WAP3205 v3

Wireless N300 Access Point

Version 1.0
Edition 1, 05/2016

User's Guide

Default Login Details	
LAN IP Address	http://192.168.1.2
User Name	admin
Password	1234

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the WAP3205 v3 and access the Web Configurator.

Note: It is recommended you use the Web Configurator to configure the WAP3205 v3.

PART I

User's Guide

Introduction

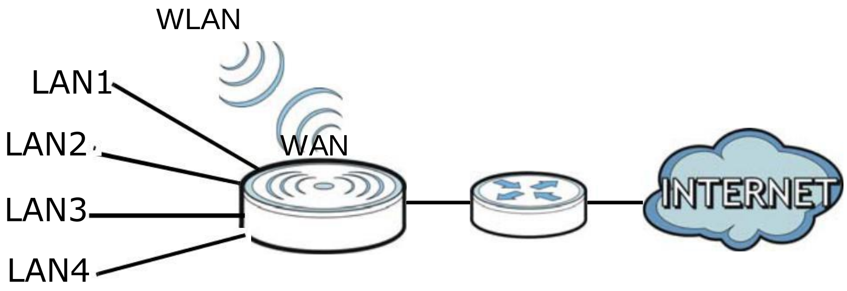
1.1 Overview

The WAP3205 v3 extends the range of your existing wired network without additional wiring, providing easy network access to mobile users.

Your can create the following connections using the WAP3205 v3:

- **LAN**. You can connect network devices via the Ethernet ports of the WAP3205 v3 so that they can communicate with each other and access the Internet.
- **WLAN**. Wireless clients can connect to the WAP3205 v3 to access network resources.

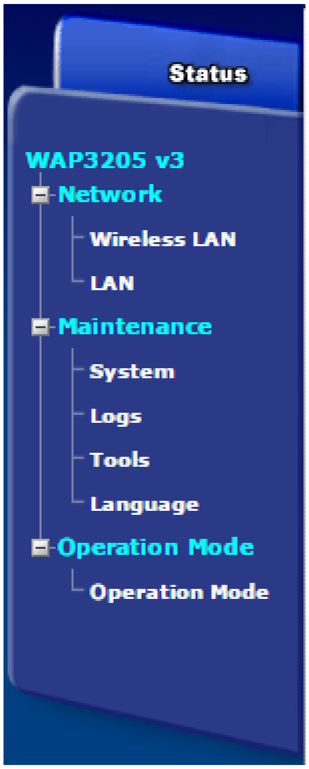
Figure 1 WAP3205 v3 Network



You can set up the WAP3205 v3 with other IEEE 802.11b/g/n compatible devices in one of the following device modes:

- Access Point
- Universal Repeater

Use a (supported) web browser to manage the WAP3205 v3. Menus vary according to which mode you're using.



See Chapter 4 on page 29 for more information on these modes.

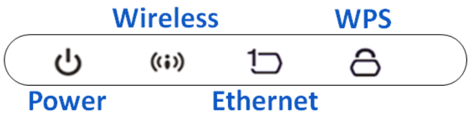
1.2 Securing the WAP3205 v3

Do the following things regularly to make the WAP3205 v3 more secure and to manage the WAP3205 v3 more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the WAP3205 v3 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the WAP3205 v3. You could simply restore your last configuration.

1.3 LEDs

Figure 2 Front Panel



The following table describes the LEDs and the WPS button.

LED	Color	Status	Behavior
Power	Green	On	The WAP3205 v3 is receiving power and functioning properly.
		Off	The WAP3205 v3 is not receiving power.
WLAN_2.4G/Wireless	Green	On	WAP3205 v3 is ready, but is not sending/receiving data.
		Blinking	The WAP3205 v3 is sending/receiving data through wireless LAN.
		Off	The wireless LAN is not ready or has failed.
Ethernet	Green	On	The WAP3205 v3 LAN port (any of 5 ports) is connected with router or client device
		Off	The WAP3205 v3 LAN port (any of 5 ports) is connected with a router or client device
WPS	Green	On	WPS is working
		Blinking	The WAP3205 v3 is negotiating a WPS connection with a wireless client
		Off	The WPS is not ready or has failed

Table 1 Front Panel LEDs and WPS Button

1.4 The WPS/RESET Button

Your WAP3205 v3 supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (recommended) on the device itself, or in its configuration utility or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

The **WPS/RESET** single button is located at the back panel of the WAP3205 v3.

1.4.1 Using the WPS/RESET Button

1 Make sure the power LED is on.

2 Press the **WPS/RESET** button within 3 seconds to turn on the WPS function

3 Press the **WPS/RESET** button for longer than 10 seconds to restart/reboot the WAP3205 v3 back to its factory-default configurations.

For more information on using **WPS/RESET**, see Section 5.3 on page 44.

1.5 Wall Mounting

You may need screw anchors if mounting on a concrete or brick wall.

Table 2 Wall Mounting Information

Distance between holes	10.50 cm
M4 Screws	Two
Screw anchors (optional)	Two

1 Select a position free of obstructions on a wall strong enough to hold the weight of the device.

2 Mark two holes on the wall at the appropriate distance apart for the screws.

Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

3 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap of about 0.5 cm.

If not using screw anchors, use a screwdriver to insert the screws into the wall. Do not insert the screws all the way in - leave a gap of about 0.5 cm.

4 Make sure the screws are fastened well enough to hold the weight of the WAP3205 v3 with the connection cables.

5 Align the holes on the back of the WAP3205 v3 with the screws on the wall. Hang the WAP3205 v3 on the screws.

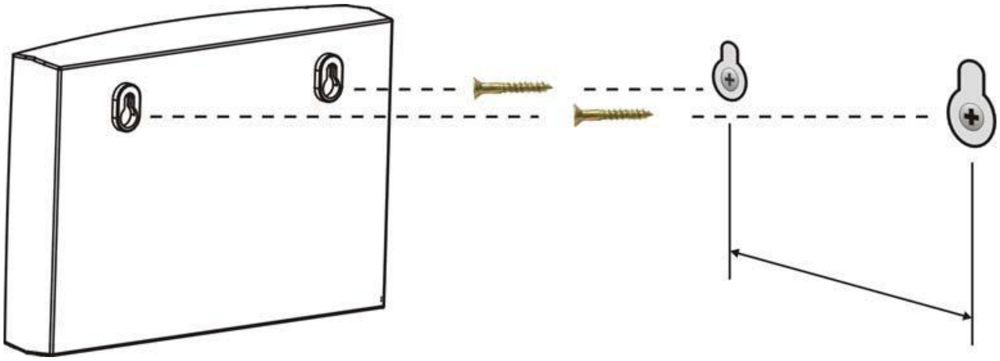


Figure 3 Wall Mounting Example

The Web Configurator

2.1 Overview

This chapter describes how to access the WAP3205 v3 Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy setup and management of the WAP3205 v3 via Internet browser. Use Internet Explorer 8.0 and later versions, Mozilla Firefox, Google Chrome or Safari. The recommended screen resolution is 1024 by 768 pixels.

In order to use the Web Configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Refer to Chapter 21 Troubleshooting to see how to make sure these functions are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

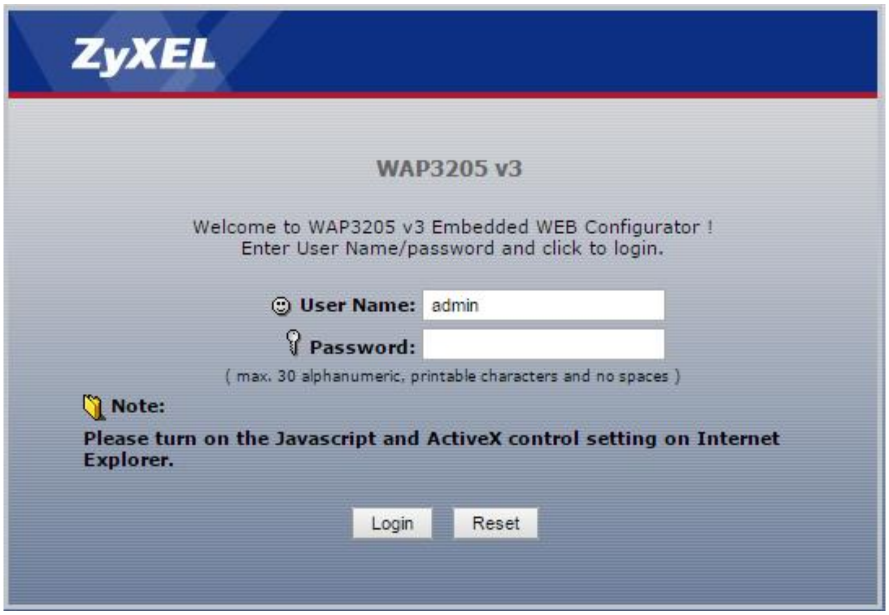
1 Make sure your WAP3205 v3 hardware is properly connected and prepare your computer or computer network to connect to the WAP3205 v3 (refer to the Quick Start Guide).

2 Launch your web browser.

3 Type "http://192.168.1.2" as the website address in your web browser
Your computer must be in the same subnet in order to access this website address.

4 Type **admin** (default) as the user name and **1234** (default) as the password and click **OK**.

Figure 4 Login Screen



WAP3205 v3

Welcome to WAP3205 v3 Embedded WEB Configurator !
Enter User Name/password and click to login.

User Name: admin

Password:

(max. 30 alphanumeric, printable characters and no spaces)

Note:

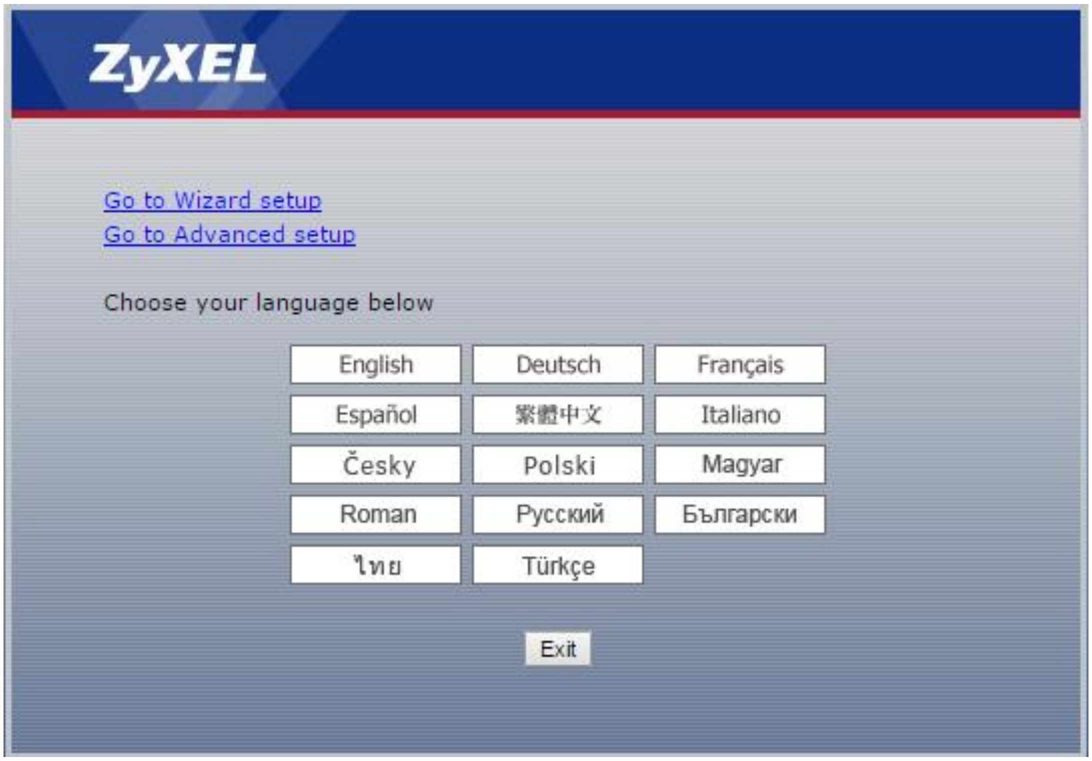
Please turn on the Javascript and ActiveX control setting on Internet Explorer.

Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the WAP3205 v3 if this happens.

5 Select the setup type you want to use.

- Click **Go to Wizard Setup** to use the Configuration Wizard for basic Internet and Wireless setup.
- Click **Go to Advanced Setup** to view and configure all the WAP3205 v3’s settings.
- Select a language to go to the basic Web Configurator in that language. To change to the advanced configurator see Chapter 20 on page 141.

Figure 5 Selecting the setup mode



2.3 Resetting the WAP3205 v3

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the **WPS/RESET** button at the back of the WAP3205 v3 to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the username will be reset to **admin** and password will be reset to **1234**. The IP address will be reset to "192.168.1.1".

Make sure the power LED is on and press the **WPS/RESET** button for longer than 10 seconds to restart/reboot and set the WAP3205 v3 back to its factory-default configurations.

Modes

4.1 Overview

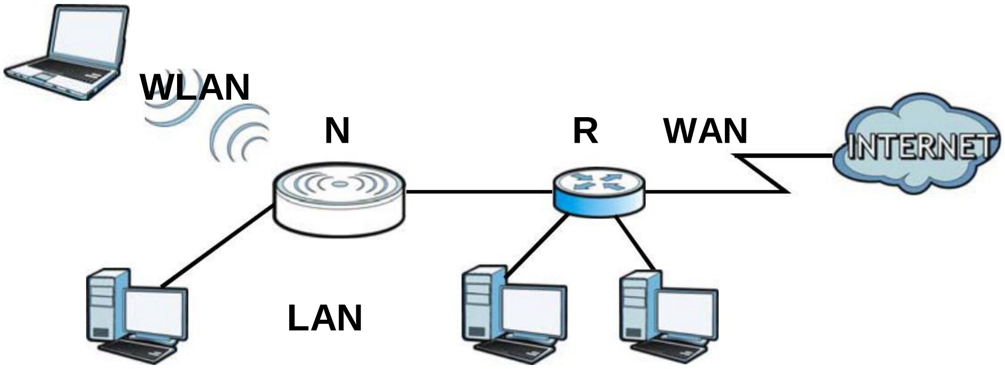
You can set up the WAP3205 v3 with other IEEE 802.11b/g/n compatible devices in different device modes.

Note: Choose your device mode carefully to avoid having to change it later. The WAP3205 v3 automatically restarts when you change modes.

The default IP address of the WAP3205 v3 is 192.168.1.2.

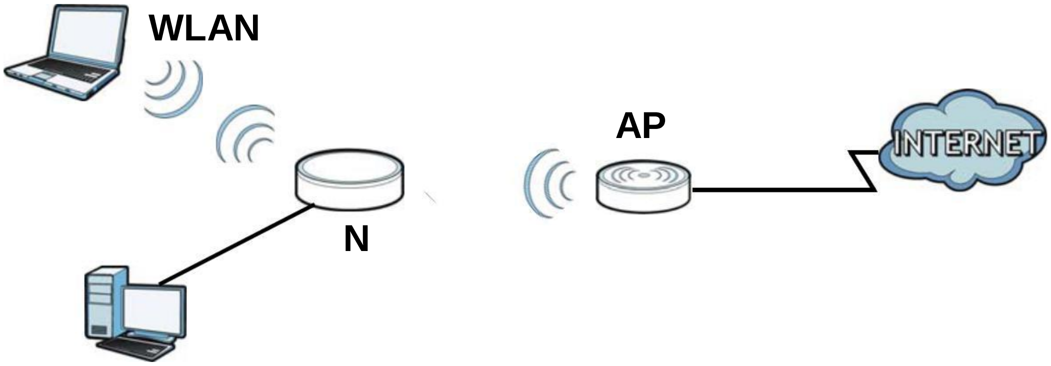
- **Access Point**: Use this mode if you already have a Router (R) in your network and you want to set up a wireless network and bridge the wired and wireless connections on the NBG-416N.

Figure 17 AP Mode



- **Universal Repeater**: In this mode, the WAP3205 v3 (N) can be an access point and a wireless client at the same time. Use this mode if there is an existing wireless router or access point in your network and you want the WAP3205 v3 (N) to wirelessly relay communications from its wireless clients to the access point.

Figure 18 Universal Repeater



4.3 Setting your WAP3205 v3 to AP Mode

1 Connect your computer to the LAN port of the WAP3205 v3.

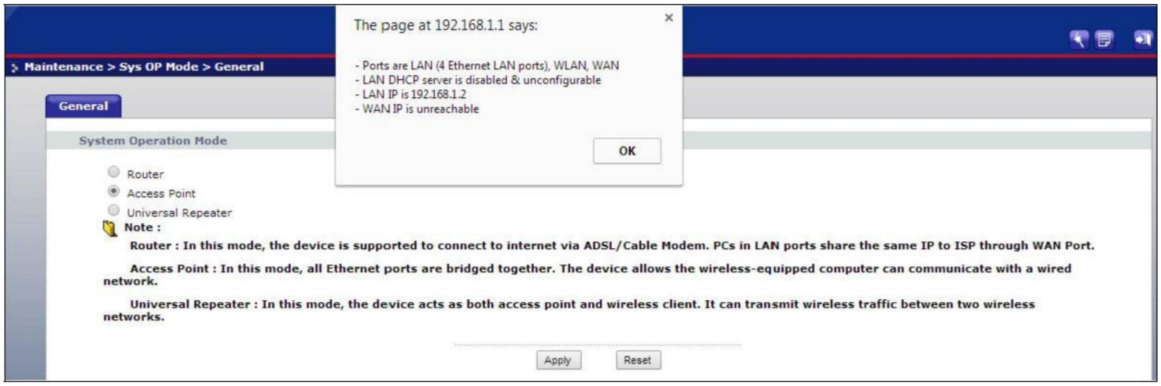
2 The default LAN IP address of the WAP3205 v3 is 192.168.1.

3 After you've set your computer's IP address, open a web browser such as Internet Explorer and type the IP address of the WAP3205 v3 as the web address in your web browser.

4 Log into the Web Configurator. See the Chapter 2 on page 17 for instructions on how to do this.

5 Go to **Maintenance > Sys OP Mode > General** and select **Access Point**.

Figure 24 Maintenance > Sys OP Mode > AP



The page at 192.168.1.1 says:

- Ports are LAN (4 Ethernet LAN ports), WLAN, WAN
- LAN DHCP server is disabled & unconfigurable
- LAN IP is 192.168.1.2
- WAN IP is unreachable

System Operation Mode

○ Router
● Access Point
○ Universal Repeater

Note :

Router : In this mode, the device is supported to connect to internet via ADSL/Cable Modem. PCs in LAN ports share the same IP to ISP through WAN Port.

Access Point : In this mode, all Ethernet ports are bridged together. The device allows the wireless-equipped computer can communicate with a wired network.

Universal Repeater : In this mode, the device acts as both access point and wireless client. It can transmit wireless traffic between two wireless networks.

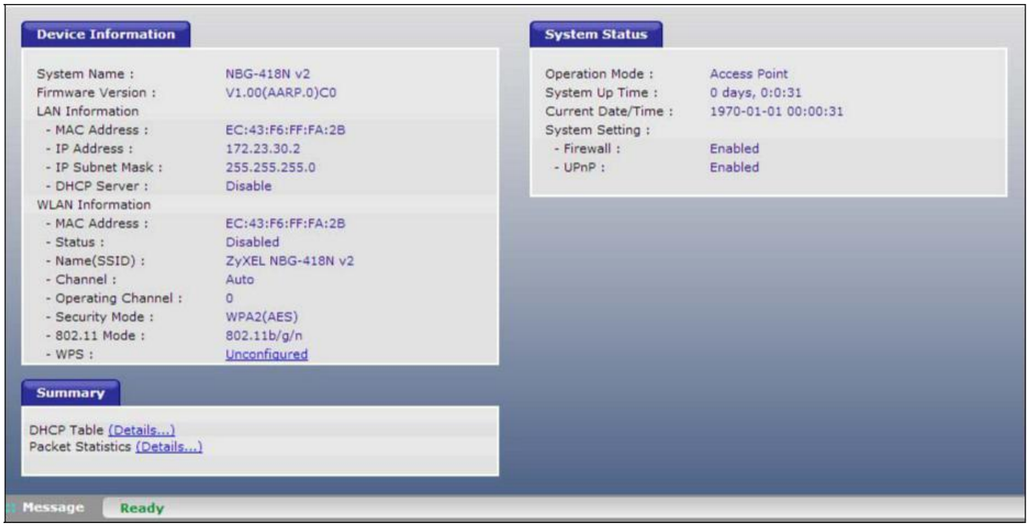
6 A pop-up window appears providing information on this mode. Click **OK** in the pop-up message window. Click **Apply**. Your WAP3205 v3 is now in **AP Mode**.

