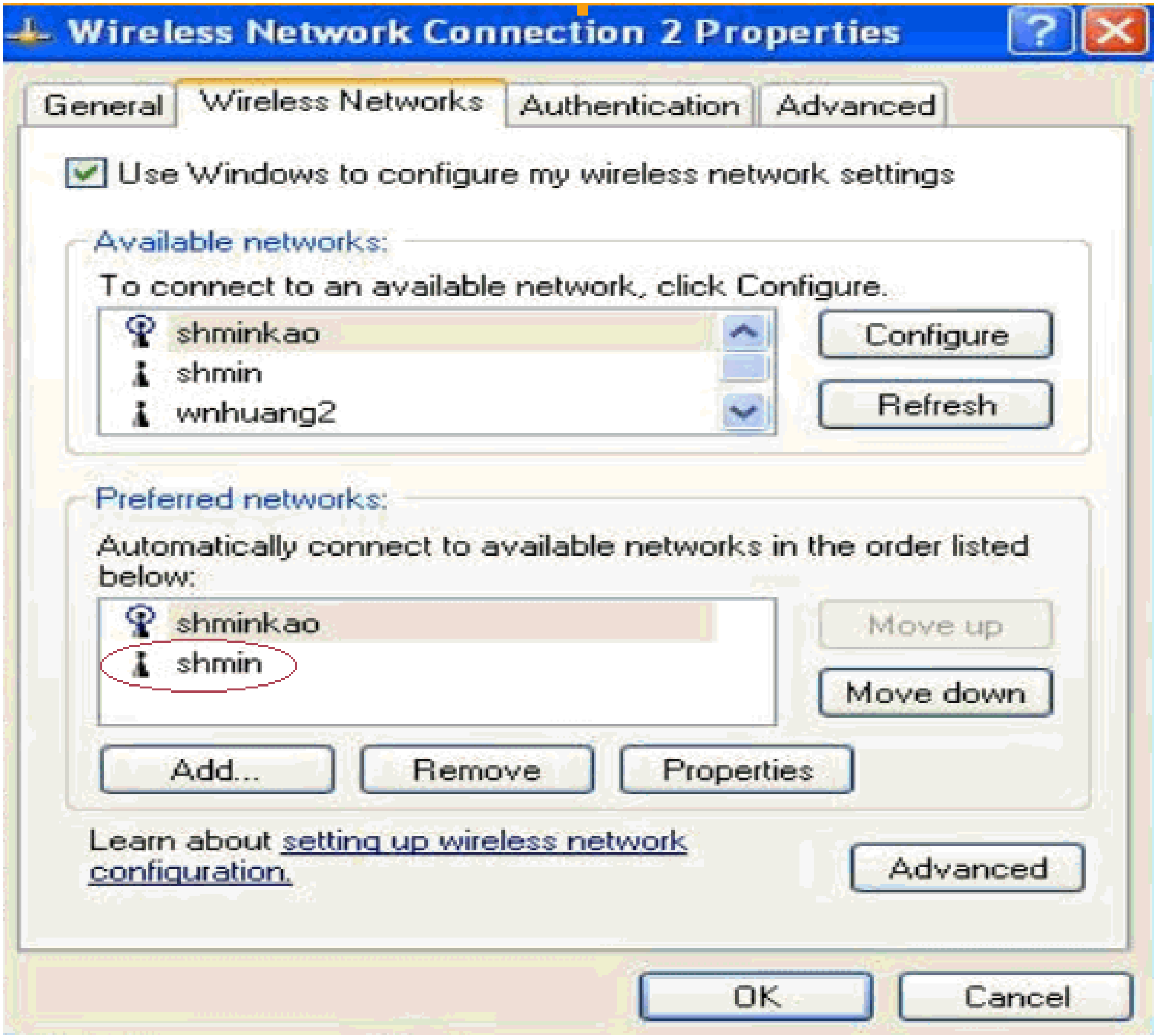
- ***Setup Windows XP 802.1x client***

Please install Windows XP that support 802.1x MD-5 challenge authentication mechanism. Don't upgrade to Service Pack 1, it support TLS authentication mechanism by default, instead of MD-5 challenge. ZyXEL Wireless AP will support TLS and TTLS in the future.

1.In the **Network** windows, choose **Wireless Network Connection** entry and click the **Properties** button.

2. In **Wireless Networks** tab, check **use windows to configure my wireless network**.

3. In **Preferred Networks** field, from the AP list found, move up the AP shmin (e.g.) that you want to use to the top by clicking on the **Move up** button (Windows XP will automatically detect the AP's ESSID and show it in **Available networks** field). If the AP is not shown in **Available networks** field, you can use the **Add...** button in **Preferred networks** to add the target AP into the list.


Wireless Network Connection 2 Properties

General | Wireless Networks | Authentication | Advanced

☑ Use Windows to configure my wireless network settings

Available networks:

To connect to an available network, click Configure.