Note: Wait while the WAP3205 v3 restarts, then log in to the Web Configurator again.

4.3.1 Status Screen (AP Mode)

Click on **Status**. The screen below shows the status screen in **AP Mode**.

Figure 25 Status Screen (AP Mode)



Device Information

System Name :	NBG-418N v2
Firmware Version :	V1.00(AARP.0)C0
LAN Information	
- MAC Address :	EC:43:F6:FF:FA:2B
- IP Address :	172.23.30.2
- IP Subnet Mask :	255.255.255.0
- DHCP Server :	Disable
WLAN Information	
- MAC Address :	EC:43:F6:FF:FA:2B
- Status :	Disabled
- Name(SSID) :	ZyXEL NBG-418N v2
- Channel :	Auto
- Operating Channel :	0
- Security Mode :	WPA2(AES)
- 802.11 Mode :	802.11b/g/n
- WPS :	Unconfigured

System Status

Operation Mode :	Access Point
System Up Time :	0 days, 0:0:31
Current Date/Time :	1970-01-01 00:00:31
System Setting :	
- Firewall :	Enabled
- UPnP :	Enabled

Summary

DHCP Table (Details...)
Packet Statistics (Details...)

Message Ready

The following table describes the labels shown in the **Status** screen.

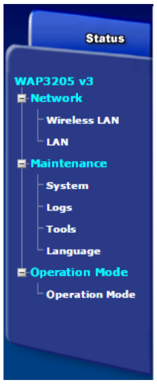
Table 12 Status Screen (AP Mode)

LABEL	DESCRIPTION
Device Information	
System Name	This is the **System Name** you enter in the **Maintenance** > **System** > **General** screen. It is for identification purposes.
Firmware Version	This is the current firmware version of the WAP3205 v3.
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port’s IP address.
- IP Subnet Mask	This shows the LAN port’s subnet mask.
- DHCP Server	This shows the LAN port’s DHCP server status.
WLAN Information	
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Status	This shows the current status of the Wireless LAN - **On**, **Off**, or **Off by scheduler**.
- Name (SSID)	This shows a descriptive name used to identify the WAP3205 v3 in the wireless LAN.
- Channel	This shows the channel number which you select manually or the WAP3205 v3 automatically scans and selects.
- Operating Channel	This shows the channel number which the WAP3205 v3 is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the WAP3205 v3 is using.
- 802.11 Mode	This shows the IEEE 802.11 standard that the WAP3205 v3 supports. Wireless clients must support the same standard in order to be able to connect to the NBG-418N v2
- WPS	This shows the WPS (WiFi Protected Setup) Status. Click the status to display **Network** > **Wireless LAN** > **WPS** screen.
System Status	
Operation Mode	This field shows the device operation mode: **Access Point**, or **Universal Repeater**.
System Up Time	This is the total time the WAP3205 v3 has been on.
Current Date/Time	This field displays your WAP3205 v3’s present date and time.
System Setting	
Firewall	This shows the firewall settings on the WAP3205 v3.
UPnP	This shows the UPnP
Summary	
DHCP Table	This shows the DHCP clients.
Packet Statistics	Use this screen to view port status and packet specific statistics.

4.3.2 AP Navigation Panel

Use the menu in the navigation panel to configure WAP3205 v3 features in **AP Mode**. The following screen and table show the features you can configure in **AP Mode**.

Figure 26 Menu: AP Mode



The following table describes the sub-menus.

Table 13 Menu: AP Mode

LINK	TAB	FUNCTION
Network		
Wireless LAN	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the WAP3205 v3 to block access to devices or block the devices from accessing the WAP3205 v3.
	Advanced	This screen allows you to configure advanced wireless settings.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
	MBSSID	Use this screen to set the SSID for wireless AP.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
Maintenance		
System	General	Use this screen to view and change administrative settings such as system and domain names, password and inactivity timer.
	Time Setting	Use this screen to change your WAP3205 v3's time and date.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
Tools	Firmware	Use this screen to upload firmware to your WAP3205 v3.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your WAP3205 v3.
	Restart	This screen allows you to reboot the WAP3205 v3 without turning the power off.
Sys OP Mode	General	This screen allows you to select the device operation mode: **Access Point**, or **Universal Repeater**.
Language	Language	This screen allows you to select the language you prefer.

4.4 Setting your WAP3205 v3 to Universal Repeater Mode

1 Connect your computer to the LAN port of the WAP3205 v3.

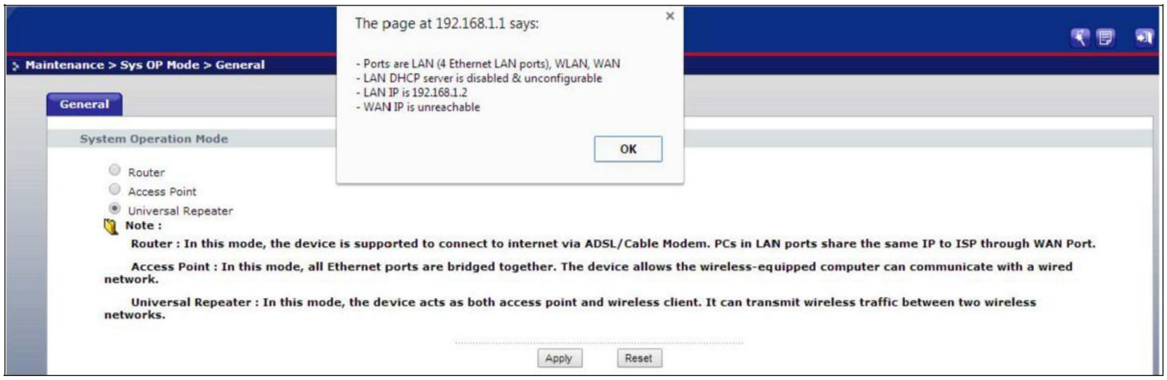
2 The default LAN IP address of the WAP3205 v3 is 192.168.1.2, you must set your computer to get an IP address automatically (computer factory default) or give it a fixed IP address in the range between 192.168.1.3 and 192.168.1.254.

3 After you've set your computer's IP address, open a web browser such as Internet Explorer and type the IP address of the WAP3205 v3 as the web address in your web browser.

4 Log into the Web Configurator. See the Chapter 2 on page 17 for instructions on how to do this.

5 Go to **Maintenance > Sys OP Mode > General** and select **Universal Repeater**.

Figure 27 Maintenance > Sys OP Mode > General



The page at 192.168.1.1 says:

- Ports are LAN (4 Ethernet LAN ports), WLAN, WAN
- LAN DHCP server is disabled & unconfigurable
- LAN IP is 192.168.1.2
- WAN IP is unreachable

○ Router
○ Access Point
● Universal Repeater

Note :

Router : In this mode, the device is supported to connect to internet via ADSL/Cable Modem. PCs in LAN ports share the same IP to ISP through WAN Port.

Access Point : In this mode, all Ethernet ports are bridged together. The device allows the wireless-equipped computer can communicate with a wired network.

Universal Repeater : In this mode, the device acts as both access point and wireless client. It can transmit wireless traffic between two wireless networks.

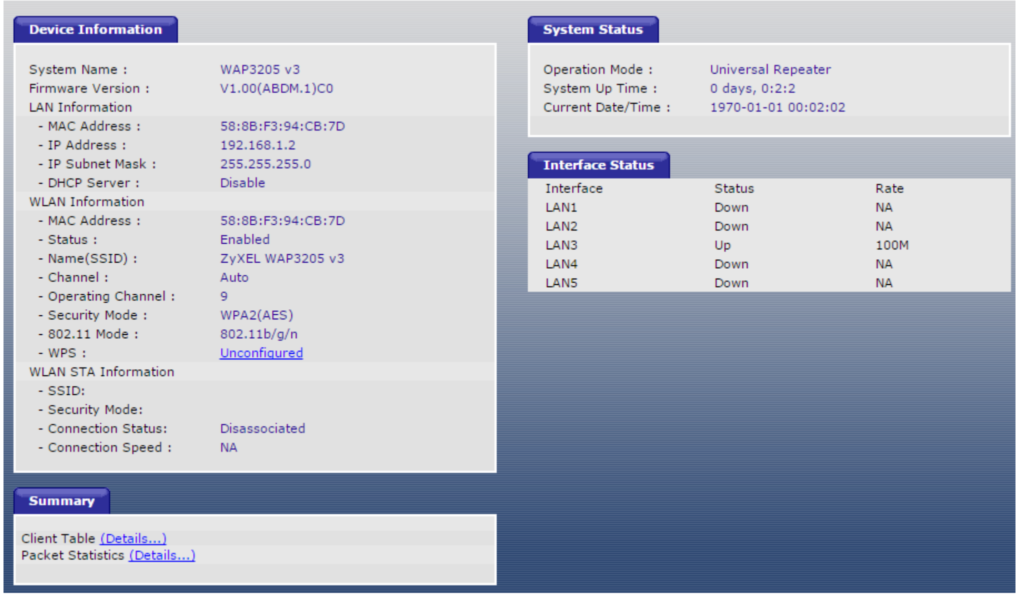
6 A pop-up window appears providing information on this mode. Click **OK** in the pop-up message window. Click **Apply**. Your WAP3205 v3 is now in **Universal Repeater** mode.

Note: Wait while the WAP3205 v3 restarts, then log in to the Web Configurator again.

4.4.1 Status Screen (Universal Repeater Mode)

Click on **Status**. The screen below shows the status screen in Universal Repeater **Mode**.

Figure 28 Status Screen (Universal Repeater Mode)



Device Information

System Name :	WAP3205 v3
Firmware Version :	V1.00(ABDM.1)C0
LAN Information	
- MAC Address :	58:8B:F3:94:CB:7D
- IP Address :	192.168.1.2
- IP Subnet Mask :	255.255.255.0
- DHCP Server :	Disable
WLAN Information	
- MAC Address :	58:8B:F3:94:CB:7D
- Status :	Enabled
- Name(SSID) :	ZyXEL WAP3205 v3
- Channel :	Auto
- Operating Channel :	9
- Security Mode :	WPA2(AES)
- 802.11 Mode :	802.11b/g/n
- WPS :	Unconfigured
WLAN STA Information	
- SSID:	
- Security Mode:	
- Connection Status:	Disassociated
- Connection Speed :	NA

Summary

Client Table (Details...)
Packet Statistics (Details...)

System Status

Operation Mode :	Universal Repeater
System Up Time :	0 days, 0:2:2
Current Date/Time :	1970-01-01 00:02:02

Interface Status

Interface	Status	Rate
LAN1	Down	NA
LAN2	Down	NA
LAN3	Up	100M
LAN4	Down	NA
LAN5	Down	NA

The following table describes the labels shown in the **Status** screen.

Table 14 Status Screen (Universal Repeater Mode)

LABEL	DESCRIPTION
Device Information	
System Name	This is the **System Name** you enter in the **Maintenance** > **System** > **General** screen. It is for identification purposes.
Firmware Version	This is the current firmware version of the WAP3205 v3.
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port’s IP address.
- IP Subnet Mask	This shows the LAN port’s subnet mask.
- DHCP Server	This shows the LAN port’s DHCP server.
WLAN AP Information	
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Status	This shows the current status of the Wireless LAN - **On**, **Off**, or **Off by scheduler**.
- Name (SSID)	This shows a descriptive SSID name used to identify the WAP3205 v3 in the wireless LAN.
- Channel	This shows the channel number which you select manually or the NBG-418N v2 automatically scans and selects.
- Operating Channel	This shows the channel number which the WAP3205 v3 is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the WAP3205 v3 is using.
- 802.11 Mode	This shows the IEEE 802.11 standard that the WAP3205 v3 supports. Wireless clients must support the same standard in order to be able to connect to the WAP3205 v3

Table 14 Status Screen (Universal Repeater Mode) (continued)

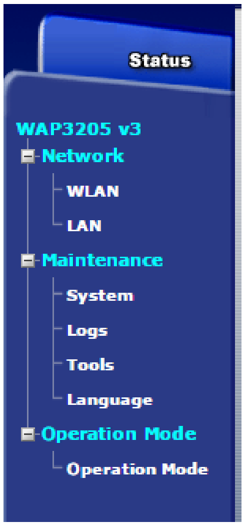
LABEL	DESCRIPTION
- WPS	This shows the WPS (WiFi Protected Setup) Status. Click the link to display **Network** > **Wireless LAN** > **WPS** screen.
WLAN STA Information	
- SSID	This is the name of the selected AP that the WAP3205 v3 is associating with.
- Security Mode	This shows the wireless security the WAP3205 v3 is using to connect to the AP.
- Connection Status	This shows whether the WAP3205 v3 is currently associated with the selected AP.
System Status	
Operation Mode	This field shows the device operation mode: **Access Point**, or **Universal Repeater**.
System Up Time	This is the total time the WAP3205 v3 has been on.
Current Date/Time	This field displays your WAP3205 v3's present date and time.
System Setting	
Firewall	This field shows the firewall status
UPnP	This field shows the UPnP status.
Summary	
DHCP table	Use this screen to view current DHCP client information.
Packet Statistics	Use this screen to view port status and packet specific statistics.
Message	Use this screen to view the status of the WAP3205 v3.

4.4.2 Universal Repeater Navigation Panel

Use the menu in the navigation panel to configure WAP3205 v3 features in **Universal Repeater Mode**.

The following screen and table show the features you can configure in **Universal Repeater Mode**.

Figure 29 Menu: Universal Repeater Mode



The following table describes the sub-menus.

Table 15 Menu: Universal Repeater Mode

LINK	TAB	FUNCTION
Status		This screen shows the WAP3205 v3's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
Network		
WLAN	AP Select	Use this screen to choose an access point that you want the WAP3205 v3 to connect to. You should know the security settings of the target AP.
	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the WAP3205 v3 to block access to devices or block the devices from accessing the WAP3205 v3.
	Advanced	This screen allows you to configure advanced wireless settings.
	QoS	Use this screen to configure Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
Maintenance		
System	General	Use this screen to view and change administrative settings such as system and domain names, password and inactivity timer.
	Time Setting	Use this screen to change your WAP3205 v3's time and date.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
Tools	Firmware	Use this screen to upload firmware to your WAP3205 v3.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your WAP3205 v3.
	Restart	This screen allows you to reboot the WAP3205 v3 without turning the power off.
Sys OP Mode	General	This screen allows you to select the device operation mode: **Access Point**, or **Universal Repeater**.
Language	Language	This screen allows you to select the language you prefer.

Tutorials

5.1 Overview

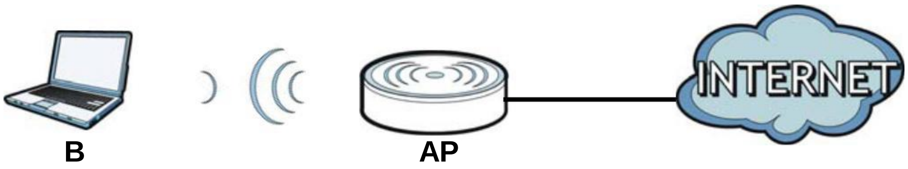
This chapter provides tutorials for your WAP3205 v3 as follows:

- How to Connect to the Internet from an AP
- Configure Wireless Security Using WPS on both your WAP3205 v3 and Wireless Client
- Enable and Configure Wireless Security without WPS on your WAP3205 v3
- Using Multiple SSIDs on the WAP3205 v3
- Using Bandwidth Management on the WAP3205 v3

5.2 How to Connect to the Internet from an AP

This section gives you an example of how to set up an access point (**AP**) and wireless client (a notebook, **B** in this example) for wireless communication. **B** can access the Internet through the AP wirelessly.

Figure 30 Wireless AP Connection to the Internet



5.3 Configure Wireless Security Using WPS on both your WAP3205 v3 and Wireless Client

This section gives you an example of how to set up wireless network using WPS. This example uses the WAP3205 v3 as the AP and NWD210N as the wireless client which connects to a notebook.

Note: The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCI card).

There are two WPS methods for creating a secure connection. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See Section 5.3.1 on page 45.This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the WAP3205 v3's interface. See Section 5.3.2 on page 46. This is the more secure method, since one device can authenticate the other.

5.3.1 Push Button Configuration (PBC)

1 Make sure that your WAP3205 v3 is turned on and that it is within range of your computer.

2 Make sure that you have installed the wireless client (this example uses the NWD210N) driver and utility in your notebook.

3 In the wireless client utility, find the WPS settings. Enable WPS and press the WPS button (**Start** or **WPS** button)

4 Log into WAP3205 v3's Web Configurator and press **Push Button** in the **Network** > **Wireless LAN** > **WPS Station** screen.

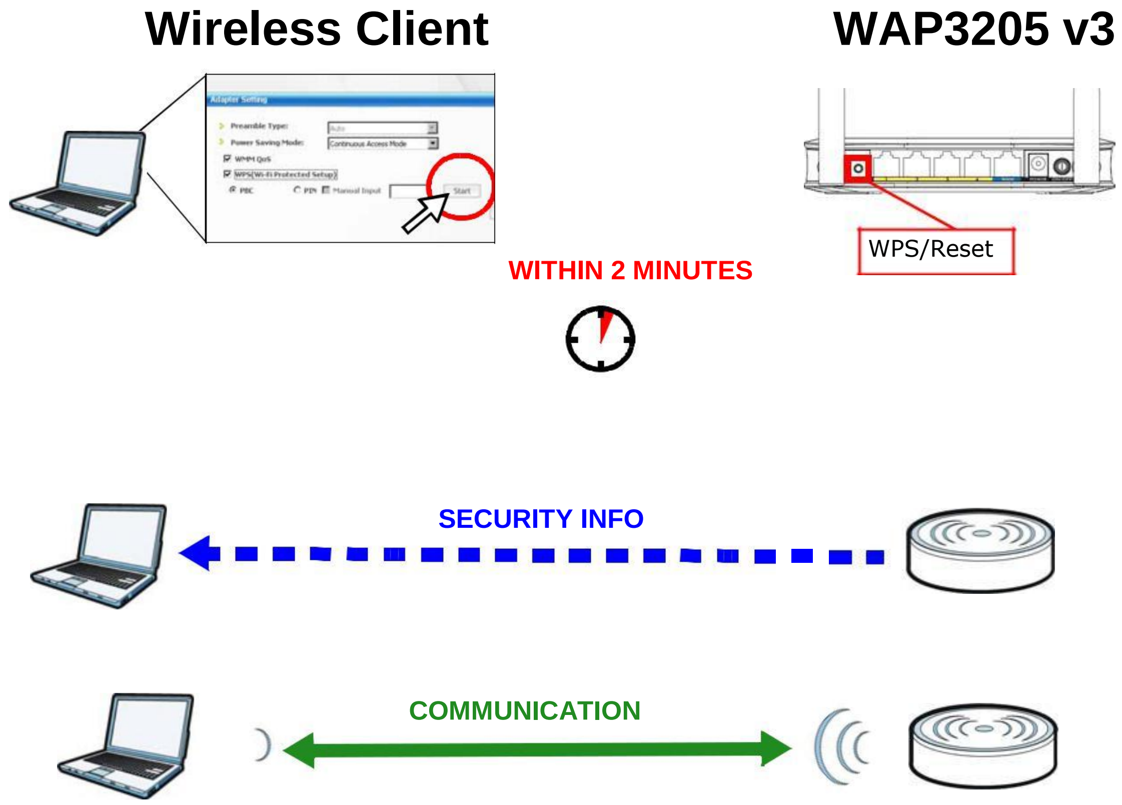
Note: Your WAP3205 v3 has a WPS/RESET button located on its back panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

Note: It doesn't matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

The WAP3205 v3 sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the WAP3205 v3 securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both WAP3205 v3 and wireless client (the NWD210N in this example).

Figure 31 Example WPS Process: PBC Method



5.3.2 PIN Configuration

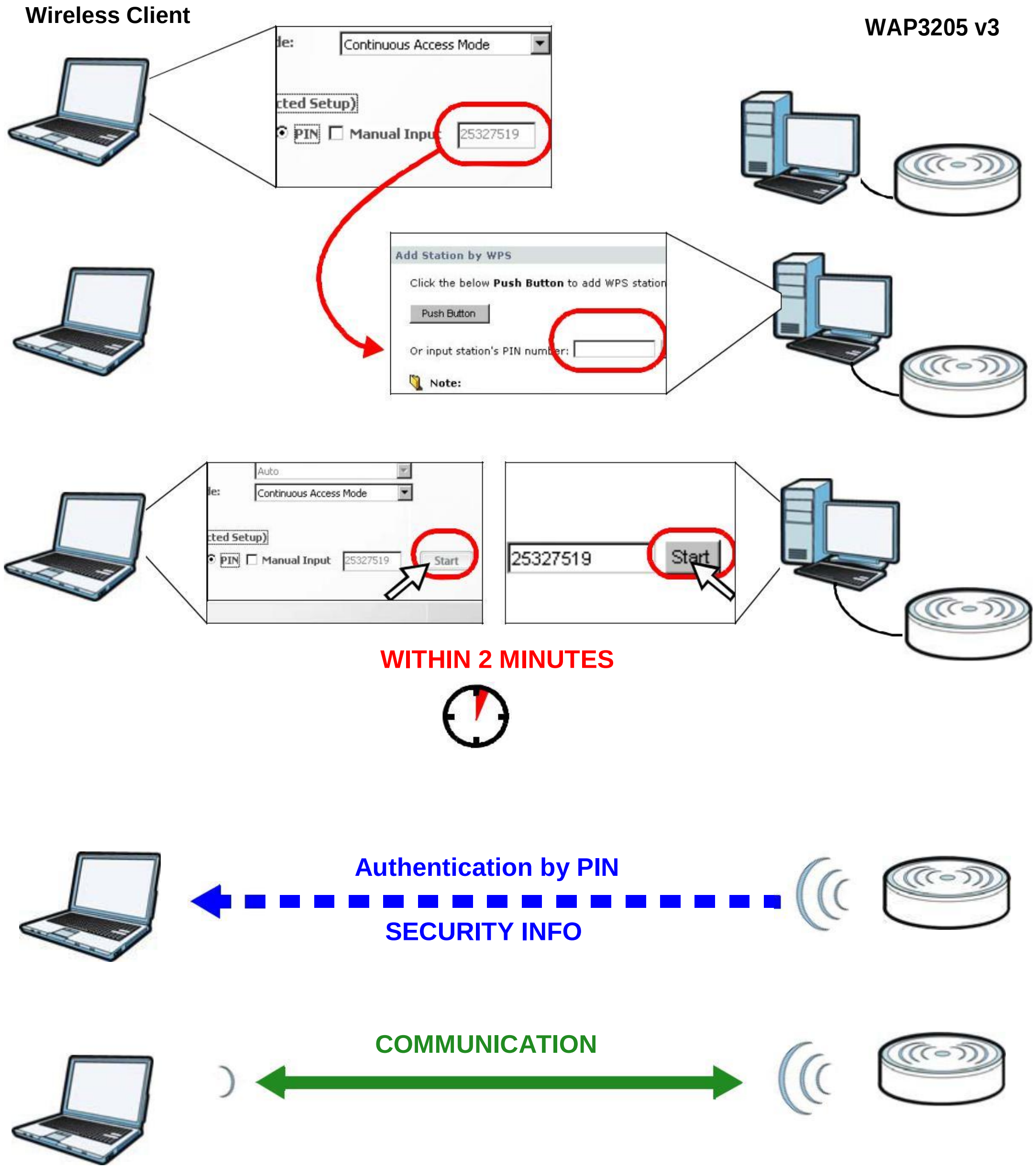
When you use the PIN configuration method, you need to use both WAP3205 v3’s configuration interface and the client’s utilities.

1. Launch your wireless client’s configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.
2. Enter the PIN number to the **PIN** field in the **Network** > **Wireless LAN** > **WPS Station** screen on the WAP3205 v3.
3. Click the **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the WAP3205 v3’s **WPS Station** screen within two minutes.

   The WAP3205 v3 authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the WAP3205 v3 securely.

   The following figure shows you the example to set up wireless network and security on WAP3205 v3 and wireless client (ex. NWD210N in this example) by using PIN method.

Figure 32 Example WPS Process: PIN Method



5.4 Enable and Configure Wireless Security without WPS on your WAP3205 v3

This example shows you how to configure wireless security settings with the following parameters on your WAP3205 v3.

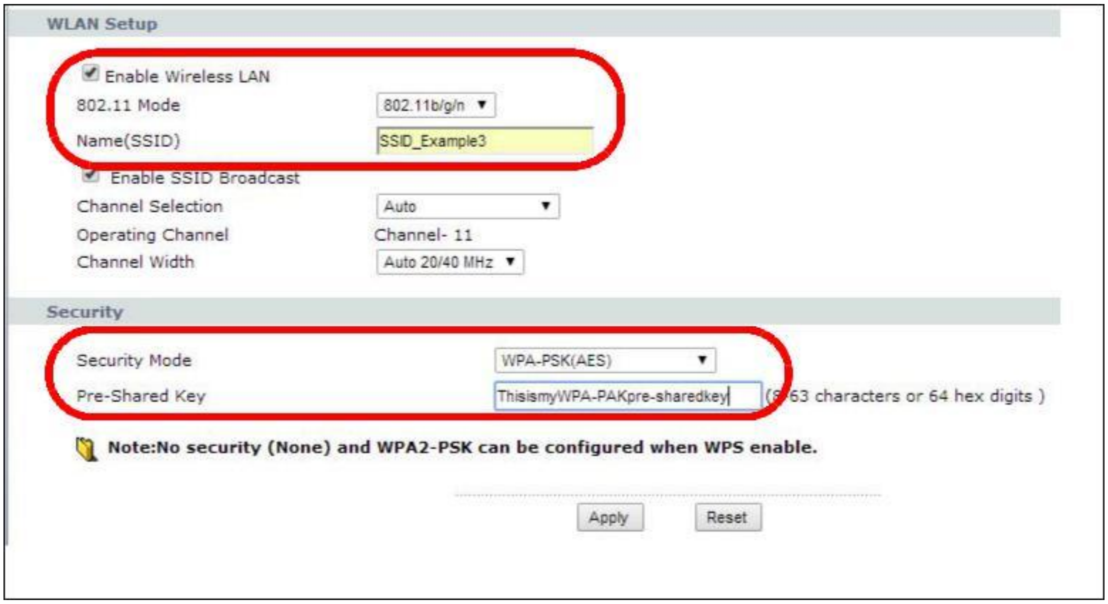
SSID	SSID_Example3
Channel	6
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

Follow the steps below to configure the wireless settings on your WAP3205 v3.

The instructions require that your hardware is connected (see the Quick Start Guide) and you are logged into the Web Configurator through your LAN connection (see Section 2.2 on page 17).

1. Open the **Wireless LAN > General** screen in the WAP3205 v3’s Web Configurator.
2. Make sure the **Enable Wireless LAN** check box is selected.
3. Enter **SSID_Example3** as the SSID and select a channel.
4. Set security mode to **WPA-PSK(AES)** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.

Figure 33 Tutorial: Network > Wireless LAN > General



WLAN Setup

☑ Enable Wireless LAN

802.11 Mode: 802.11b/g/n ▼

Name(SSID): SSID_Example3

☑ Enable SSID Broadcast

Channel Selection: Auto ▼

Operating Channel: Channel- 11

Channel Width: Auto 20/40 MHz ▼

Security

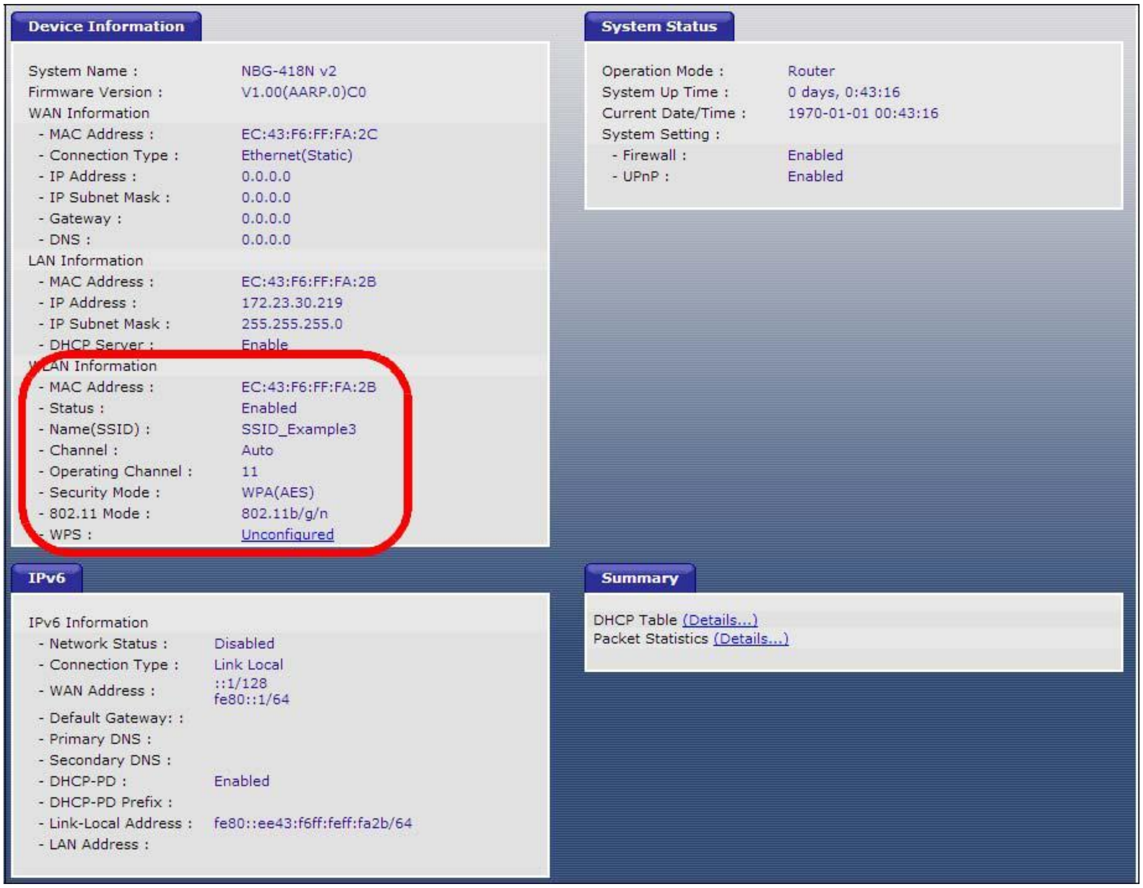
Security Mode: WPA-PSK(AES) ▼

Pre-Shared Key: ThisismyWPA-PAKpre-sharedkey (8~63 characters or 64 hex digits)

Note:No security (None) and WPA2-PSK can be configured when WPS enable.

5. Open the **Status** screen. Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.

Figure 34 Tutorial: Status Screen



Device Information

System Name :	NBG-418N v2
Firmware Version :	V1.00(AARP.0)C0
WAN Information	
- MAC Address :	EC:43:F6:FF:FA:2C
- Connection Type :	Ethernet(Static)
- IP Address :	0.0.0.0
- IP Subnet Mask :	0.0.0.0
- Gateway :	0.0.0.0
- DNS :	0.0.0.0
LAN Information	
- MAC Address :	EC:43:F6:FF:FA:2B
- IP Address :	172.23.30.219
- IP Subnet Mask :	255.255.255.0
- DHCP Server :	Enable
WLAN Information	
- MAC Address :	EC:43:F6:FF:FA:2B
- Status :	Enabled
- Name(SSID) :	SSID_Example3
- Channel :	Auto
- Operating Channel :	11
- Security Mode :	WPA(AES)
- 802.11 Mode :	802.11b/g/n
- WPS :	Unconfigured

System Status

Operation Mode :	Router
System Up Time :	0 days, 0:43:16
Current Date/Time :	1970-01-01 00:43:16
System Setting :	
- Firewall :	Enabled
- UPnP :	Enabled

IPv6

IPv6 Information	
- Network Status :	Disabled
- Connection Type :	Link Local
- WAN Address :	::1/128 fe80::1/64
- Default Gateway: :	
- Primary DNS :	
- Secondary DNS :	
- DHCP-PD :	Enabled
- DHCP-PD Prefix :	
- Link-Local Address :	fe80::ee43:f6ff:feff:fa2b/64
- LAN Address :	

Summary

DHCP Table (Details...)
Packet Statistics (Details...)

5.4.1 Configure Your Wireless Client

Note: We use the ZyXEL M-302 wireless adapter utility screens as an example for the wireless client. The screens may vary for different models.

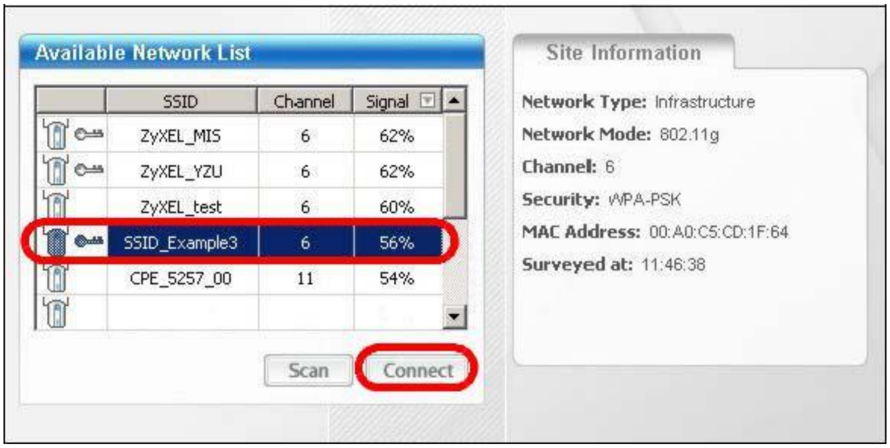
1 The WAP3205 v3 supports IEEE 802.11b, IEEE 802.11g and IEEE 802.11n wireless clients. Make sure that your notebook or computer’s wireless adapter supports one of these standards.

2 Wireless adapters come with software sometimes called a “utility” that you install on your computer. See your wireless adapter’s User’s Guide for information on how to do that.

3 After you’ve installed the utility, open it. If you cannot see your utility’s icon on your screen, go to **Start > Programs** and click on your utility in the list of programs that appears. The utility displays a list of APs within range, as shown in the example screen below.

4 Select **SSID_Example3** and click **Connect**.

Figure 35 Connecting a Wireless Client to a Wireless Network t



Available Network List

	SSID	Channel	Signal
	ZyXEL_MIS	6	62%
	ZyXEL_YZU	6	62%
	ZyXEL_test	6	60%
	SSID_Example3	6	56%
	CPE_5257_00	11	54%

Site Information

Network Type: Infrastructure

Network Mode: 802.11g

Channel: 6

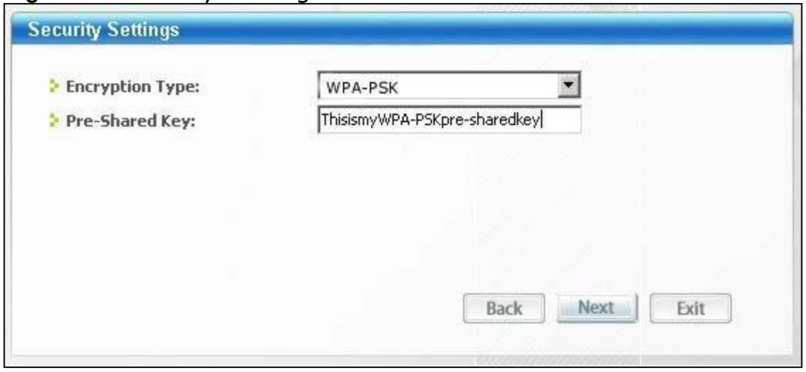
Security: WPA-PSK

MAC Address: 00:A0:C5:CD:1F:64

Surveyed at: 11:46:38

5 Select WPA2-PSK and type the security key in the following screen. Click **Next**.

Figure 36 Security Settings



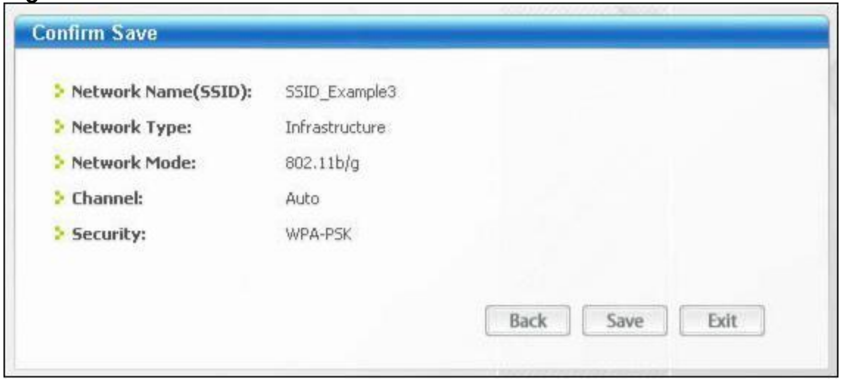
Security Settings

Encryption Type: WPA-PSK

Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

6 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

Figure 37 Confirm Save



Confirm Save

Network Name(SSID): SSID_Example3

Network Type: Infrastructure

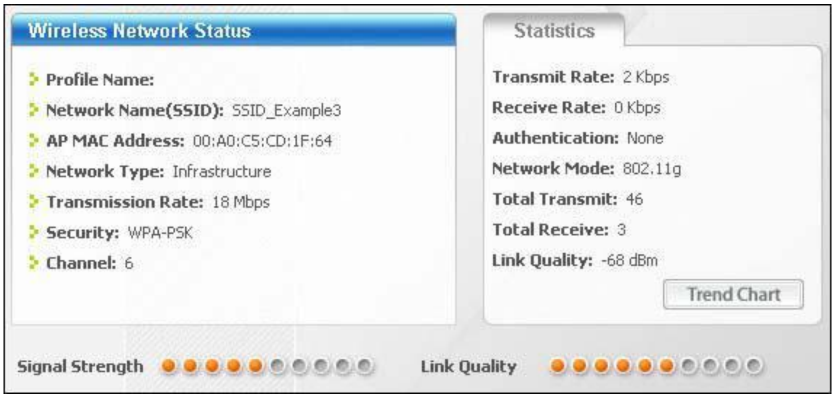
Network Mode: 802.11b/g

Channel: Auto

Security: WPA-PSK

7 Check the status of your wireless connection in the screen below. If your wireless connection is weak or you have no connection, see the Troubleshooting section of this User's Guide.