- shminkao
- shmin
- wnhuang2

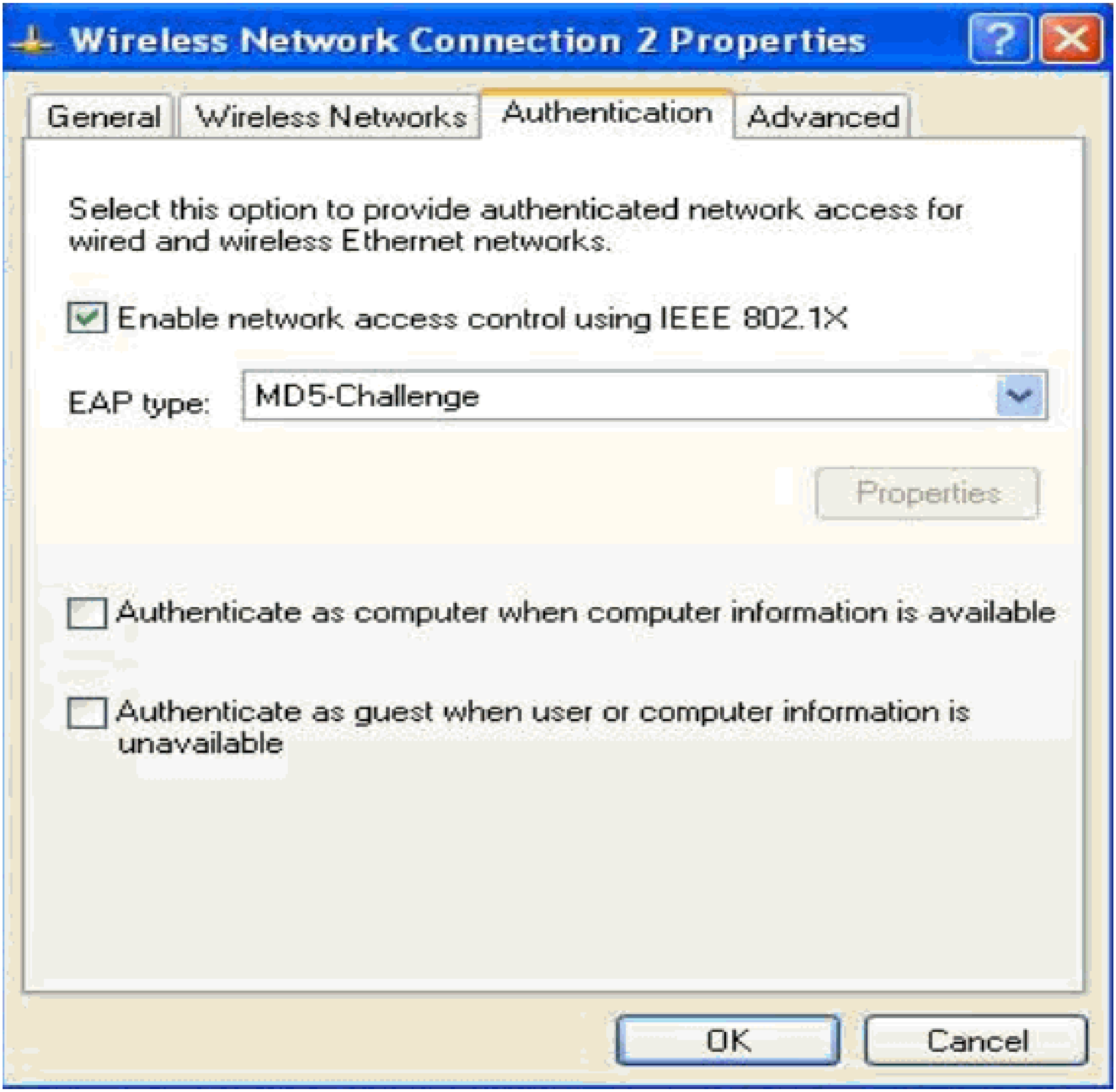
Preferred networks:

Automatically connect to available networks in the order listed below:

- shminkao
- shmin

Learn about setting up wireless network configuration.

4. In **Authentication** tab, check **Enable network access control using IEEE 8021.x** and choose the **MD5-Challenge** in the **EAP type:** list, as shown below.



Wireless Network Connection 2 Properties

General | Wireless Networks | Authentication | Advanced

Select this option to provide authenticated network access for wired and wireless Ethernet networks.

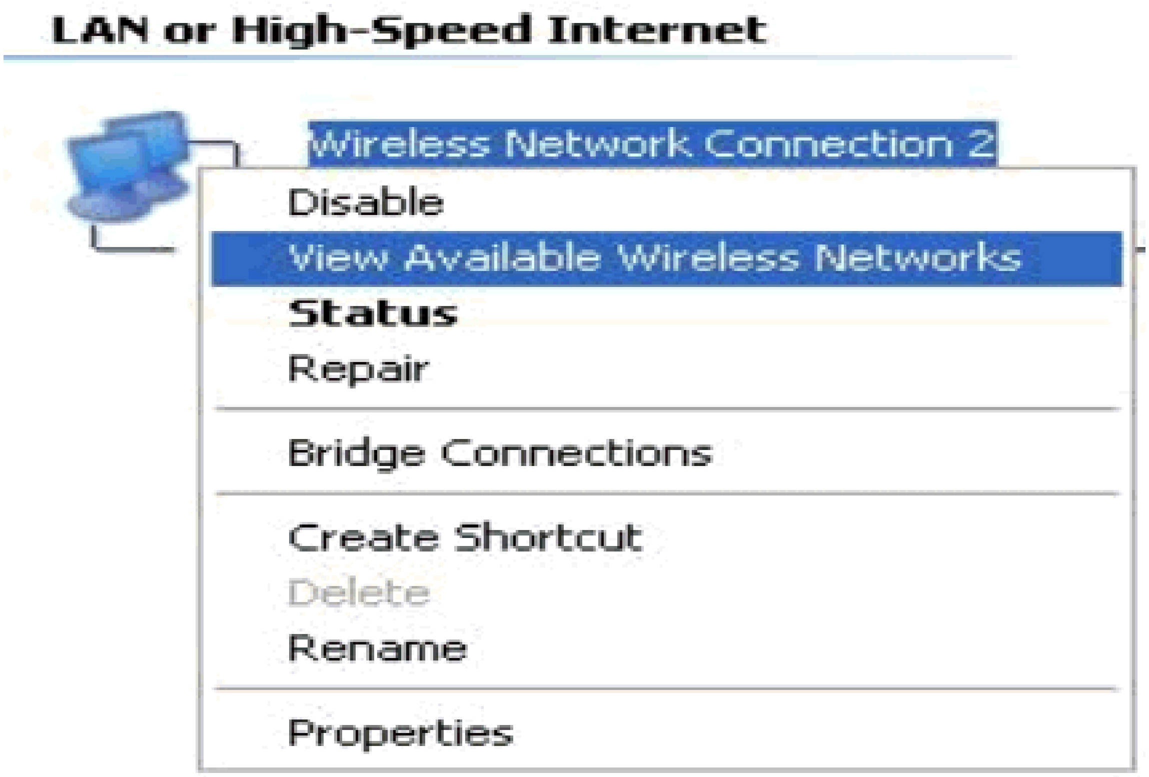
☑ Enable network access control using IEEE 802.1X