Figure 38 Link Status



Wireless Network Status

- Profile Name:
- Network Name(SSID): SSID_Example3
- AP MAC Address: 00:A0:C5:CD:1F:64
- Network Type: Infrastructure
- Transmission Rate: 18 Mbps
- Security: WPA-PSK
- Channel: 6

Statistics

Transmit Rate: 2 Kbps
Receive Rate: 0 Kbps
Authentication: None
Network Mode: 802.11g
Total Transmit: 46
Total Receive: 3
Link Quality: -68 dBm

If your connection is successful, open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

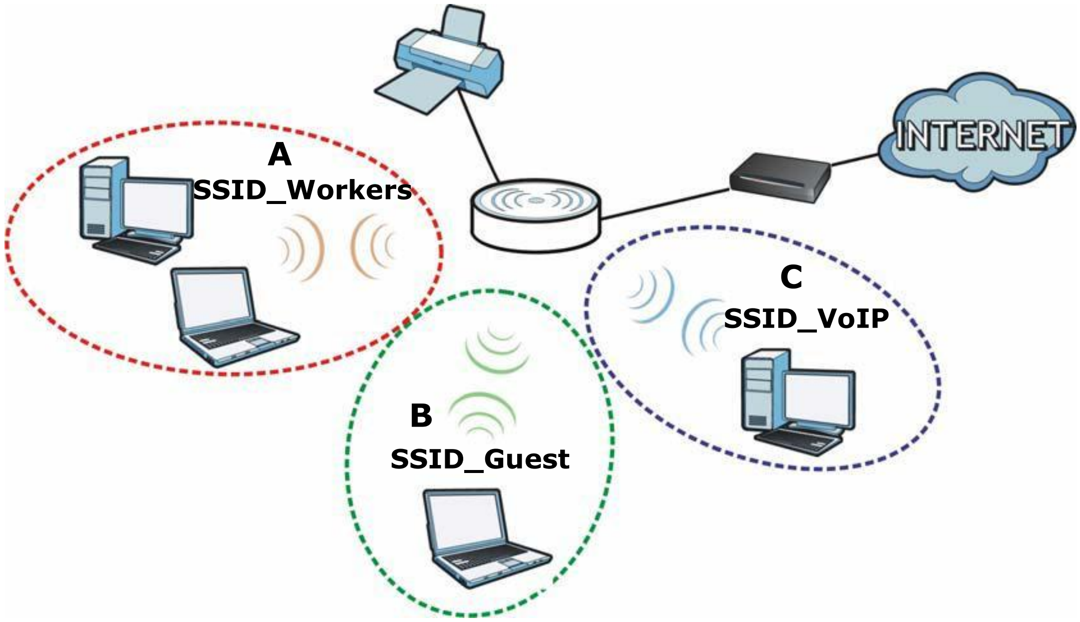
5.5 Using Multiple SSIDs on the WAP3205 v3

You can configure more than one SSID on a WAP3205 v3. See Section 11.4 on page 97.

This allows you to configure multiple independent wireless networks on the WAP3205 v3 as if there were multiple APs (virtual APs). Each virtual AP has its own SSID, wireless security type and MAC filtering settings. That is, each SSID on the WAP3205 v3 represents a different access point/ wireless network to wireless clients in the network.

Clients can associate only with the SSIDs for which they have the correct security settings. Clients using different SSIDs can access the Internet and the wired network behind the WAP3205 v3 (such as a printer).

For example, you may set up three wireless networks (**A**, **B** and **C**) in your office. **A** is for workers, **B** is for guests and **C** is specific to a VoIP device in the meeting room.



PART II

Technical Reference

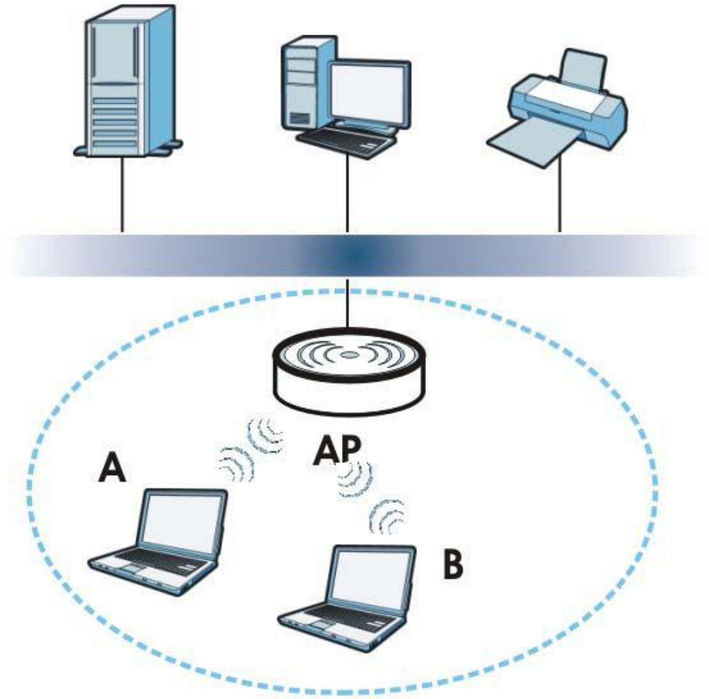
Wireless LAN

6.1 Overview

This chapter discusses how to configure the wireless network settings in your WAP3205 v3. See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 40 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** are called wireless clients. The wireless clients use the access point (**AP**) to interact with other devices (such as the printer) or with the Internet. Your WAP3205 v3 is the AP in the above example.

6.2 What You Can Do

Wireless screens vary according to the device mode you are using.

Wireless Screen	Access Point	Universal Repeater
General		
MAC Filter		
Advanced		
QoS		
WPS		
WPS Station		
Scheduling		
AP Select		

See Chapter 4 on page 29 for more information on device modes.

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the wireless security mode (Section 6.4 on page 63).
- Use the **MAC Filter** screen to allow or deny wireless stations based on their MAC addresses from connecting to the WAP3205 v3 (Section 6.5 on page 68).
- Use the **Advanced** screen to allow intra-BSS networking and set the RTS/CTS Threshold (Section 6.6 on page 69).
- Use the **WPS** screen to quickly set up a wireless network with strong security, without having to configure security settings manually (Section 6.7 on page 70).
- Use the **WPS Station** screen to add a wireless station using WPS (Section 6.8 on page 71).
- Use the **Scheduling** screen to set the times your wireless LAN is turned on and off (Section 6.9 on page 71).
- Use the **AP Select** screen to choose an access point that you want the WAP3205 v3 (in universal repeater mode) to connect to. You should know the security settings of the target AP (Section 6.11 on page 74).
- Use the **MBSSID** screen to view the SSID and security of the selected AP wireless network (Section 6.10 on page 72).

6.3 What You Should Know

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID. The

  SSID is the name of the wireless network. It stands for Service Set IDentity.

- If two wireless networks overlap, they should use different channels.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every wireless client in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

6.3.1 Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

6.3.2 MBSSID

Traditionally, you need to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there is also the possibility of channel interference. The WAP3205 v3's MBSSID (Multiple Basic Service Set IDentifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying QoS priorities and/or security modes to different SSIDs.

Wireless devices can use different BSSIDs to associate with the same AP.

6.3.2.1 Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.
- You must use different keys for different BSSs. If two wireless devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other's communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

6.3.3 MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

You can use the MAC address filter to tell the AP which wireless clients are allowed or not allowed to use the wireless network. If a wireless client is allowed to use the wireless network, it still has to have the correct settings (SSID, channel, and security). If a wireless client is not allowed to use the wireless network, it does not matter if it has the correct settings.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized wireless client. Then, they can use that MAC address to use the wireless network.

[1] Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.

[2] Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

6.3.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

Table 16 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION
Weakest	No Security
↕	Static WEP
	WPA-PSK
Strongest	WPA2-PSK

For example, if users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. Suppose the wireless network has two wireless clients. Device A only supports WEP, and device B supports WEP and WPA2-PSK. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use WPA2-PSK, or stronger encryption. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized devices to figure out the original information pretty quickly.

When you select **WPA2-PSK** in your WAP3205 v3, you can also select an option (**WPA Compatible**) to support WPA-PSK as well. In this case, if some wireless clients support WPA-PSK and some support WPA2-PSK, you should set up **WPA2-PSK** and select the **WPA Compatible** option in the WAP3205 v3.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every wireless client in the wireless network must have the same key.

6.3.5 WPS

WiFi Protected Setup (WPS) is an industry standard specification, defined by the WiFi Alliance. WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Depending on the devices in your network, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (Personal Identification Number) in the devices. Then, they connect and set up a secure network by themselves. See how to set up a secure wireless network using WPS in the Section 5.3 on page 44.

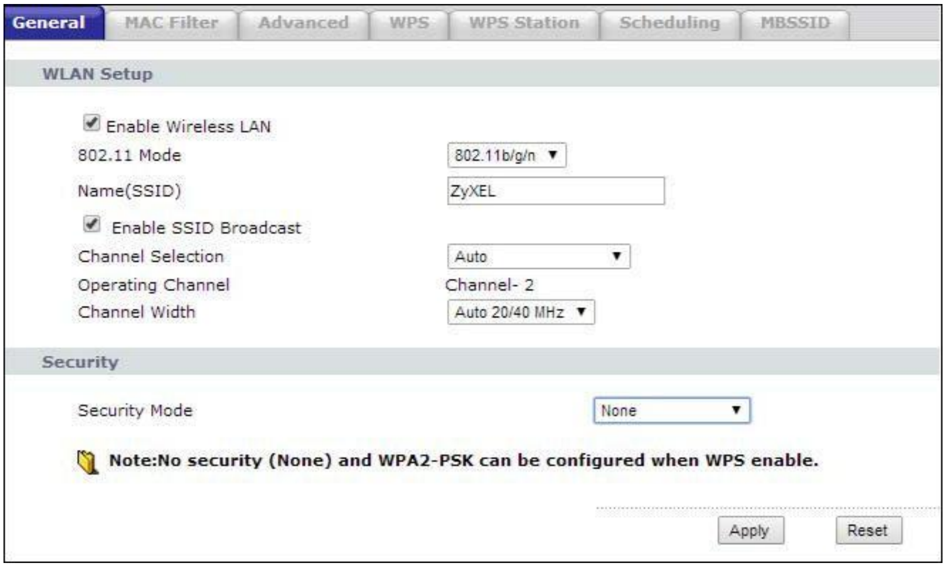
6.4 General Wireless LAN Screen

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode.

Note: If you are configuring the WAP3205 v3 from a computer connected to the wireless LAN and you change the WAP3205 v3's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the WAP3205 v3's new settings.

Click **Network** > **Wireless LAN** to open the **General** screen.

Figure 41 Network > Wireless LAN > General (Access Point Mode)



WLAN Setup

☑ Enable Wireless LAN

802.11 Mode: 802.11b/g/n ▼

Name(SSID): ZyXEL

☑ Enable SSID Broadcast

Channel Selection: Auto ▼

Operating Channel: Channel- 2

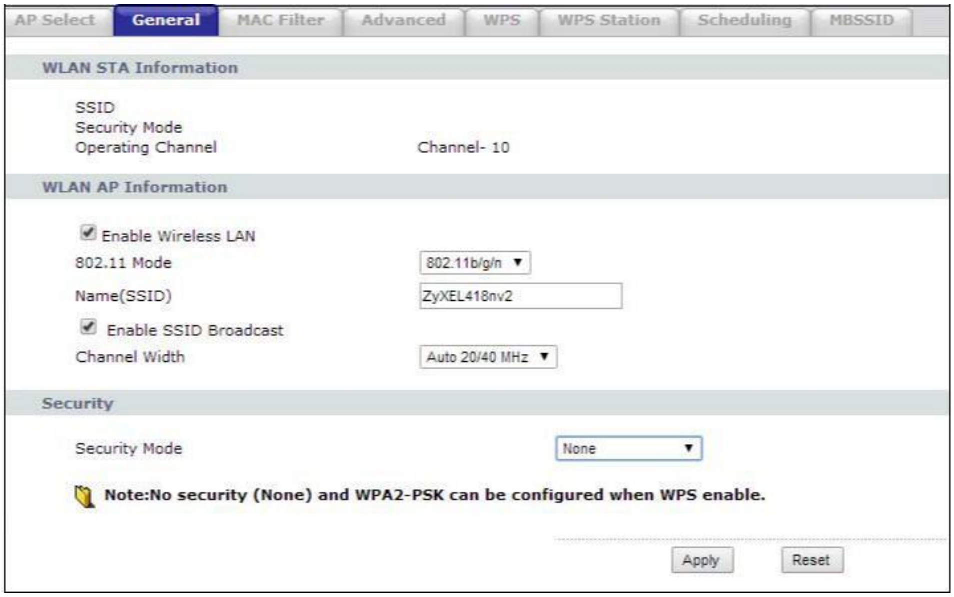
Channel Width: Auto 20/40 MHz ▼

Security

Security Mode: None ▼

Note:No security (None) and WPA2-PSK can be configured when WPS enable.

Figure 42 Network > Wireless LAN > General (Universal Repeater Mode)



WLAN STA Information

SSID

Security Mode

Operating Channel: Channel- 10

WLAN AP Information

☑ Enable Wireless LAN

802.11 Mode: 802.11b/g/n ▼

Name(SSID): ZyXEL418nv2

☑ Enable SSID Broadcast

Channel Width: Auto 20/40 MHz ▼

Security

Security Mode: None ▼

Note:No security (None) and WPA2-PSK can be configured when WPS enable.

The following table describes the general wireless LAN labels in this screen.

Table 17 Network > Wireless LAN > General

LABEL	DESCRIPTION
WLAN STA Information	This section is available only when the WAP3205 v3 is in universal repeater mode. This shows the wireless and security settings of the selected AP wireless network.
SSID	This displays the Service Set IDentity of the wireless device to which you are connecting.
Security Mode	This displays the type of security configured on the wireless device to which you are connecting.
Operating Channel	This displays the channel used by the wireless device to which you are connecting.
WLAN AP Information / Wireless Setup	Use this section to configure the wireless settings between the WAP3205 v3and its wireless clients.
Enable Wireless LAN	Click the check box to activate wireless LAN.
802.11 Mode	Click the drop-down list to choose the **802.11 mode** you want to operate.
Name(SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
Enable SSID Broadcast	Select the **Enable SSID Broadcast** check box to enable the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. Refer to the Connection Wizard chapter for more information on channels. This option is only available if **Auto Channel Selection** is disabled.
Operating Channel	This displays the channel the WAP3205 v3 is currently using.
Channel Width	Select whether the WAP3205 v3 uses a wireless channel width of **20MHz**, **40MHz** or **Auto 20/40MHz**. A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps. Because not all devices support 40MHz channels, select **Auto 20/40MHz** to allow the WAP3205 v3 to adjust the channel bandwidth automatically.
Security	Use this section to configure the wireless security between the WAP3205 v3 and its wireless clients.
Security Mode	Select **Static WEP**, **WPA-PSK** or **WPA2-PSK** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. See 6.4.2 and 6.4.3 sections. Or you can select **No Security** to allow any client to associate this network without authentication.
Apply	Click **Apply** to save your changes back to the WAP3205 v3.
Reset	Click **Reset** to reload the previous configuration for this screen.

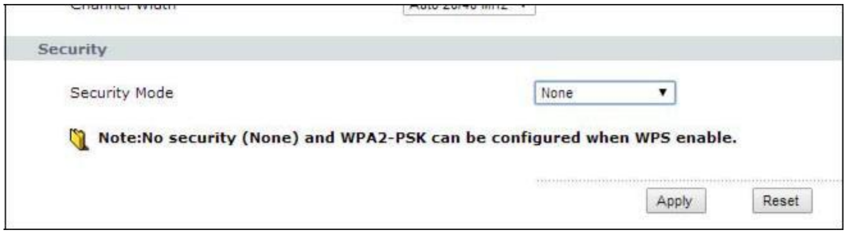
See the rest of this chapter for information on the other labels in this screen.

6.4.1 No Security

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption.

Note: If you do not enable any wireless security on your WAP3205 v3, your network is accessible to any wireless networking device that is within range.

Figure 43 Network > Wireless LAN > General: No Security



Security

Security Mode: None

Note:No security (None) and WPA2-PSK can be configured when WPS enable.

The following table describes the labels in this screen.

Table 18 Network > Wireless LAN > General: No Security

LABEL	DESCRIPTION
Security Mode	Choose **None** from the drop-down list box.
Apply	Click **Apply** to save your changes back to the WAP3205 v3.
Reset	Click **Reset** to reload the previous configuration for this screen.

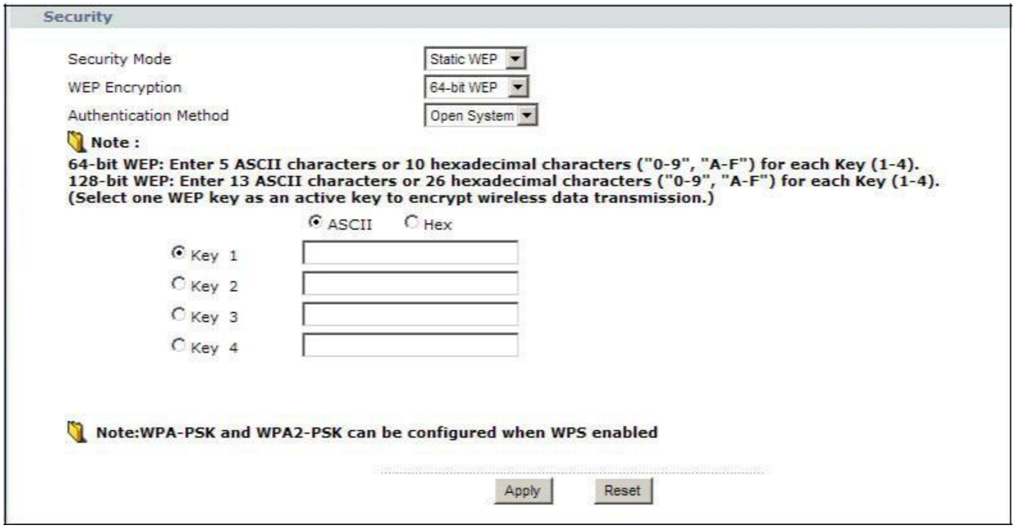
6.4.2 WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

Your WAP3205 v3 allows you to configure up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

In order to configure and enable WEP encryption; click **Network** > **Wireless LAN** to display the **General** screen. Select **Static WEP** from the **Security Mode** list.

Figure 44 Network > Wireless LAN > General: Static WEP



Security

Security Mode: Static WEP

WEP Encryption: 64-bit WEP

Authentication Method: Open System

Note :

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

Note:WPA-PSK and WPA2-PSK can be configured when WPS enabled

The following table describes the wireless LAN security labels in this screen.

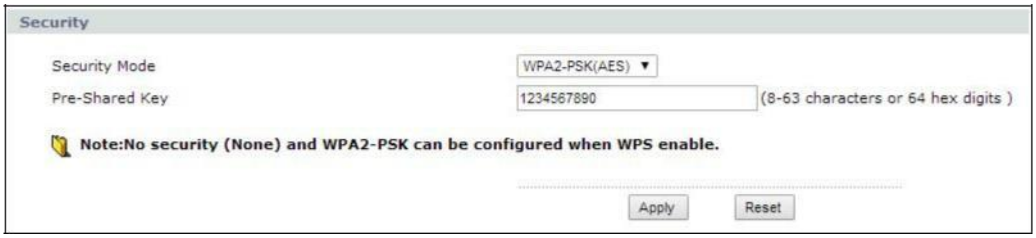
Table 19 Network > Wireless LAN > General: Static WEP

LABEL	DESCRIPTION
Security Mode	Choose **Static WEP** from the drop-down list box.
WEP Encryption	Select **64-bit WEP** or **128-bit WEP** to enable data encryption.
Authentication Method	Select **Auto, Open System** or **Shared Key** from the drop-down list box. This field specifies whether the wireless clients have to provide the WEP key to login to the wireless client. Keep this setting at **Auto** or **Open System** unless you want to force a key verification before communication between the wireless client and the ZyXEL Device occurs. Select **Shared Key** to force the clients to provide the WEP key prior to communication.
ASCII	Select this option in order to enter ASCII characters as WEP key.
Hex	Select this option in order to enter hexadecimal characters as a WEP key. The preceding "0x", that identifies a hexadecimal key, is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the WAP3205 v3 and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Apply	Click **Apply** to save your changes back to the WAP3205 v3.
Reset	Click **Reset** to reload the previous configuration for this screen.