EAP type: MD5-Challenge

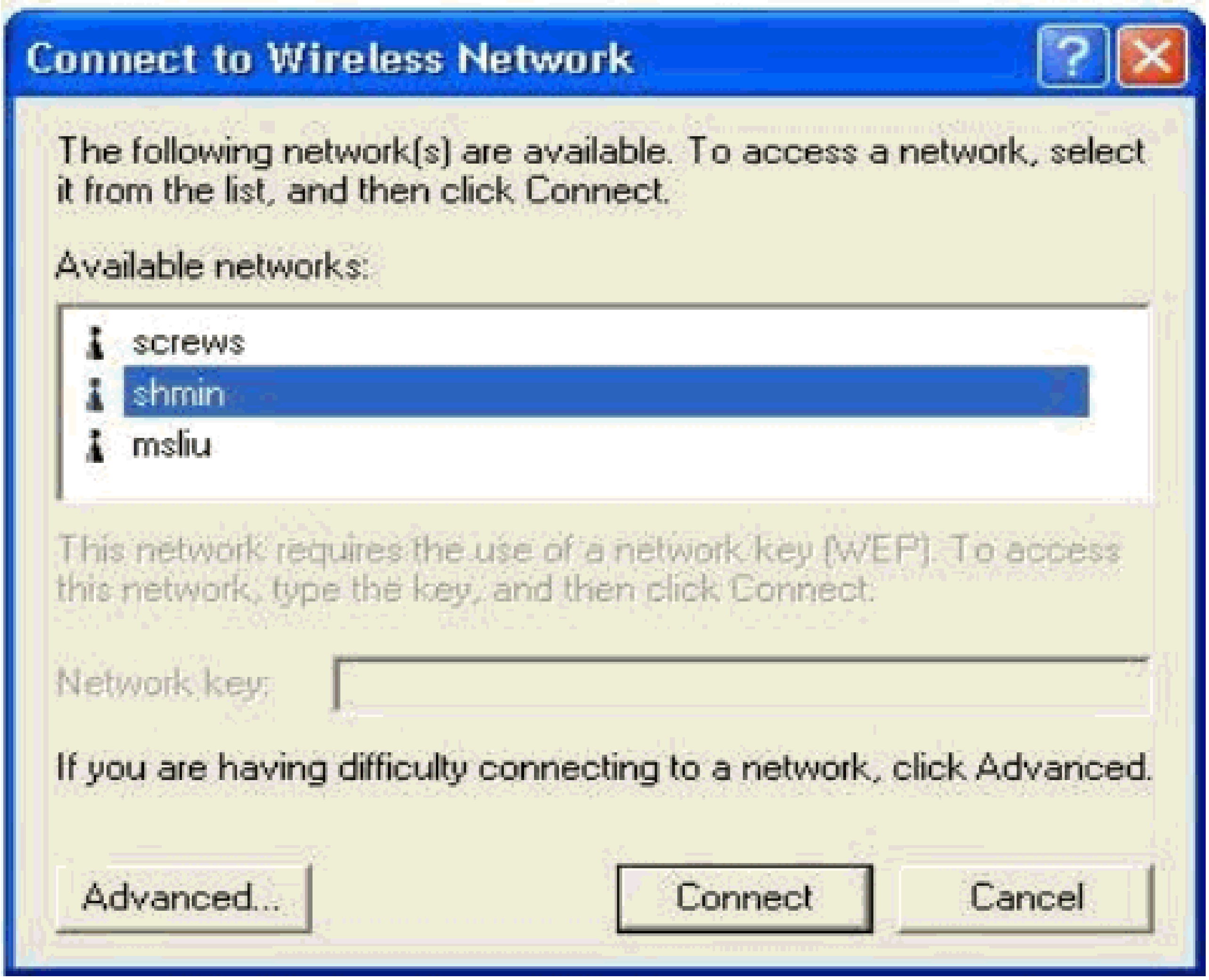
□ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

5. Connect to ZyXEL AP, in **Wireless Network Connection**, choose **View Available Wireless Networks**


LAN or High-Speed Internet
Wireless Network Connection 2
Disable
View Available Wireless Networks
Status
Repair
Bridge Connections
Create Shortcut
Delete
Rename
Properties

6. In the **Connect to Wireless Network** window, select the AP you would like to connect in the **Available networks** field then click **Connect** button for connection.



Connect to Wireless Network

The following network(s) are available. To access a network, select it from the list, and then click Connect.

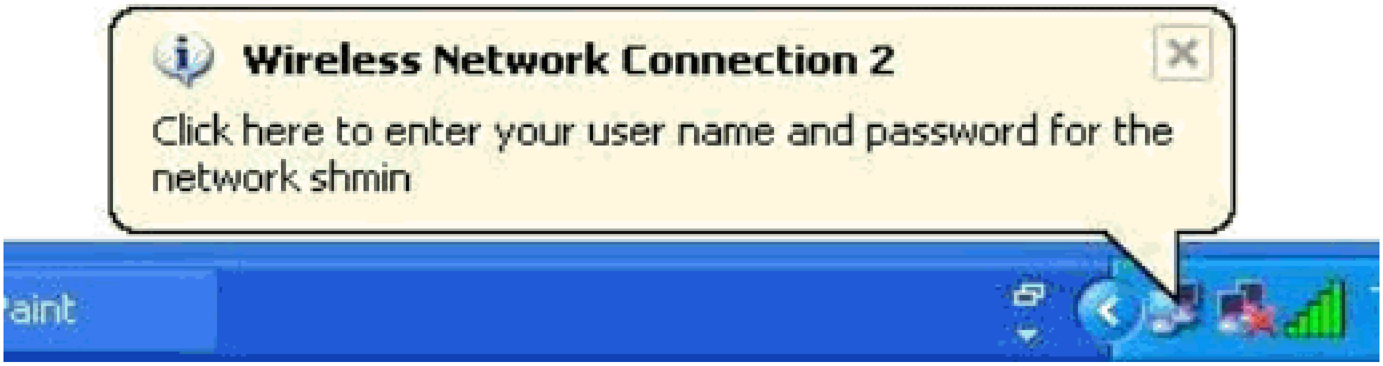
Available networks:

This network requires the use of a network key (WEP). To access this network, type the key, and then click Connect.

Network key:

If you are having difficulty connecting to a network, click Advanced.