6.4.3 WPA-PSK/WPA2-PSK

Click **Network** > **Wireless LAN** to display the **General** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 45 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK



Security

Security Mode: WPA2-PSK(AES)

Pre-Shared Key: 1234567890 (8-63 characters or 64 hex digits)

Note:No security (None) and WPA2-PSK can be configured when WPS enable.

The following table describes the labels in this screen.

Table 20 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Security Mode	Choose **WPA-PSK** or **WPA2-PSK** from the drop-down list box.
WPA Compatible	This option is available only when you select **WPA2-PSK** in the **Security Mode** field. Select this option to have both WPA2 and WPA wireless clients be able to communicate with the WAP3205 v3 even when the WAP3205 v3 is using WPA2-PSK.

Table 20 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK (continued)

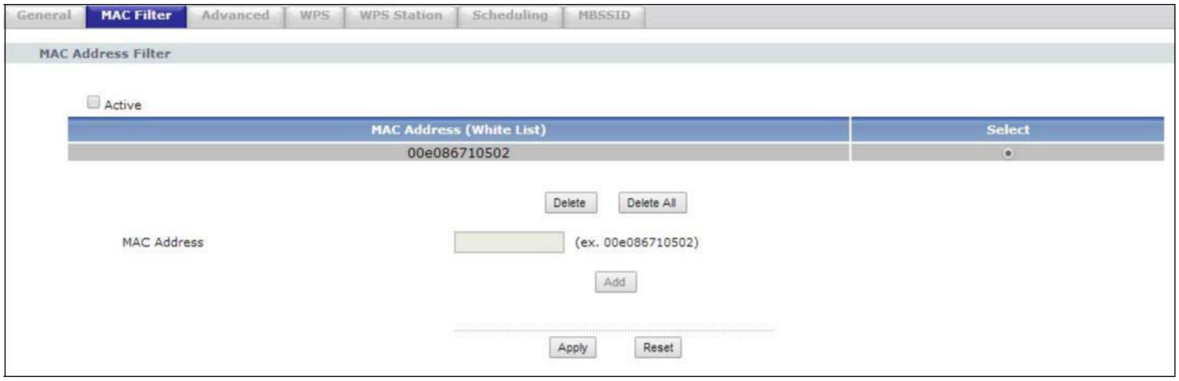
LABEL	DESCRIPTION
Cipher Type	Select the encryption type (**TKIP**, **AES** or **TKIP+AES**) for data encryption. Select **AES** if your wireless clients can all use AES. Otherwise, select **TKIP** or select **TKIP+AES** to allow the wireless clients to use either TKIP or AES
Pre-Shared Key	**WPA-PSK**/**WPA2-PSK** uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive **ASCII** characters (including spaces and symbols). Type a pre-shared key less than 64 case-sensitive **HEX** characters ("0-9", "A-F").
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK/WPA2-PSK** key management) or RADIUS server (if using **WPA/WPA2** key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA-PSK/WPA2-PSK** mode.
Apply	Click **Apply** to save your changes back to the WAP3205 v3.
Reset	Click **Reset** to reload the previous configuration for this screen.

6.5 MAC Filter

The MAC filter screen allows you to configure the WAP3205 v3 to give exclusive access to up to 16 devices (Allow) or exclude up to 16 devices from accessing the WAP3205 v3 (Deny). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your WAP3205 v3’s MAC filter settings, click **Network** > **Wireless LAN** > **MAC Filter**. The screen appears as shown.

Figure 46 Network > Wireless LAN > MAC Filter



MAC Address Filter

☐ Active

MAC Address (White List)	Select
00e086710502	●

MAC Address (ex. 00e086710502)

The following table describes the labels in this menu.

Table 21 Network > Wireless LAN > MAC Filter

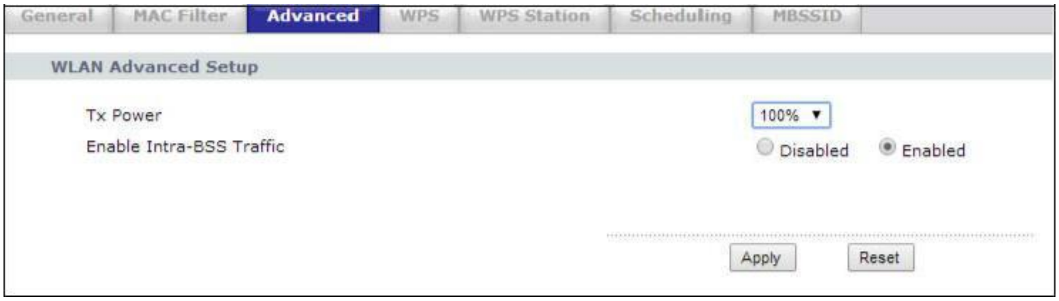
LABEL	DESCRIPTION
Active	Click **Active** check box to enable MAC address filtering.
MAC Address (White List)	This field shows the MAC addresses of the wireless station that are allowed or denied access to the WAP3205 v3 in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Select	Click the **Select** radio button to select a MAC filter entry.
Delete	Click the **Delete** button to delete the selected MAC filter entry.
Delete All	Click the **Delete All** button to remove all MAC filter entries.
MAC Address	Enter the **MAC addresses** of the wireless station that are allowed or denied access to the WAP3205 v3 in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Add	Click **Add** to add a new MAC address to the MAC Filtering rule.
Apply	Click **Apply** to save your changes back to the WAP3205 v3.
Reset	Click **Reset** to reload the previous configuration for this screen.

6.6 Wireless LAN Advanced Screen

Use this screen to allow intra-BSS networking and set the RTS/CTS Threshold.

Click **Network** > **Wireless LAN** > **Advanced**. The screen appears as shown.

Figure 47 Network > Wireless LAN > Advanced (Universal Repeater Mode)



WLAN Advanced Setup

Tx Power: 100%

Enable Intra-BSS Traffic: ○ Disabled ● Enabled

The following table describes the labels in this screen.

Table 22 Network > Wireless LAN > Advanced (Universal Repeater Mode)

LABEL	DESCRIPTION
Wireless Advanced Setup	
Tx Power	This field controls the transmission power of the WAP3205 v3. When using the NBG-418N v2 with a notebook computer, select a transmission power level from the drop-down list. Choose a lower transmission power level when you are close to the AP in order to conserve battery power.

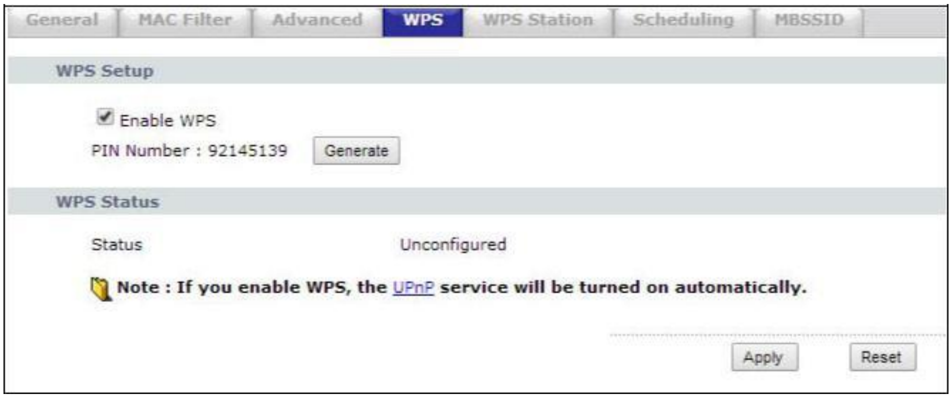
Table 22 Network > Wireless LAN > Advanced (Universal Repeater Mode)

LABEL	DESCRIPTION
Enable Intra-BSS Traffic	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.
Apply	Click **Apply** to save your changes to the WAP3205 v3.
Reset	Click **Reset** to reload the previous configuration for this screen.

6.7 WPS Screen

Use this screen to enable/disable WPS, view or generate a new PIN number and check current WPS status. To open this screen, click **Network** > **Wireless LAN** > **WPS** tab.

Figure 48 Network > Wireless LAN > WPS



WPS Setup

☑ Enable WPS

PIN Number : 92145139

WPS Status

Status Unconfigured

Note : If you enable WPS, the UPnP service will be turned on automatically.

The following table describes the labels in this screen.

Table 23 Network > Wireless LAN > WPS

LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Click the **Enable WPS** check box to enable the WPS feature. Click again to disable it.
PIN Number	This displays a PIN number last time system generated. Click **Generate** to generate a new PIN number.
WPS Status	
Status	This displays **Configured** when the WAP3205 v3 has connected to a wireless network using WPS or when **Enable WPS** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Unconfigured** if WPS is disabled and there are no wireless or wireless security changes on the WAP3205 v3 or you click **Release_Configuration** to remove the configured wireless and wireless security settings.
Release Configuration	This button is only available when the WPS status displays **Configured**. Click this button to remove all configured wireless and wireless security settings for WPS connections on the WAP3205 v3.

Table 23 Network > Wireless LAN > WPS (continued)

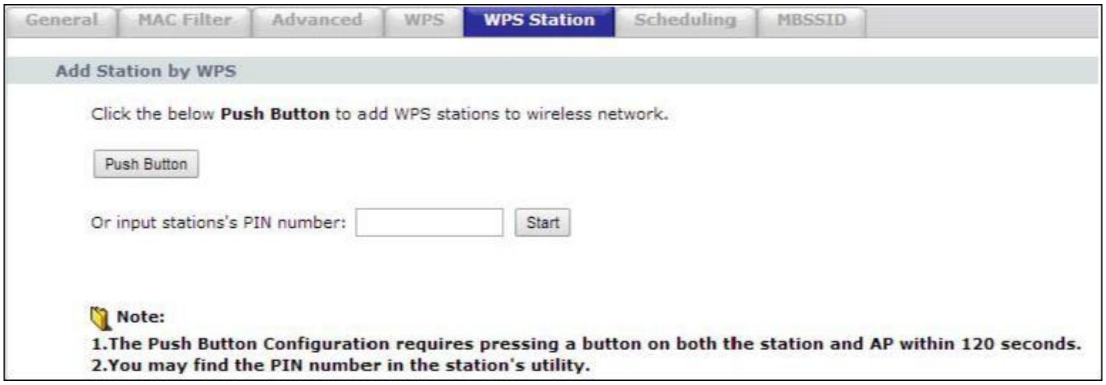
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the WAP3205 v3.
Refresh	Click **Refresh** to get this screen information afresh.

6.8 WPS Station Screen

Use this screen when you want to add a wireless station using WPS. To open this screen, click **Network** > **Wireless LAN** > **WPS Station** tab.

Note: Note: After you click **Push Button** on this screen, you have to press a similar button in the wireless station utility within 2 minutes. To add the second wireless station, you have to press these buttons on both device and the wireless station again after the first 2 minutes.

Figure 49 Network > Wireless LAN > WPS Station



Add Station by WPS

Click the below **Push Button** to add WPS stations to wireless network.

Or input stations's PIN number:

Note:
1.The Push Button Configuration requires pressing a button on both the station and AP within 120 seconds.
2.You may find the PIN number in the station's utility.

The following table describes the labels in this screen.

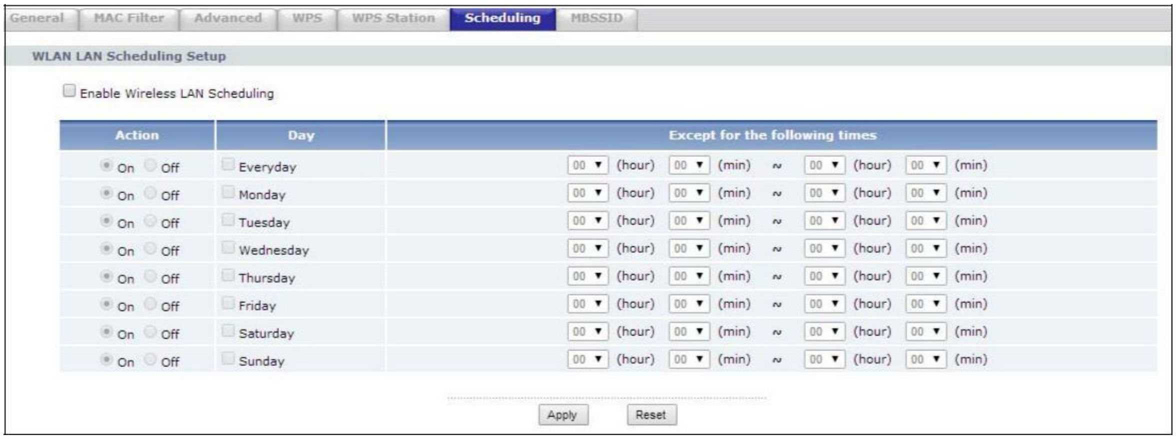
Table 24 Network > Wireless LAN > WPS Station

LABEL	DESCRIPTION
Push Button	Use this button when you use the PBC (Push Button Configuration) method to configure wireless stations’s wireless settings. See Section 5.3.1 on page 45. Click this to start WPS-aware wireless station scanning and the wireless security information synchronization.
Or input station’s PIN number	Use this button when you use the PIN Configuration method to configure wireless station’s wireless settings. See Section 5.3.2 on page 46. Type the same PIN number generated in the wireless station’s utility. Then click **Start** to associate to each other and perform the wireless security information synchronization.

6.9 Scheduling Screen

Use this screen to set the times your wireless LAN is turned on and off. Wireless LAN scheduling is disabled by default. The wireless LAN can be scheduled to turn on or off on certain days and at certain times. To open this screen, click **Network** > **Wireless LAN** > **Scheduling** tab.

Figure 50 Network > Wireless LAN > Scheduling



WLAN LAN Scheduling Setup

□ Enable Wireless LAN Scheduling

Action	Day	Except for the following times
● On ○ Off	□ Everyday	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
● On ○ Off	□ Monday	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
● On ○ Off	□ Tuesday	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
● On ○ Off	□ Wednesday	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
● On ○ Off	□ Thursday	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
● On ○ Off	□ Friday	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
● On ○ Off	□ Saturday	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
● On ○ Off	□ Sunday	00 (hour) 00 (min) ~ 00 (hour) 00 (min)

The following table describes the labels in this screen.

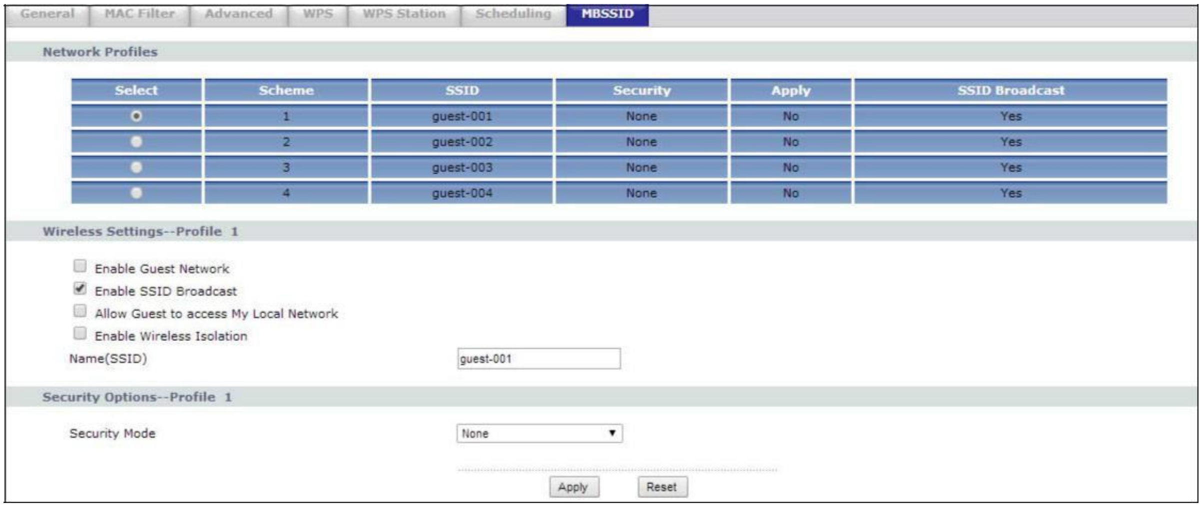
Table 25 Network > Wireless LAN > Scheduling

LABEL	DESCRIPTION
Enable Wireless LAN Scheduling	Select this to enable Wireless LAN scheduling.
Action	Select **On** or **Off** to specify whether the Wireless LAN is turned on or off. This field works in conjunction with the **Day** and **Except for the following times** fields.
Day	Select **Everyday** or the specific days to turn the Wireless LAN on or off. If you select **Everyday** you can not select any specific days. This field works in conjunction with the **Except for the following times** field.
Except for the following times	Select a begin time using the first set of **hour** and minute (**min**) drop down boxes and select an end time using the second set of **hour** and minute (**min**) drop down boxes. If you have chosen **On** earlier for the WLAN Status the Wireless LAN will turn off between the two times you enter in these fields. If you have chosen **Off** earlier for the WLAN Status the Wireless LAN will turn on between the two times you enter in these fields. Note: Entering the same begin time and end time will mean the whole day.
Apply	Click **Apply** to save your changes back to the WAP3205 v3.
Reset	Click **Reset** to reload the previous configuration for this screen.

6.10 MBSSID Screen

Use this screen to set multiple SSID (MBSSID) for the wireless clients on the WAP3205 v3. Click **Network** > **Wireless LAN** > **MBSSID** to open the following screen.

Figure 51 Network > Wireless LAN > MBSSID



Network Profiles

Select	Scheme	SSID	Security	Apply	SSID Broadcast
●	1	guest-001	None	No	Yes
○	2	guest-002	None	No	Yes
○	3	guest-003	None	No	Yes
○	4	guest-004	None	No	Yes

Wireless Settings--Profile 1

□ Enable Guest Network
☑ Enable SSID Broadcast
□ Allow Guest to access My Local Network
□ Enable Wireless Isolation

Name(SSID) guest-001

Security Options--Profile 1

Security Mode None

The following table describes the labels in this screen.

Table 26 Network > Wireless LAN > MBSSID

LABEL	DESCRIPTION
Network Profiles	
Select	Click the **Select** radio button to select the Multiple Basic Service Set Identifier (MBSSID) you wish to edit.
Scheme	This field displays the index number of the SSID.
SSID	This field displays the **SSID** name of the Wireless client.
Security	This field displays the **Security** mode of the wireless client. If there’s no security, it will display **None**.
Apply	This field displays whether the **Enable Guest Network** check box of the SSID is enabled.
SSID Broadcast	This field displays whether the **Enable SSID Broadcast** check box of the SSID is enabled.
Wireless Settings--Profile 1	
Enable Guest Network	Click the **Enable Guest Network** check box to enable this SSID wireless client.
Enable SSID Broadcast	Click the **Enable SSID Broadcast** check box to activate the SSID broadcast to different wireless clients.
Allow Guest to access My Local Network	Click the **Allow Guest to access my Local Network** check box to allow the client to access the local network resources behind the WAP3205 v3.
Enable Wireless Isolation	Click the **Enable Wireless Isolation** check box to keep the wireless clients in this SSID from communicating with each other through the WAP3205 v3.
Name (SSID)	This field displays the **SSID** name you selected using the select radio button.
Security Options--Profile1	
Security Mode	Select Basic **WEP** or More Secure **WPA2-PSK** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Device. When you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about this field.

Table 26 Network > Wireless LAN > MBSSID

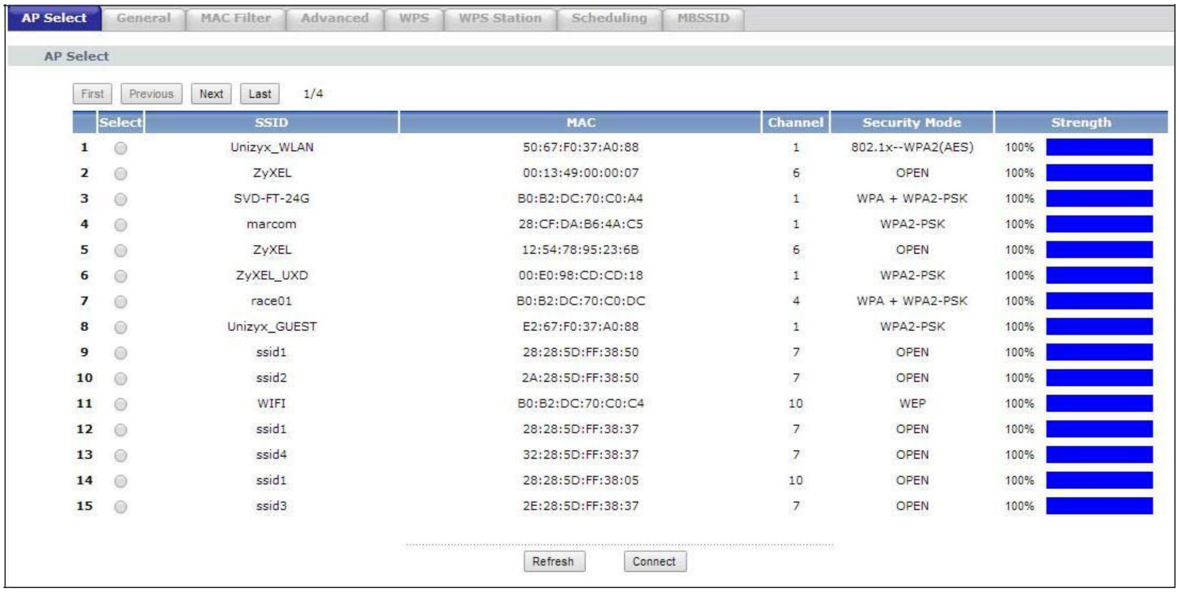
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the WAP3205 v3.
Reset	Click **Reset** to reload the previous configuration for this screen.

6.11 AP Select Screen

Use this screen to choose an access point that you want the WAP3205 v3 in universal repeater mode) to connect to. You should know the security settings of the target AP.

To open this screen, click **Network** > **Wireless LAN** > **AP Select** tab.

Figure 52 Network > Wireless LAN > AP Select



	Select	SSID	MAC	Channel	Security Mode	Strength
1	○	Unizyx_WLAN	50:67:F0:37:A0:88	1	802.1x--WPA2(AES)	100%
2	○	ZyXEL	00:13:49:00:00:07	6	OPEN	100%
3	○	SVD-FT-24G	B0:B2:DC:70:C0:A4	1	WPA + WPA2-PSK	100%
4	○	marcom	28:CF:DA:B6:4A:C5	1	WPA2-PSK	100%
5	○	ZyXEL	12:54:78:95:23:6B	6	OPEN	100%
6	○	ZyXEL_UXD	00:E0:98:CD:CD:18	1	WPA2-PSK	100%
7	○	race01	B0:B2:DC:70:C0:DC	4	WPA + WPA2-PSK	100%
8	○	Unizyx_GUEST	E2:67:F0:37:A0:88	1	WPA2-PSK	100%
9	○	ssid1	28:28:5D:FF:38:50	7	OPEN	100%
10	○	ssid2	2A:28:5D:FF:38:50	7	OPEN	100%
11	○	WIFI	B0:B2:DC:70:C0:C4	10	WEP	100%
12	○	ssid1	28:28:5D:FF:38:37	7	OPEN	100%
13	○	ssid4	32:28:5D:FF:38:37	7	OPEN	100%
14	○	ssid1	28:28:5D:FF:38:05	10	OPEN	100%
15	○	ssid3	2E:28:5D:FF:38:37	7	OPEN	100%

The following table describes the labels in this screen.

Table 27 Network > Wireless LAN > AP Select

LABEL	DESCRIPTION
AP Select	
First	Click **First** button to go to the first page of the AP select table.
Previous	Click **Previous** button to go to the Previous page in the AP select table.
Next	Click **Next** button to go to the next page in the AP select table.
Last	Click **Last** button to go to the last page of the AP select table.
Select	Use the radio button to select the wireless device to which you want to connect.
SSID	This displays the Service Set IDentity of the wireless device. The SSID is a unique name that identifies a wireless network. All devices in a wireless network must use the same SSID.
MAC	This displays the MAC address of the wireless device.
Channel	This displays the channel number used by this wireless device.

Table 27 Network > Wireless LAN > AP Select (continued)

LABEL	DESCRIPTION
Mode	This displays which IEEE 802.11b/g/n wireless networking standards the wireless device supports.
Security Mode	This displays the type of security configured on the wireless device. **OPEN** means no security is configured and you can connect to it without a password.
Strength	This displays the strength of the wireless signal. The signal strength mainly depends on the antenna output power and the distance between your WAP3205 v3 and this device.
Refresh	Click this button to search for available wireless devices within transmission range and update this table.
Connect	Click this button to associate to the selected wireless device.

6

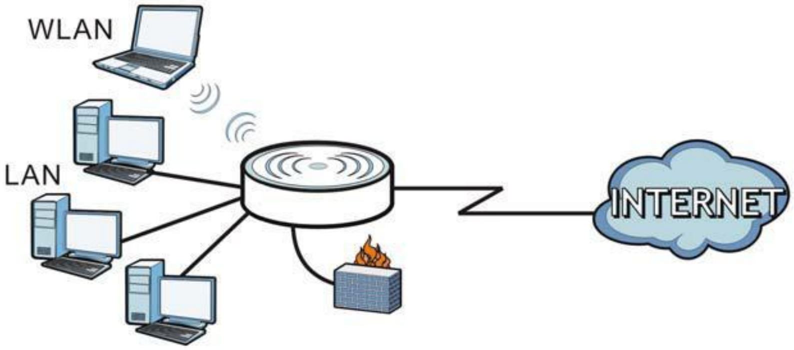
LAN

8.1 Overview

This chapter describes how to configure LAN settings.

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, and partition your physical network into logical networks.

Figure 64 LAN Setup

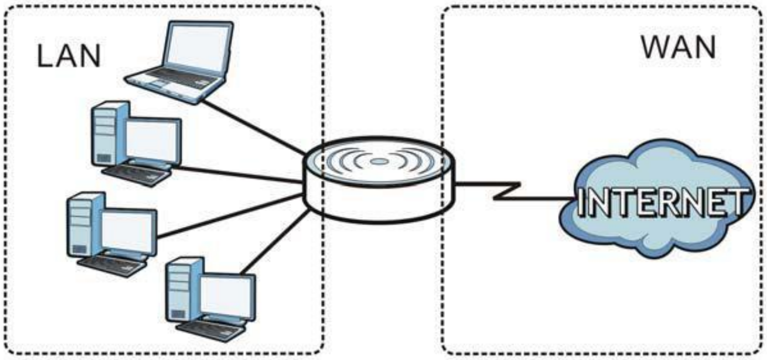


The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

8.2 What You Need To Know

The actual physical connection determines whether the WAP3205 v3 ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 65 LAN and WAN IP Addresses



The LAN parameters of the WAP3205 v3 are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded Web Configurator help regarding what fields need to be configured.

8.2.1 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your WAP3205 v3, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your WAP3205 v3 will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the WAP3205 v3 unless you are instructed to do otherwise.

8.2.2 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The WAP3205 v3 can get the DNS server addresses in the following ways.

1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **Wizard** and/or **WAN > Internet Connection** screen.

2 If the ISP did not give you DNS server information, leave the **DNS Server** fields set to **0.0.0.0** in the **Wizard** screen and/or set to **From ISP** in the **WAN > Internet Connection** screen for the ISP to dynamically assign the DNS server IP addresses.

8.2.3 IP Pool Setup

The WAP3205 v3 is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the WAP3205 v3 itself) in the lower range (192.168.1.2 to 192.168.1.32) for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

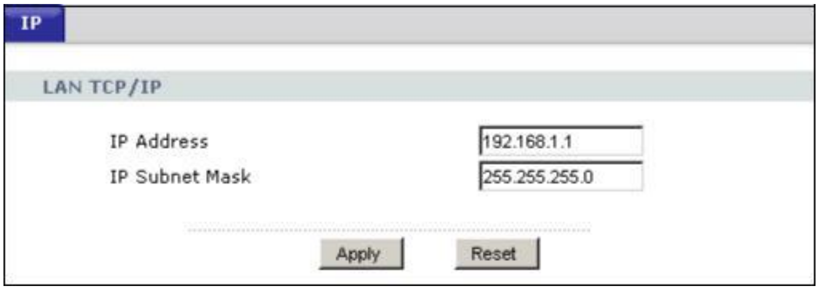
8.2.4 LAN TCP/IP

The WAP3205 v3 has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

8.3 LAN IP Screen

Use this screen to change your basic LAN settings. Click **Network** > **LAN**.

Figure 66 Network > LAN > IP



IP Address: 192.168.1.1
IP Subnet Mask: 255.255.255.0

The following table describes the labels in this screen.

Table 38 Network > LAN > IP

LABEL	DESCRIPTION
IP Address	Type the IP address of your WAP3205 v3 in dotted decimal notation 192.168.1.1 (factory default).

Table 38 Network > LAN > IP (continued)

LABEL	DESCRIPTION
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG-418N v2 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the WAP3205 v3.
Apply	Click **Apply** to save your changes back to the WAP3205 v3.
Reset	Click **Reset** to begin configuring this screen afresh.

Language

20.1 Language Screen

Use this screen to change the language for the Web Configurator display.

Click the language you prefer. The Web Configurator language changes after a while without restarting the WAP3205 v3.

Figure 109 Language

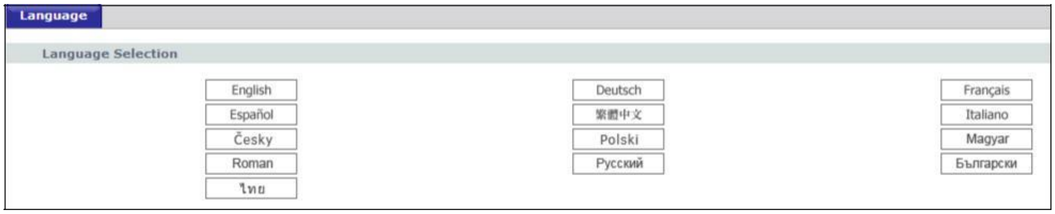
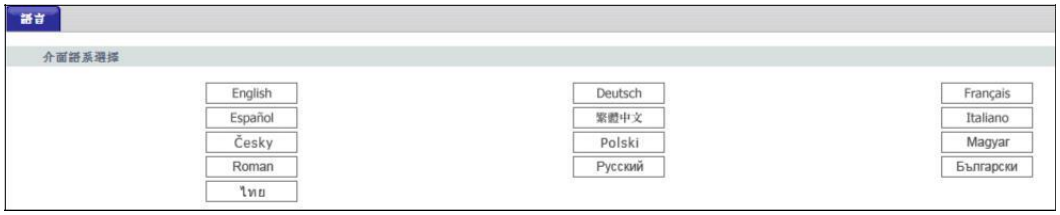


Figure 110 Language Change Example



8

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: The screens used below belong to Internet Explorer version 6, 7 and 8. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

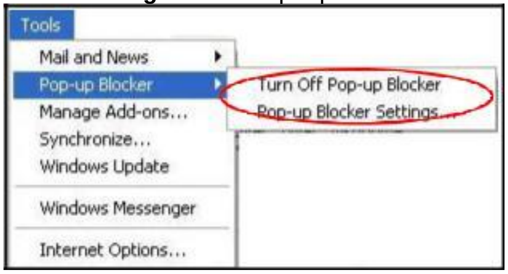
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 117 Pop-up Blocker

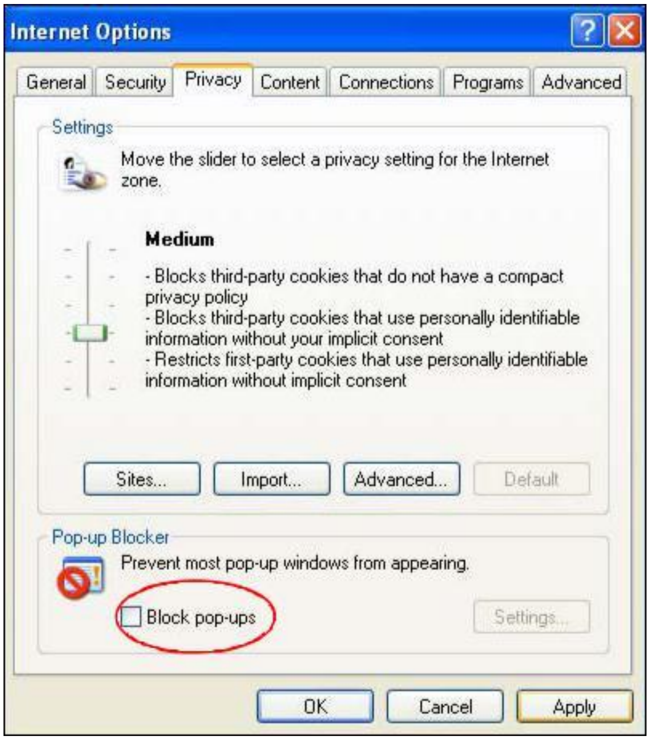


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 118 Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Prevent most pop-up windows from appearing.

□ Block pop-ups

3 Click **Apply** to save this setting.

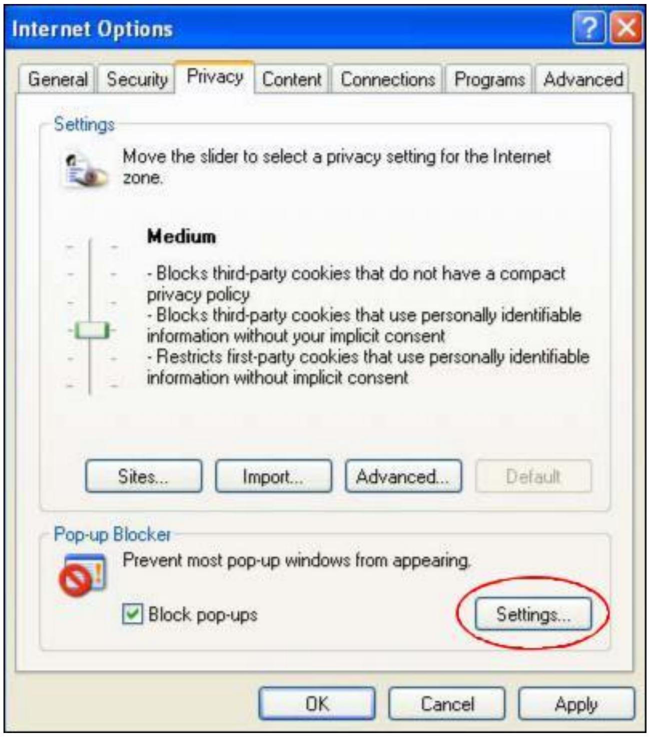
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

Figure 119 Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

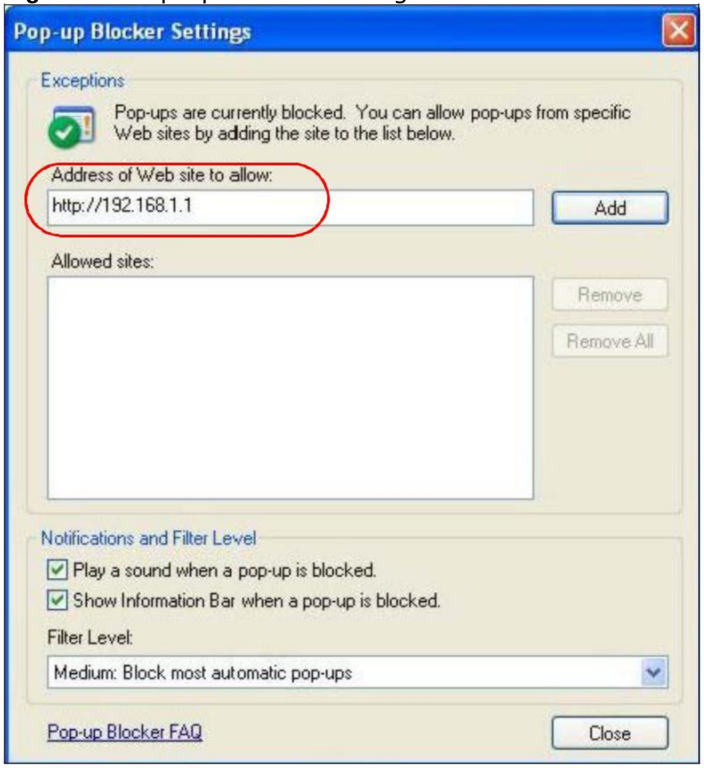
Prevent most pop-up windows from appearing.

☑ Block pop-ups

3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 120 Pop-up Blocker Settings



Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow: http://192.168.1.1

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level: Medium: Block most automatic pop-ups

5 Click **Close** to return to the **Privacy** screen.

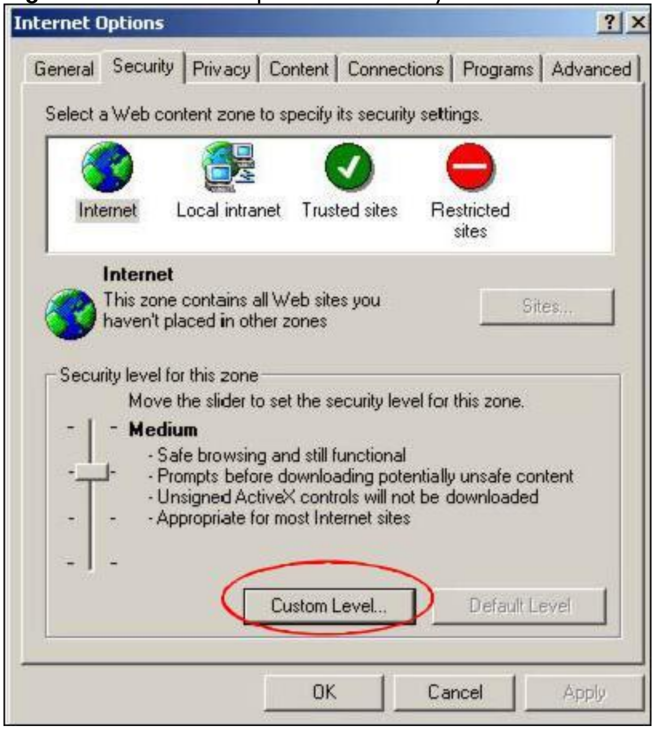
6 Click **Apply** to save this setting.

JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 121 Internet Options: Security



Select a Web content zone to specify its security settings.

Internet

This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Move the slider to set the security level for this zone.