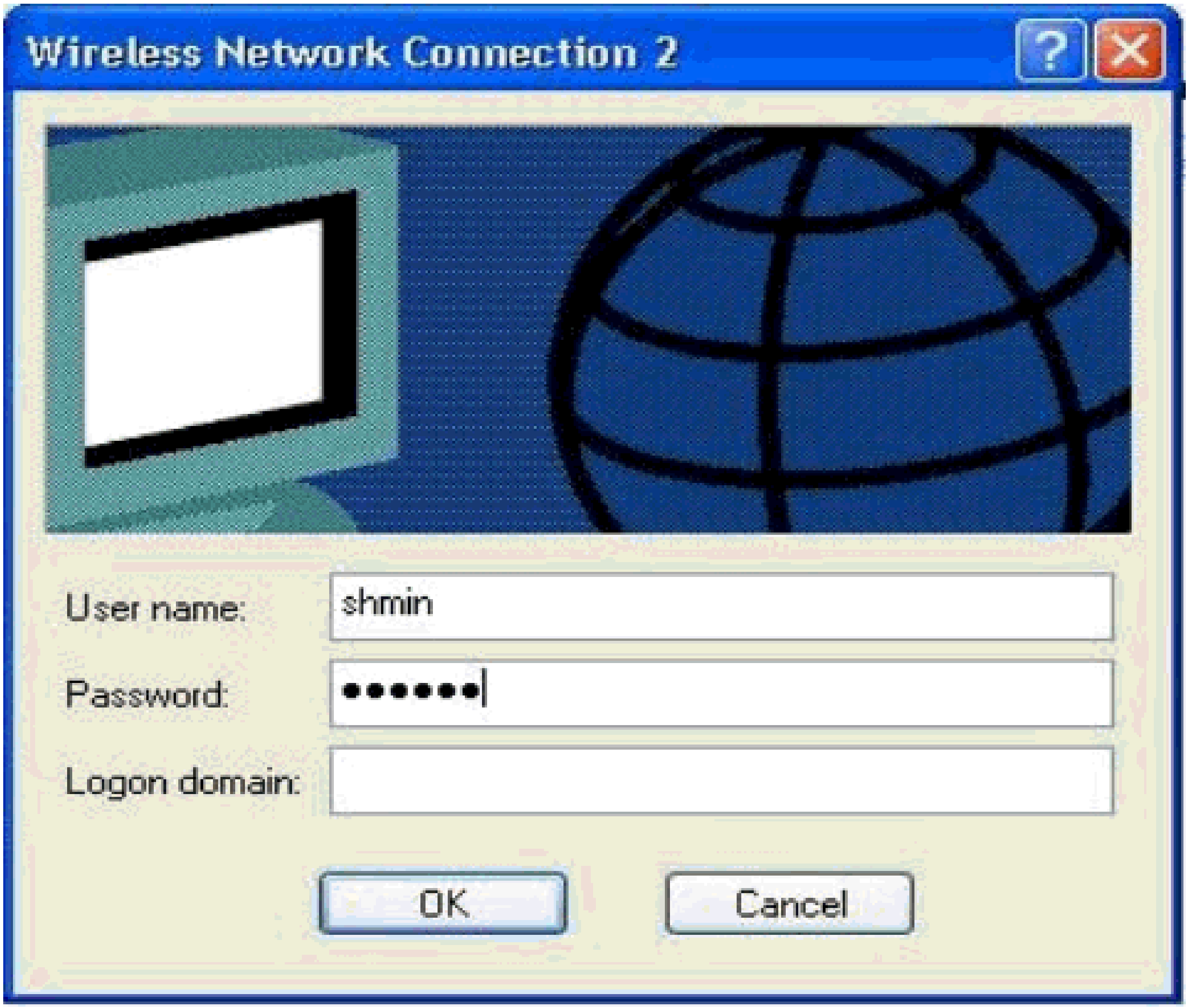
7. Windows XP will show you the message "**Click here to enter your user name and password for the network <AP_name>**" where the <AP_name> is the AP's name you chose on previous step. Click on the message box or the icon shown on the icon list.



Wireless Network Connection 2

Click here to enter your user name and password for the network shmin

8. In the **Wireless Network Connection** window, enter the <user_name> in the **User name** field and <pass_word> in the **Password** field that are already set in AP for login. Click **OK** to finish the connection.



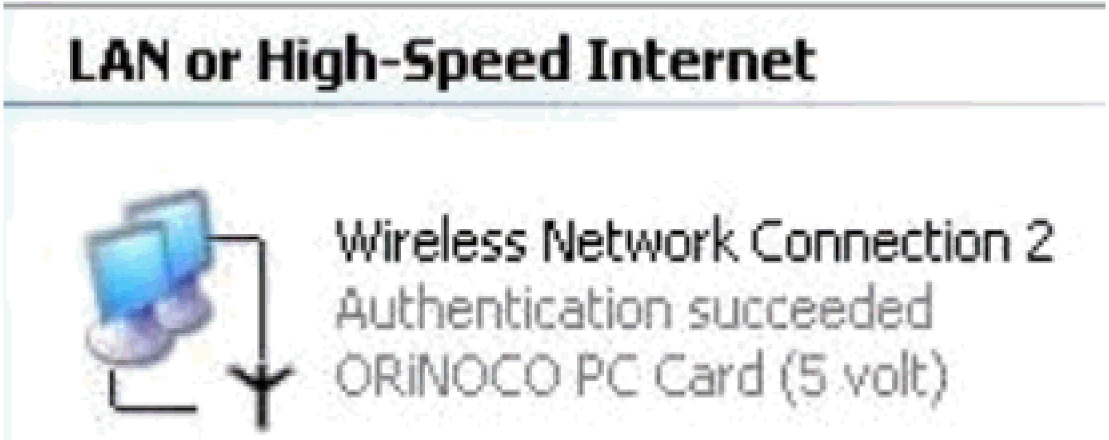
Wireless Network Connection 2

User name: shmin

Password: ●●●●●●●

Logon domain:

9. Windows XP completes the negotiation and changes the status for you automatically as shown on following figure.

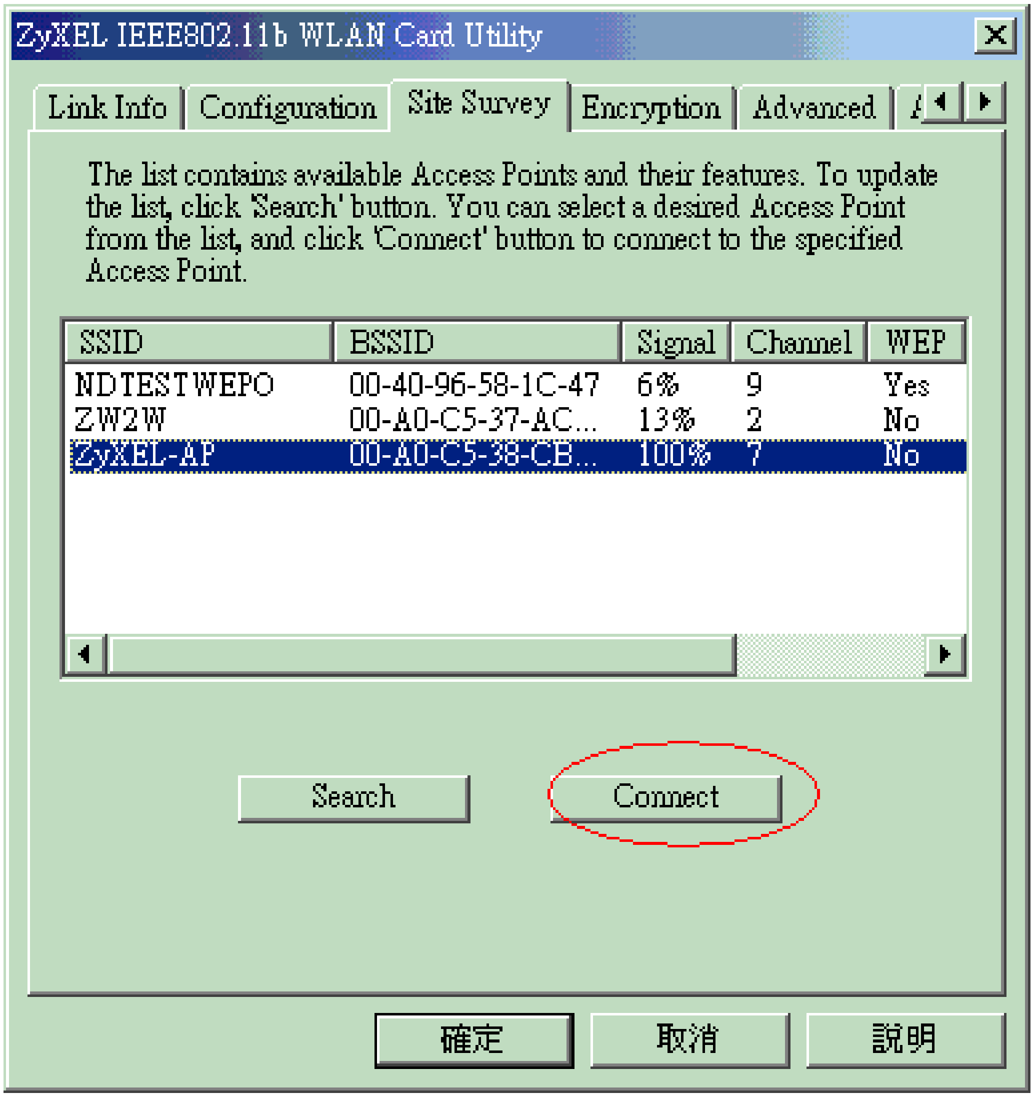


LAN or High-Speed Internet

Wireless Network Connection 2
Authentication succeeded
ORiNOCO PC Card (5 volt)

- ***Setup MeetingHouse AEGIS 802.1x client***

1. Please connect your wireless client to AP before configuring AEGIS 802.1x client.

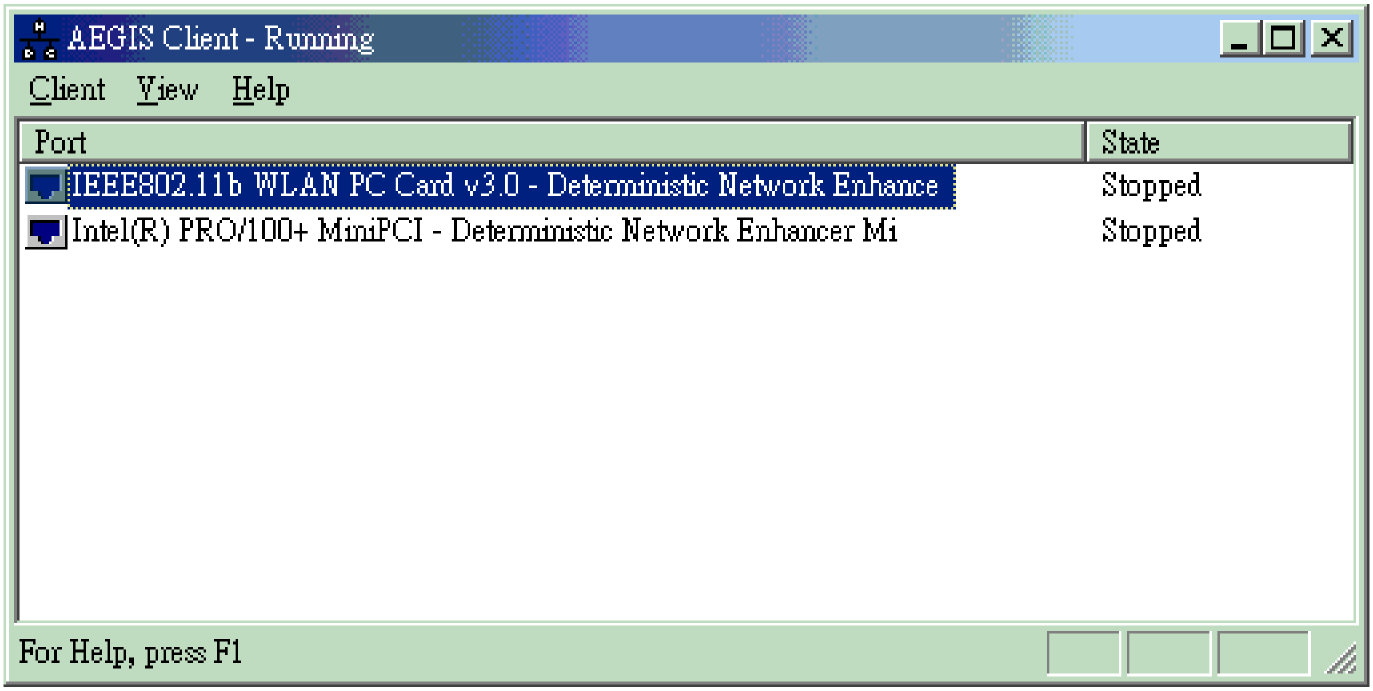


The list contains available Access Points and their features. To update the list, click 'Search' button. You can select a desired Access Point from the list, and click 'Connect' button to connect to the specified Access Point.

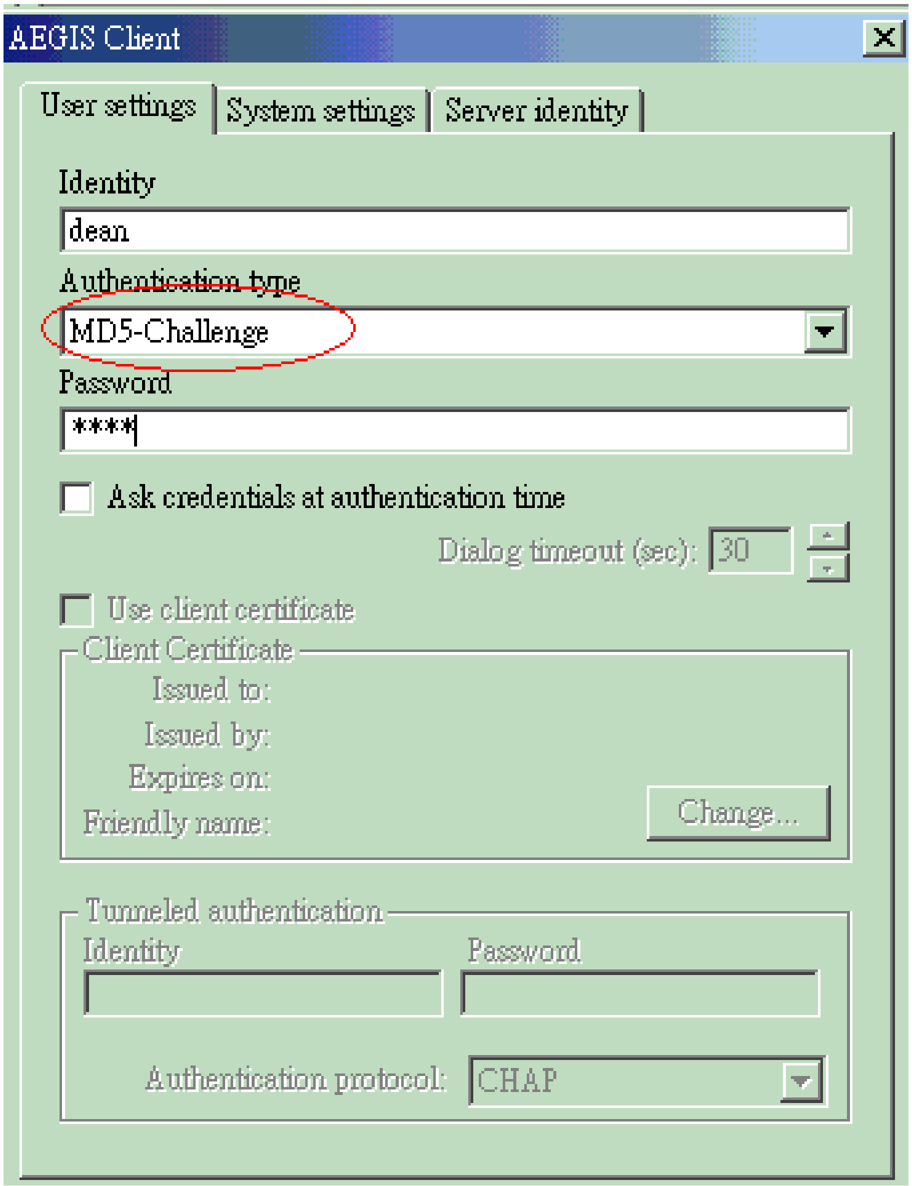
SSID	BSSID	Signal	Channel	WEP
NDTESTWEPO	00-40-96-58-1C-47	6%	9	Yes
ZW2W	00-A0-C5-37-AC...	13%	2	No
ZyXEL-AP	00-A0-C5-38-CB...	100%	7	No