Medium

- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

2 Click the **Custom Level...** button.

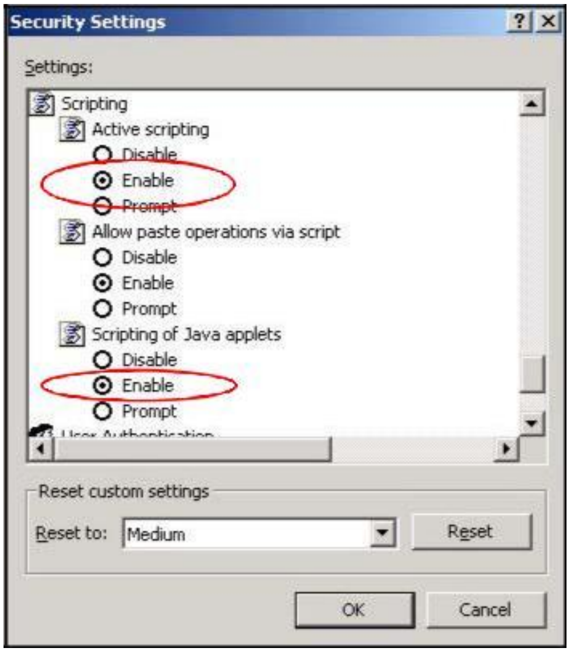
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 122 Security Settings - Java Scripting



Security Settings

Settings:

Scripting

Active scripting
○ Disable
● Enable
○ Prompt

Allow paste operations via script
○ Disable
● Enable
○ Prompt

Scripting of Java applets
○ Disable
● Enable
○ Prompt

User Authentication

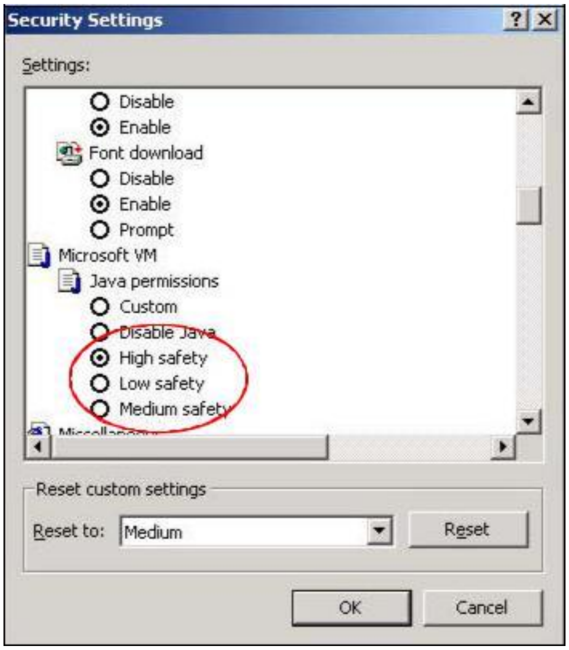
Reset custom settings

Reset to: Medium

Java Permissions

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.
2. Click the **Custom Level...** button.
3. Scroll down to **Microsoft VM**.
4. Under **Java permissions** make sure that a safety level is selected.
5. Click **OK** to close the window.

Figure 123 Security Settings - Java



Security Settings

Settings:

○ Disable
● Enable
Font download
○ Disable
● Enable
○ Prompt
Microsoft VM
Java permissions
○ Custom
○ Disable Java
● High safety
○ Low safety
○ Medium safety

Reset custom settings

Reset to: Medium

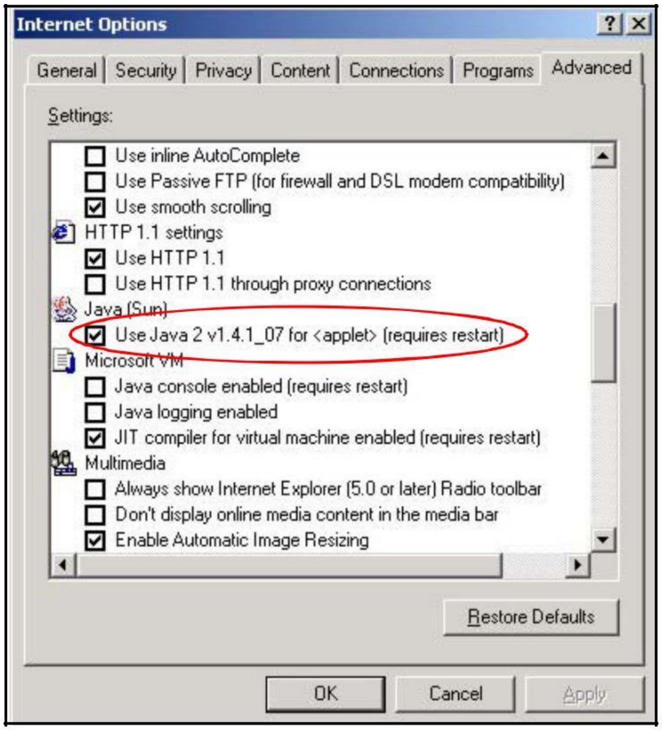
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 124 Java (Sun)



Internet Options

Settings:

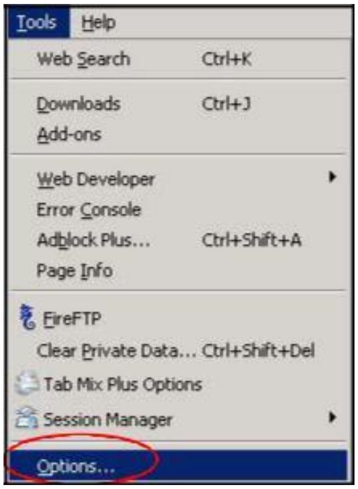
□ Use inline AutoComplete
□ Use Passive FTP (for firewall and DSL modem compatibility)
☑ Use smooth scrolling
HTTP 1.1 settings
☑ Use HTTP 1.1
□ Use HTTP 1.1 through proxy connections
Java (Sun)
☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)
Microsoft VM
□ Java console enabled (requires restart)
□ Java logging enabled
☑ JIT compiler for virtual machine enabled (requires restart)
Multimedia
□ Always show Internet Explorer (5.0 or later) Radio toolbar
□ Don't display online media content in the media bar
☑ Enable Automatic Image Resizing

Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary slightly. The steps below apply to Mozilla Firefox 3.0 as well.

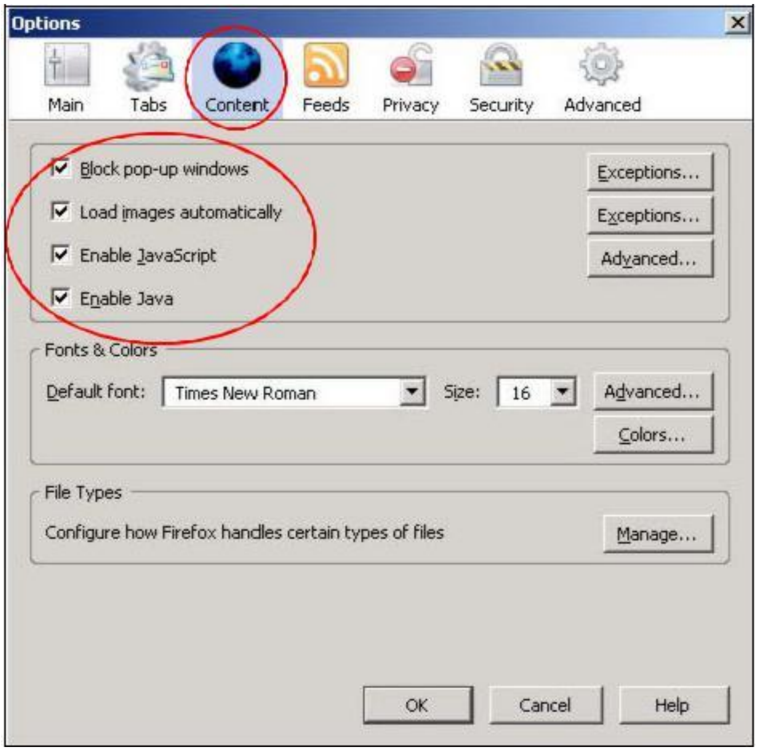
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 125 Mozilla Firefox: TOOLS > Options



Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

Figure 126 Mozilla Firefox Content Security



☑ Block pop-up windows

☑ Load images automatically

☑ Enable JavaScript

☑ Enable Java

Fonts & Colors

Default font: Times New Roman Size: 16

File Types

Configure how Firefox handles certain types of files

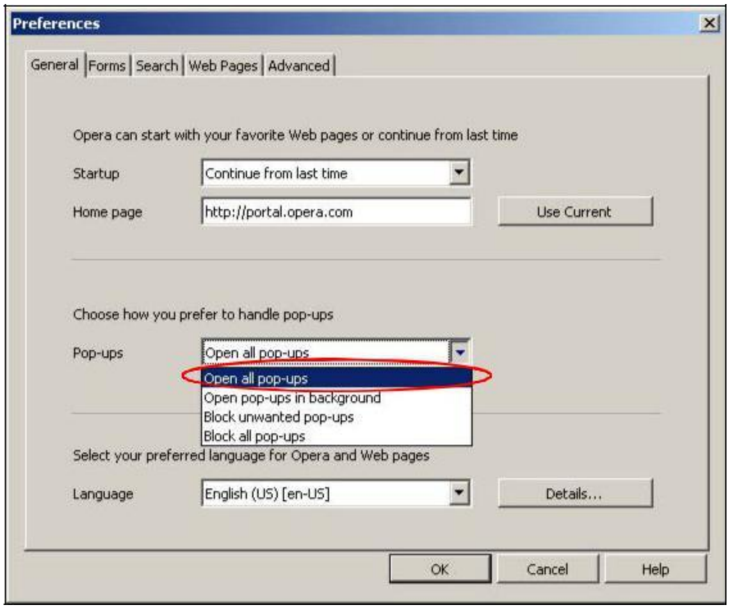
Opera

Opera 10 screens are used here. Screens for other versions may vary slightly.

Allowing Pop-Ups

From Opera, click **Tools**, then **Preferences**. In the **General** tab, go to **Choose how you prefer to handle pop-ups** and select **Open all pop-ups**.

Figure 127 Opera: Allowing Pop-Ups



Opera can start with your favorite Web pages or continue from last time

Startup: Continue from last time

Home page: http://portal.opera.com

Choose how you prefer to handle pop-ups

Pop-ups: Open all pop-ups

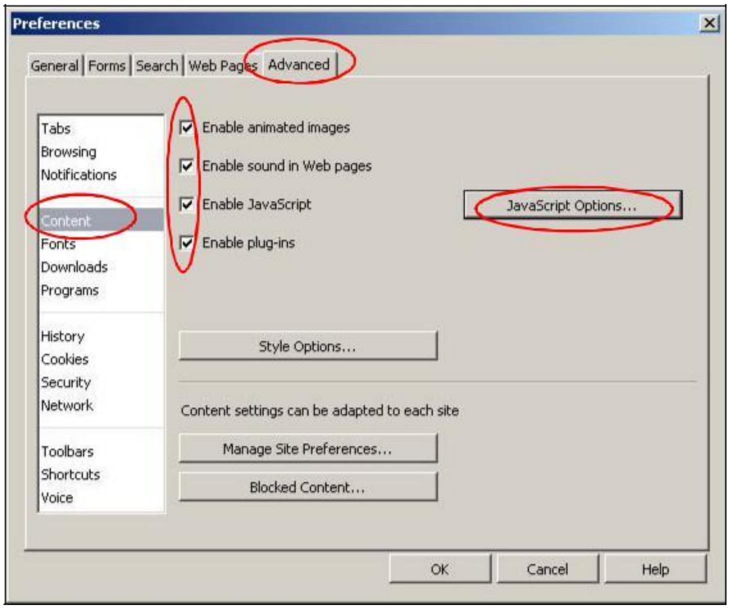
Select your preferred language for Opera and Web pages

Language: English (US) [en-US]

Enabling Java

From Opera, click **Tools**, then **Preferences**. In the **Advanced** tab, select **Content** from the left-side menu. Select the check boxes as shown in the following screen.

Figure 128 Opera: Enabling Java



☑ Enable animated images

☑ Enable sound in Web pages

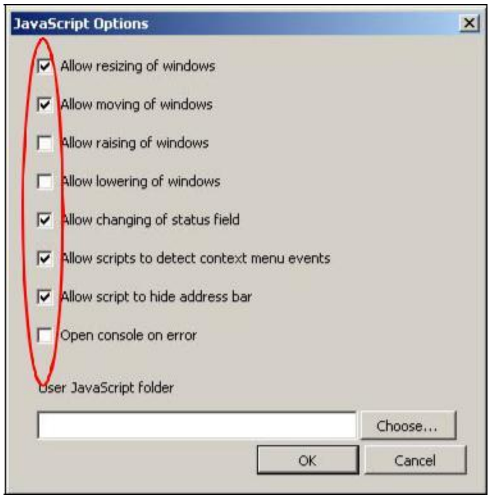
☑ Enable JavaScript

☑ Enable plug-ins

Content settings can be adapted to each site

To customize JavaScript behavior in the Opera browser, click **JavaScript Options**.

Figure 129 Opera: JavaScript Options



☑ Allow resizing of windows

☑ Allow moving of windows

☐ Allow raising of windows

☐ Allow lowering of windows

☑ Allow changing of status field

☑ Allow scripts to detect context menu events

☑ Allow script to hide address bar

☐ Open console on error

User JavaScript folder

Select the items you want Opera’s JavaScript to apply.

Setting Up Your Computer’s IP Address

Note: Your specific WAP3205 v3 may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/ OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network’s computers have IP addresses that place them in the same subnet.

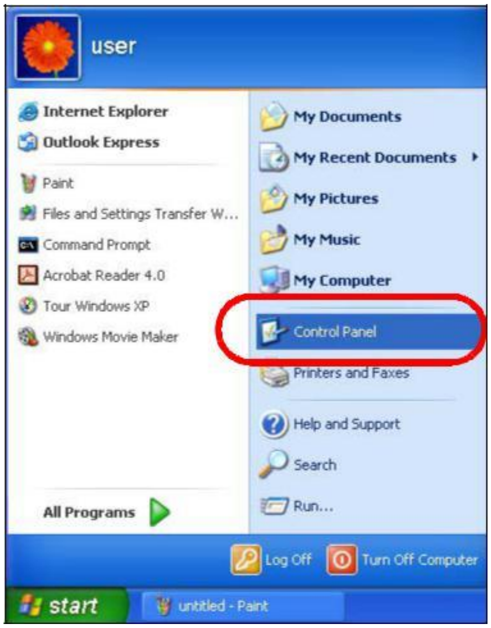
In this appendix, you can set up an IP address for:

- Windows XP/NT/2000 on page 167
- Windows Vista on page 171
- Windows 7 on page 175
- Mac OS X: 10.3 and 10.4 on page 179
- Mac OS X: 10.5 and 10.6 on page 182
- Linux: Ubuntu 8 (GNOME) on page 185
- Linux: openSUSE 10.3 (KDE) on page 189

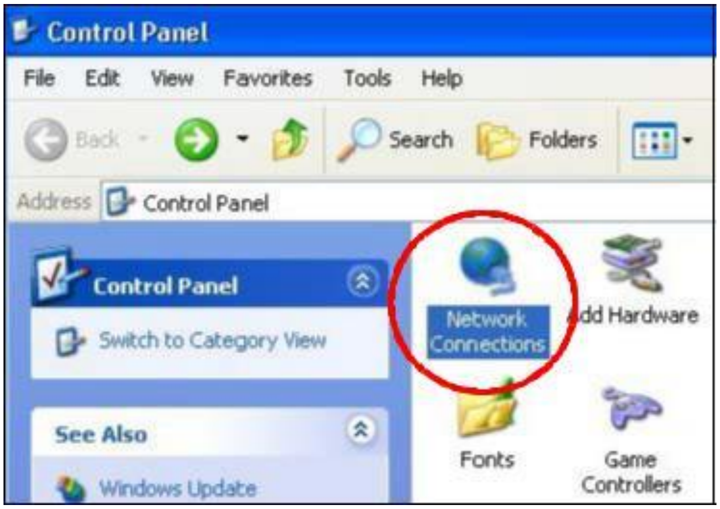
Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

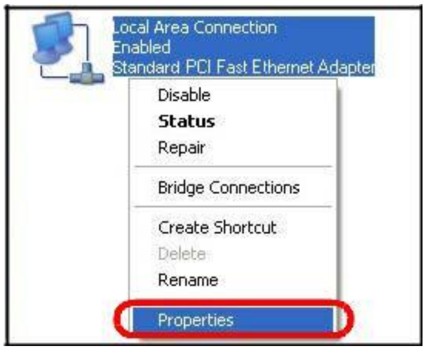
1 Click **Start** > **Control Panel**.



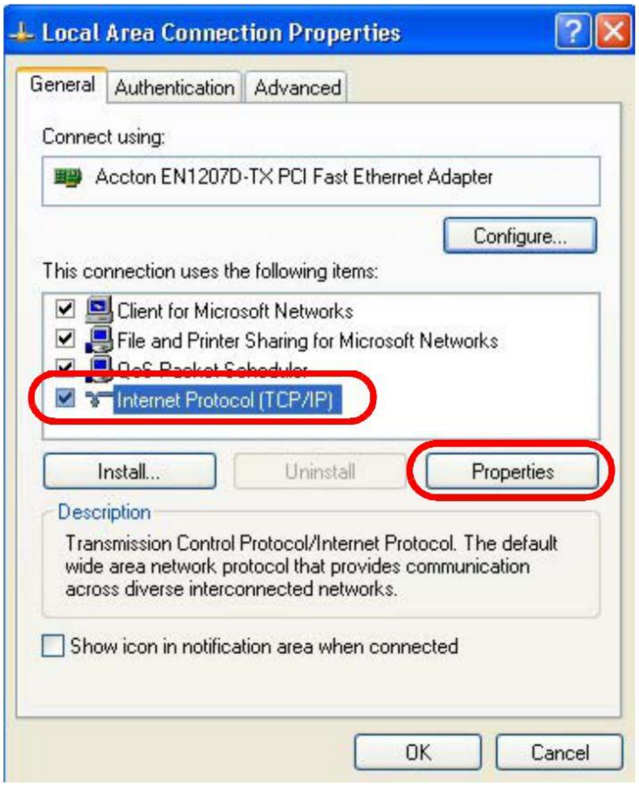
2 In the **Control Panel**, click the **Network Connections** icon.



3 Right-click **Local Area Connection** and then select **Properties**.



4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.



Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

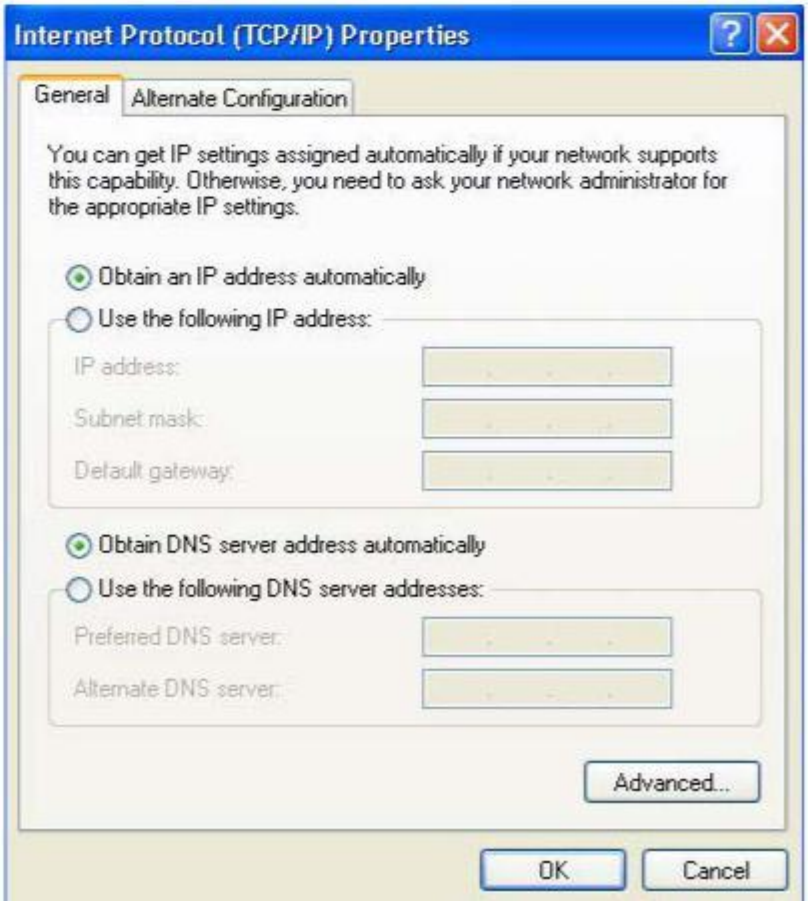
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

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 The **Internet Protocol TCP/IP Properties** window opens.