2. Open **AEGIS Client- Running** window, choose **Client** --> **Configure** --> Select **User settings** tag --> Type the username into the **Identity** field --> Select **MD5-Challenge authentication type -->** Type password into **Password** field --> Click **Apply** button to save your configuration and return to AEGIS Client window.

Setup 802.1x client in the station



Port	State
IEEE802.11b WLAN PC Card v3.0 - Deterministic Network Enhance	Stopped
Intel(R) PRO/100+ MiniPCI - Deterministic Network Enhancer Mi	Stopped



Identity: dean

Authentication type: MD5-Challenge

Password: ****

□ Ask credentials at authentication time

Dialog timeout (sec): 30

□ Use client certificate

Client Certificate

Issued to:

Issued by:

Expires on:

Friendly name:

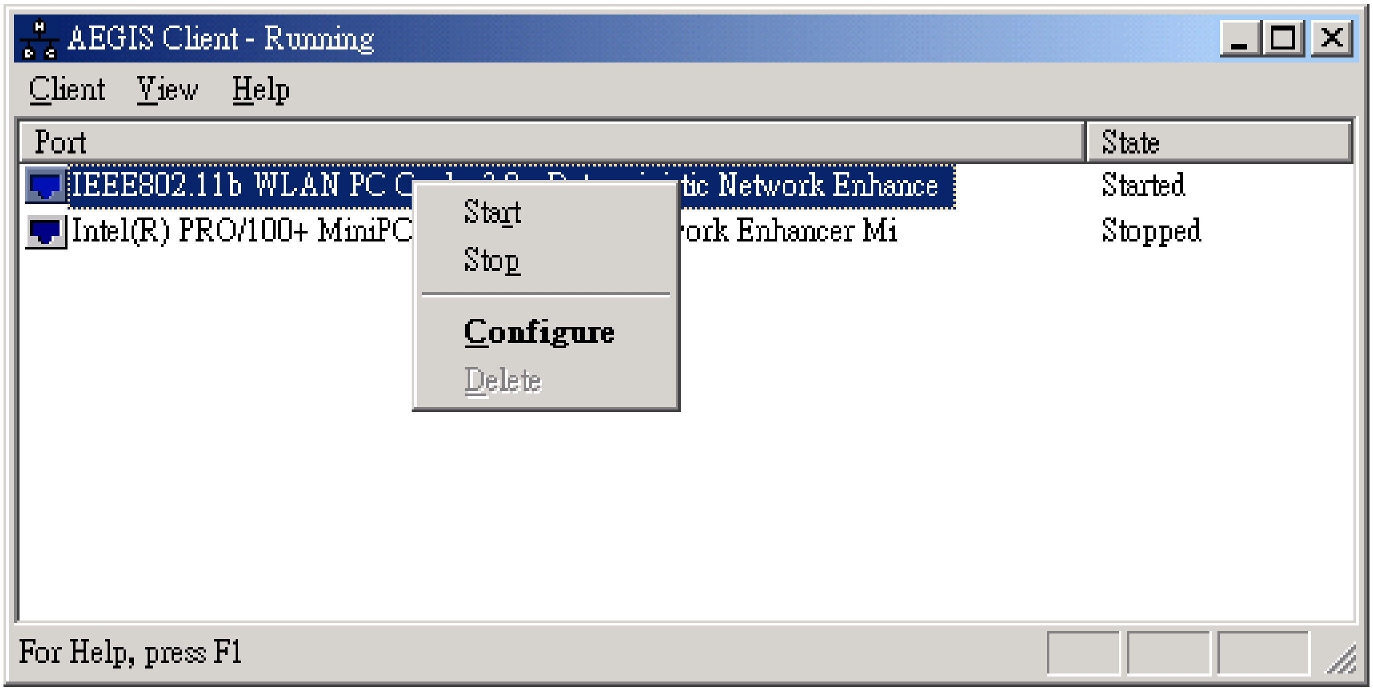
Tunneled authentication

Identity

Password

Authentication protocol: CHAP

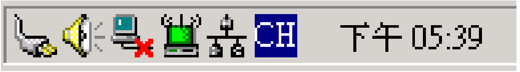
3. Right click the specified wireless client adapter in the AEGIS Client --> Select **Start** to start the 802.1x authentication on the specified wireless clinet adapter.



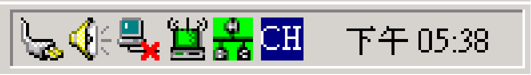
Port	State
IEEE802.11b WLAN PC C ... tic Network Enhance	Started
Intel(R) PRO/100+ MiniPC ... ork Enhancer Mi	Stopped

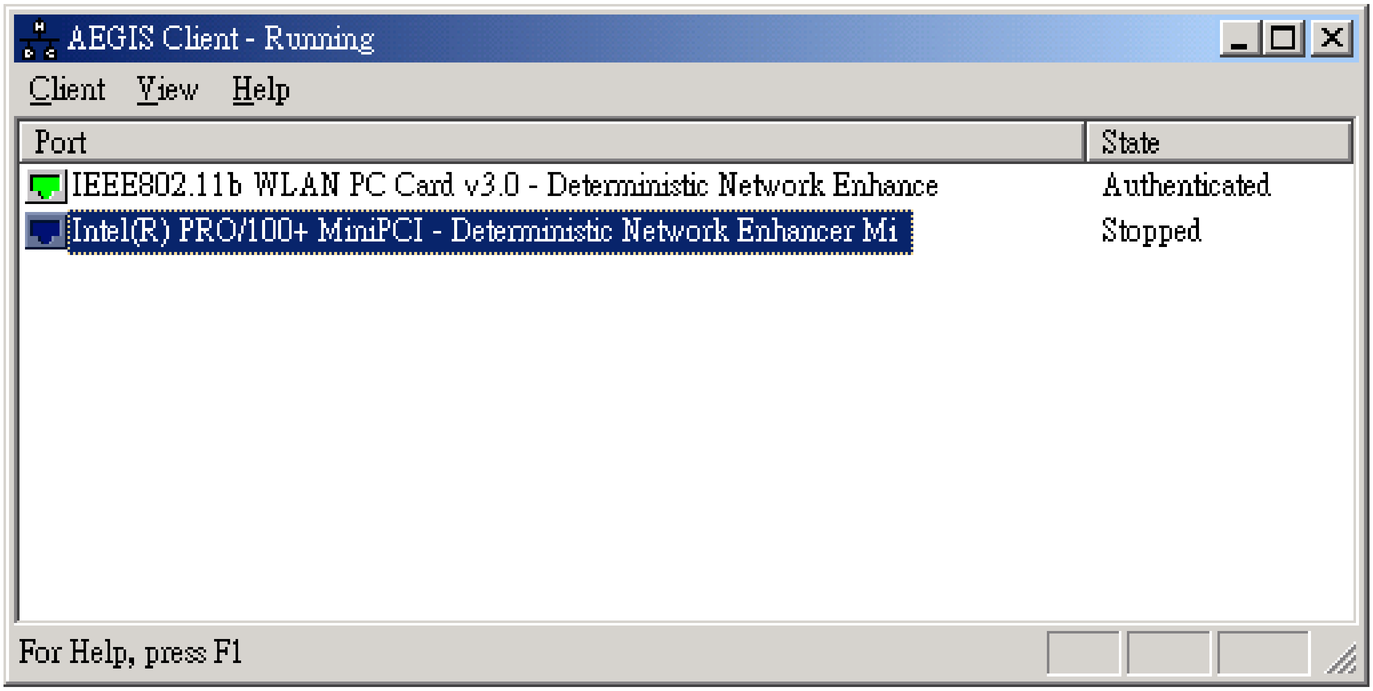
4. AEGIS 8021.x client completes the negotiation and changes status automatically.

Before 802.1x authentication :



After 802.1x authentication is completed :





Port	State
IEEE802.11b WLAN PC Card v3.0 - Deterministic Network Enhance	Authenticated
Intel(R) PRO/100+ MiniPCI - Deterministic Network Enhancer Mi	Stopped

5. If AEGIS 802.1x client does not start to negotiate with wireless AP, please perform Step 1 again.

I 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		

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
	diagnose			self-diagnostics
	essid		[ess id]	set ESS ID
	scan			scan wireless channels
	version			display WLAN version information
wlan1				
	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				
	radius	authentication	Show	show current radius authentication server configuration
		accounting	Show	show current radius accounting server configuration
	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

Wireless Troubleshooting

Is it a hardware problem ?

If following symptoms happen on the access point

- None of the LEDs turn on when I plug in the power adapter

Make sure you are using the supplied power adapter and that it is plugged in to an appropriate power source. Check that the power source is turned on. If the problem persists, you may have a hardware problem. In this case, you should contact your local vendor.

- The ZyAIR reboots automatically sometimes

The supplied power to ZyAIR is too low. Check that the ZyAIR is receiving enough power.

How can I check to be sure if I am interfered or not ?

There may not be an easy or quick answer to this. One thing to notice first is whether the problems are continuous or intermittent. Interference usually occurs intermittently, or else it would have likely been noticed when the link was first commissioned.

If I've confirmed it is an interference problem. What should I do?

Change the location and choose other radio channel to see whether the impact of the interference decreases and the link quality improves.

What should I do if I have low signal or high noise ?

To improve the signal, check or get the antennas with reverse SMA type connectors. For noise problems, please shield or remove the interference. If the situation doesn't improve, please change radio channels.

Unable to associate to the access point

1. Verify that the PC card or PCI adapter is installed correctly.
2. Is the signal strength and link quality good ? Move closer to the access point to see if it helps ? If not, you may have radio problems. Make sure you are in the wireless coverage of your access point.
3. Temporarily disable the WLAN MAC Filter function on the access point. If this solves the problem, check to make sure the MAC address of the wireless client is not contained in the list of denied MAC addressed.
4. Temporarily disable any security feature on both the access point and the client. If this solves the problem, check to make sure that the Wired Equivalent Privacy (WEP) key you use to transmit data is set up exactly the same on your AP and on any wireless devices with which it associates.
5. Make sure the configuration on access point and wireless consistent. Verify that the configuration for the SSID on PC matches the access point's ESSID.

You can verify the result of association by using wireless client utility or entering command "wlan association disp" in SMT Menu 24.8..

```
G3000H> wlan association disp
[NUM] MAC Address Association time
-------------------------------------------------------------
[001] 0x00:0x60:0xb3:0x69:0x03:0x37 00:00:02 2000/01/01 1
-------------------------------------------------------------
Total: 1
```

Unable to authenticate to the access point

If your client adapter is unable to authenticate to an access point, check the security settings of your client adapter and the access point. These include the following areas:

Authentication with shared key (WEP):

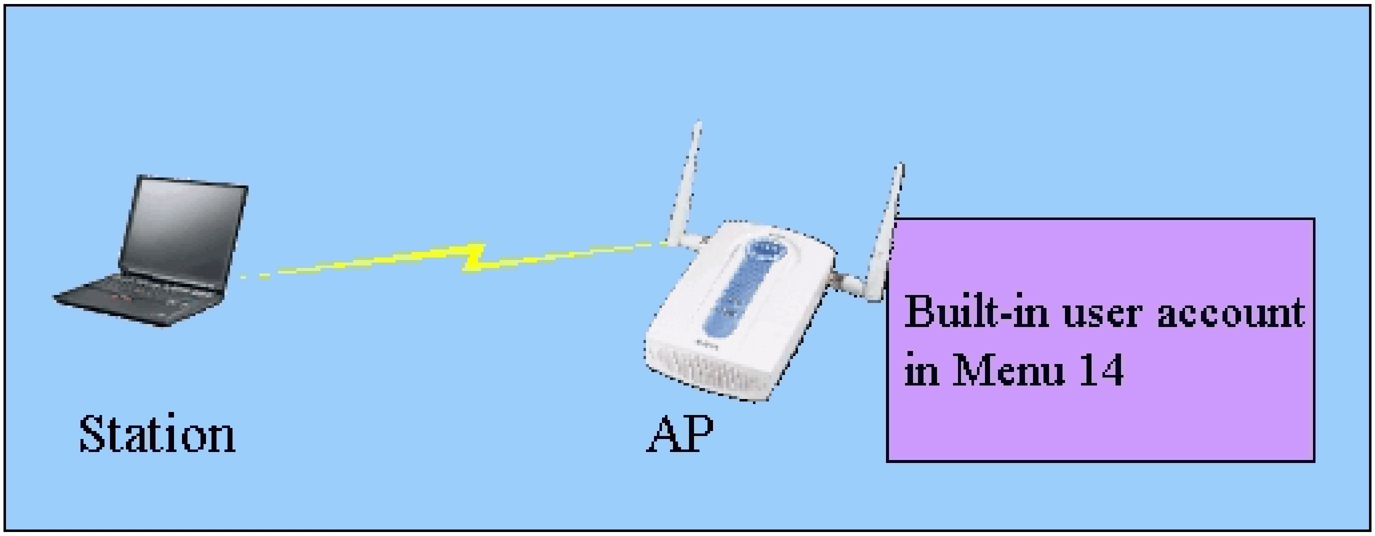
If you use WEP shared key to authenticate the wireless clients, you should check whether following configuration parameters on both AP and wireless clients match:

- WEP key values, WEP key sizes, WEP activation, and WEP transmit key parameters

Authentication with 802.1X:

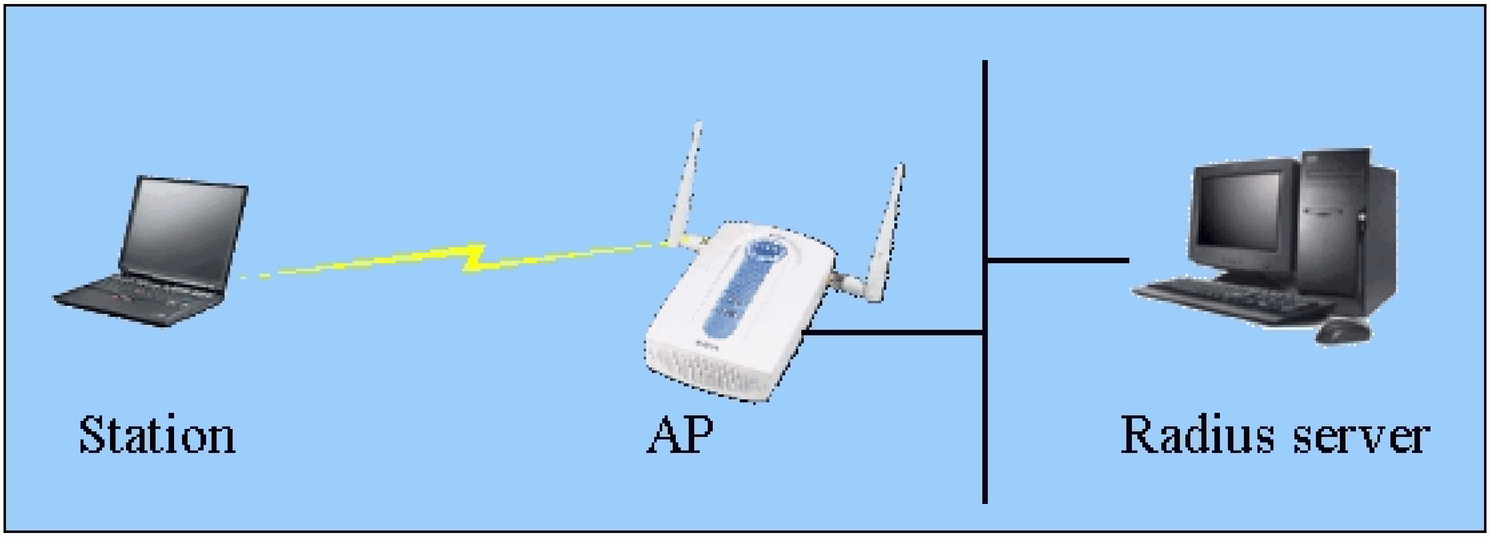
If 802.1X security is used in your network, you can troubleshoot the authentication through SMT Menu 24.3.1 - System Maintenance - Log and Trace. Here is the format of the log message: [user] [mac of user`s STA] [type] [message]

802.1X with built-in user account:



```
[test] [0:a:8a:a2:ae:4e] [login success] [accepted by profiles]

[test] [0:a:8a:a2:ae:4e] [login fail] [user password error related to profiles]

[mars] [0:a:8a:a2:ae:4e] [login fail] [user not found in profiles]
```

802.1X with RADIUS server:



```
[test] [0:60:b3:69:3:37] [login fail] [rejected by RADIUS server]

[test] [0:60:b3:69:3:37] [auth enticating ...] [no response from RADIUS server]

[test] [0:60:b3:69:3:37] [logout] [user requested]
```

Note: Some wireless clients (for example, Symbol PCMCIA client) support open authentication and WEP encryption for data traffic. To support these clients in your network, you need to select either 'Open System' or 'Auto' for authentication method when WEP is enable. If you have a mix network which mean there are adapter from different vendor, the suggest configuration is 'Auto'. The system will automatically detect your adapter type and auto configure to the client adapter when WEP is enabled.

Unable to get an IP address via DHCP

1. Verify that the DHCP server service is running.
2. The other wired clients on the same segment are able to be successfully addressed dynamically.
3. Verify that the ethernet interface on the access point is up.
4. Verify that the client has passed association and authentication to the access point.
5. Verify that the Wired Equivalent Privacy (WEP) key on the client is set up exactly the same on your AP.

Unable to transmit traffic

1. Verify that the client has passed association and authentication.
2. Make sure the client is configured with exact IP setting or get a valid IP address from DHCP server. You can go to a DOS prompt and type: ipconfig and press Enter to verify this.
3. Ping the gateway in your network. A response other than Request timed out indicates a successful ping.
4. Enable packet trace function on the access point Verify that the Wired Equivalent Privacy (WEP) key on the client is set up exactly the same on your AP.

What should I get back to my technical support for analysis ?

Following information are helpful to your technical support to troubleshoot your problem, please get back the answer and associated files to your support:

1. Is this a new or existing installation ?
2. Did it work before ?
3. Have there been any recent changes that might affect the LAN, the client workstation or the radio environment ?
4. What is the firmware version you are using now ? Do you have uploaded firmware recently ?
5. Is addresses, networking information and ROMFILE available ? If yes, please send it (include your password) to your support.