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:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.

7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

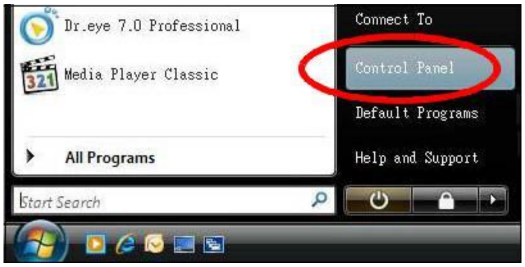
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

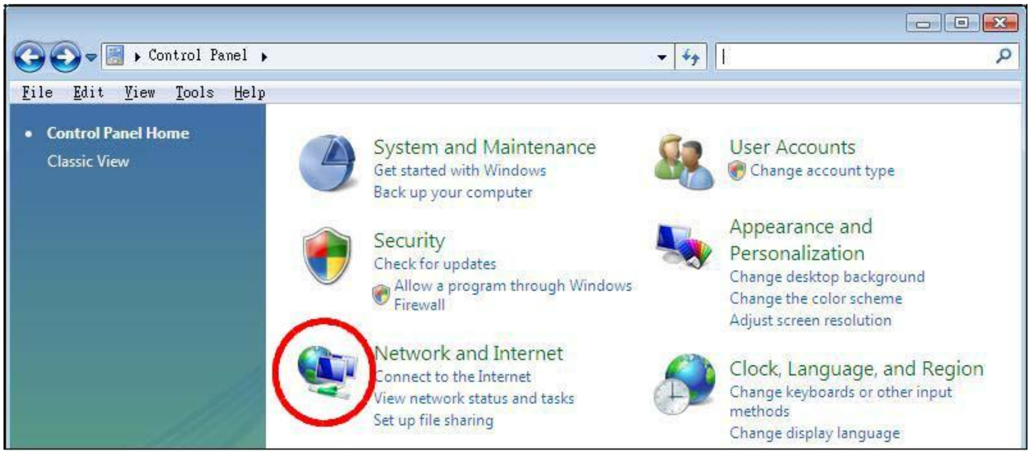
Windows Vista

This section shows screens from Windows Vista Professional.

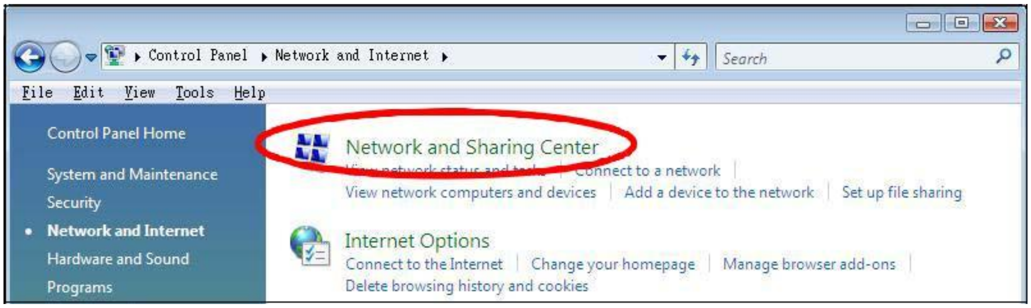
1 Click **Start** > **Control Panel**.



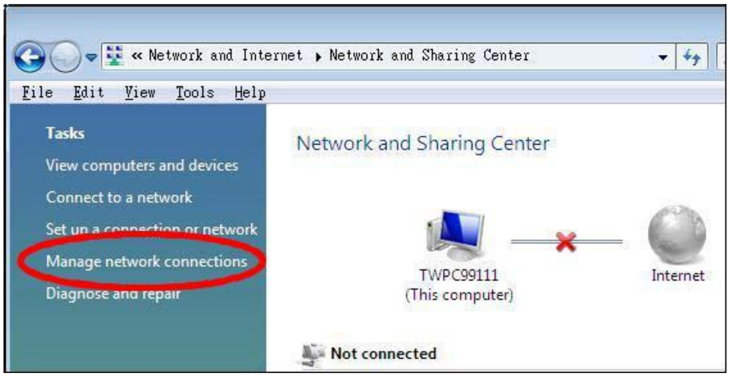
2 In the **Control Panel**, click the **Network and Internet** icon.



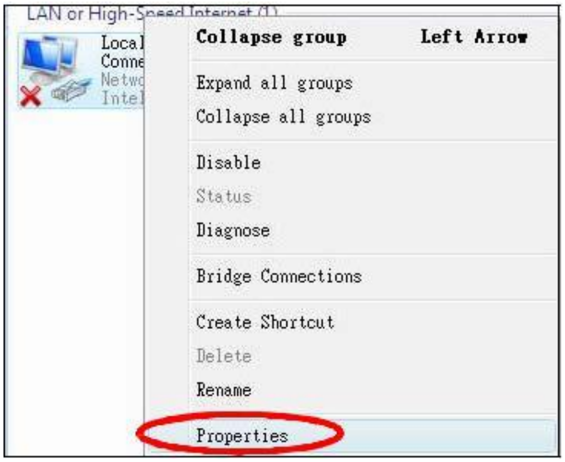
3 Click the **Network and Sharing Center** icon.



4 Click **Manage network connections**.

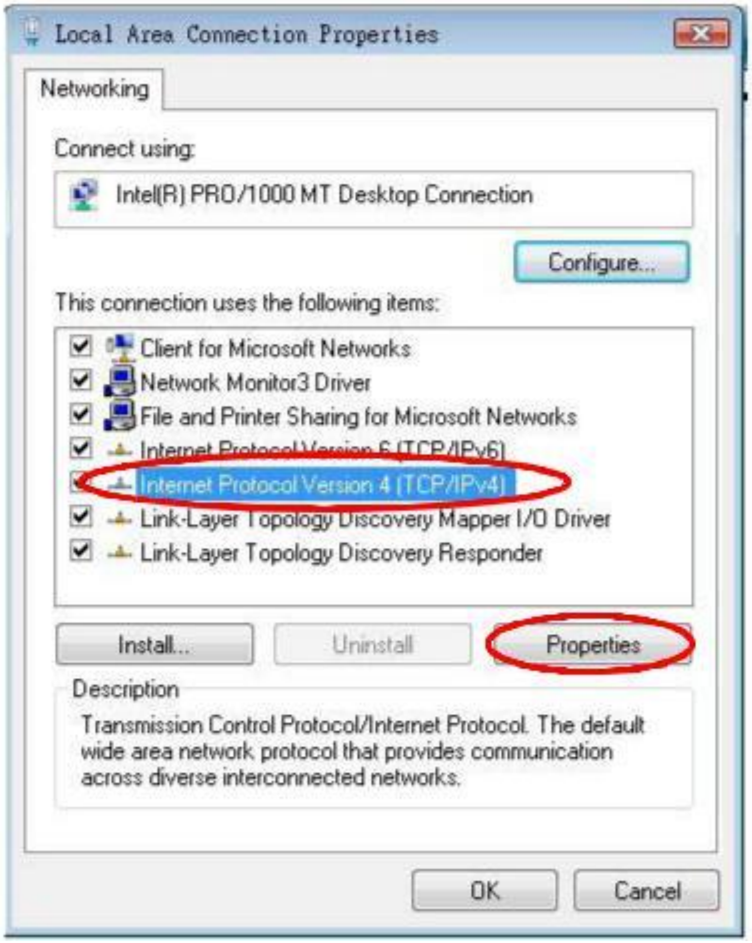

« Network and Internet ▸ Network and Sharing Center
File Edit View Tools Help
Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair
Network and Sharing Center
TWPC99111
(This computer)
Internet
Not connected

5 Right-click **Local Area Connection** and then select **Properties**.



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



Connect using:

Intel(R) PRO/1000 MT Desktop Connection

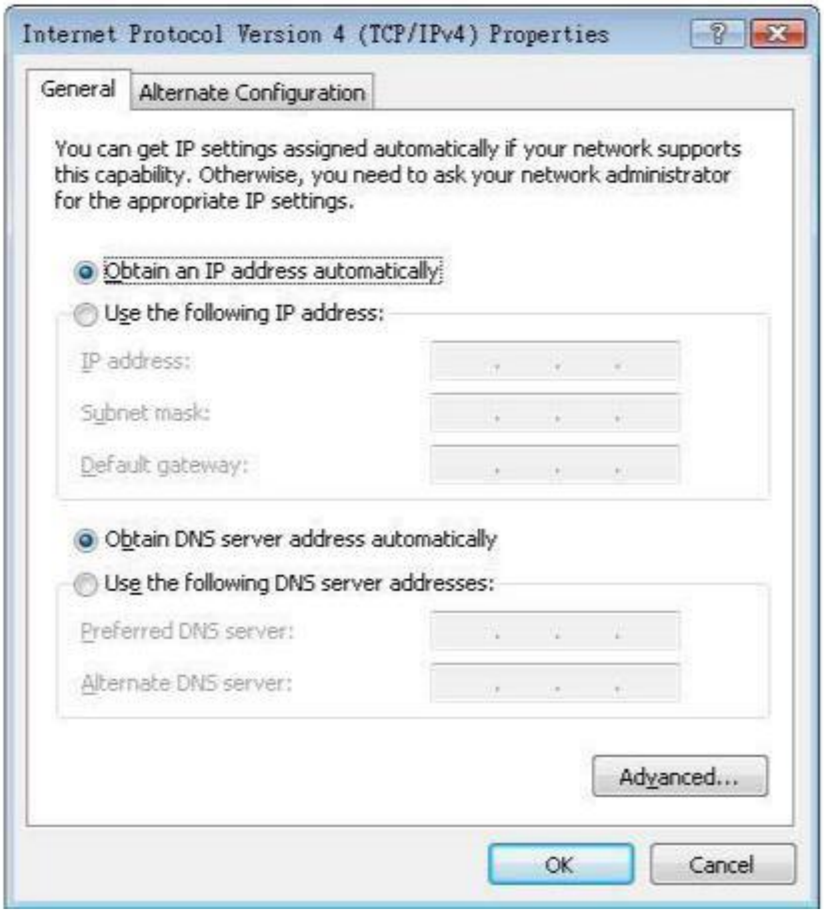
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ Network Monitor3 Driver
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

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

7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.



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: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.Click **Advanced**.

9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

10 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

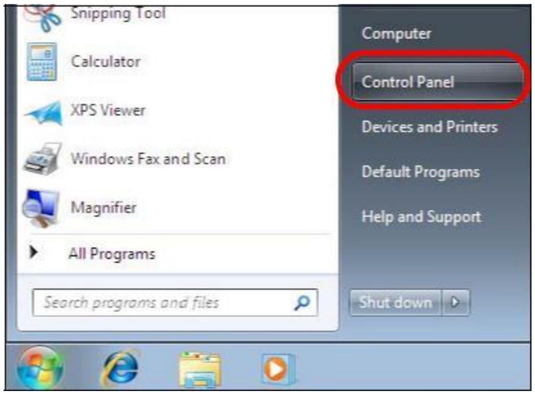
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

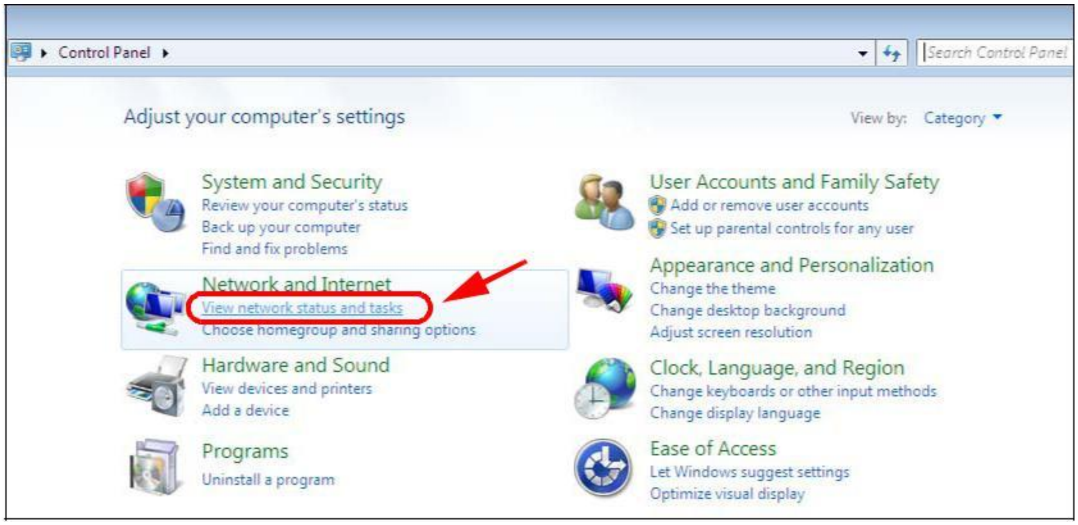
Windows 7

This section shows screens from Windows 7 Enterprise.

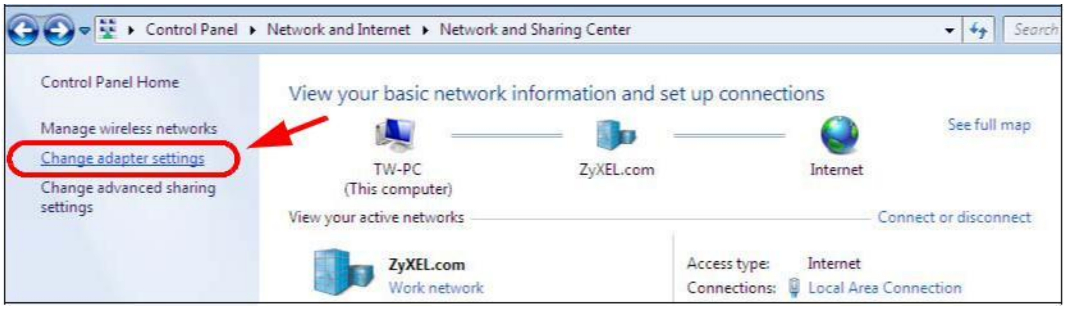
1 Click **Start** > **Control Panel**.



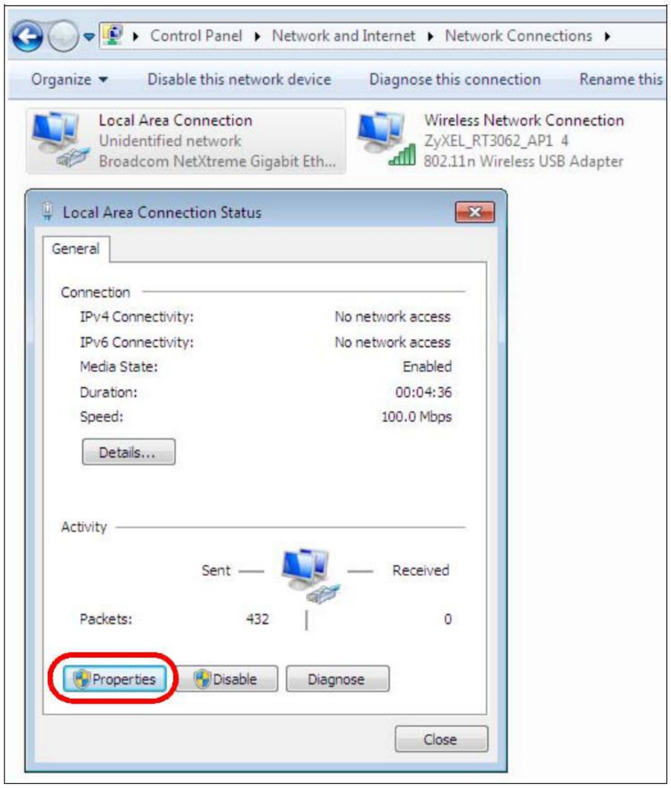
2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.


Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Change display language
Ease of Access
Let Windows suggest settings
Optimize visual display

3 Click **Change adapter settings**.


Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
TW-PC
(This computer)
ZyXEL.com
Internet
View your active networks
Connect or disconnect
ZyXEL.com
Work network
Access type: Internet
Connections: Local Area Connection

4 Double click **Local Area Connection** and then select **Properties**.


Control Panel ▸ Network and Internet ▸ Network Connections ▸
Organize ▾
Disable this network device
Diagnose this connection
Rename this
Local Area Connection
Unidentified network
Broadcom NetXtreme Gigabit Eth...
Wireless Network Connection
ZyXEL_RT3062_AP1 4
802.11n Wireless USB Adapter
Local Area Connection Status
General
Details...
Properties
Disable
Diagnose
Close

Connection

IPv4 Connectivity: No network access

IPv6 Connectivity: No network access

Media State: Enabled

Duration: 00:04:36

Speed: 100.0 Mbps

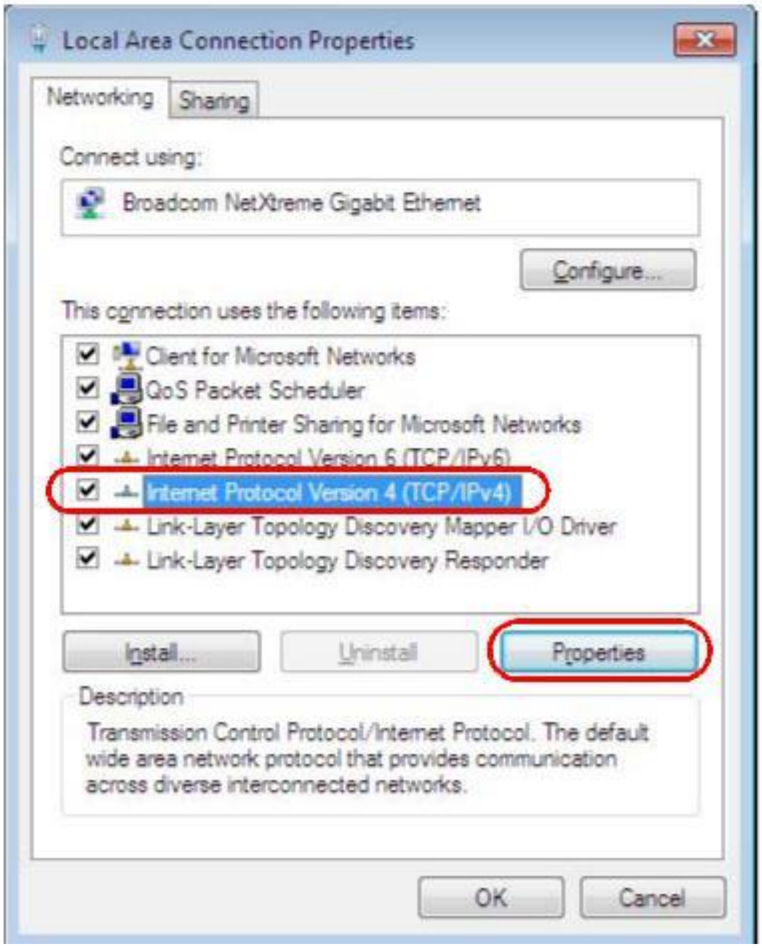
Activity

Sent — — Received

Packets: 432 | 0

Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

5 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



Local Area Connection Properties

Connect using:

Broadcom NetXtreme Gigabit Ethernet

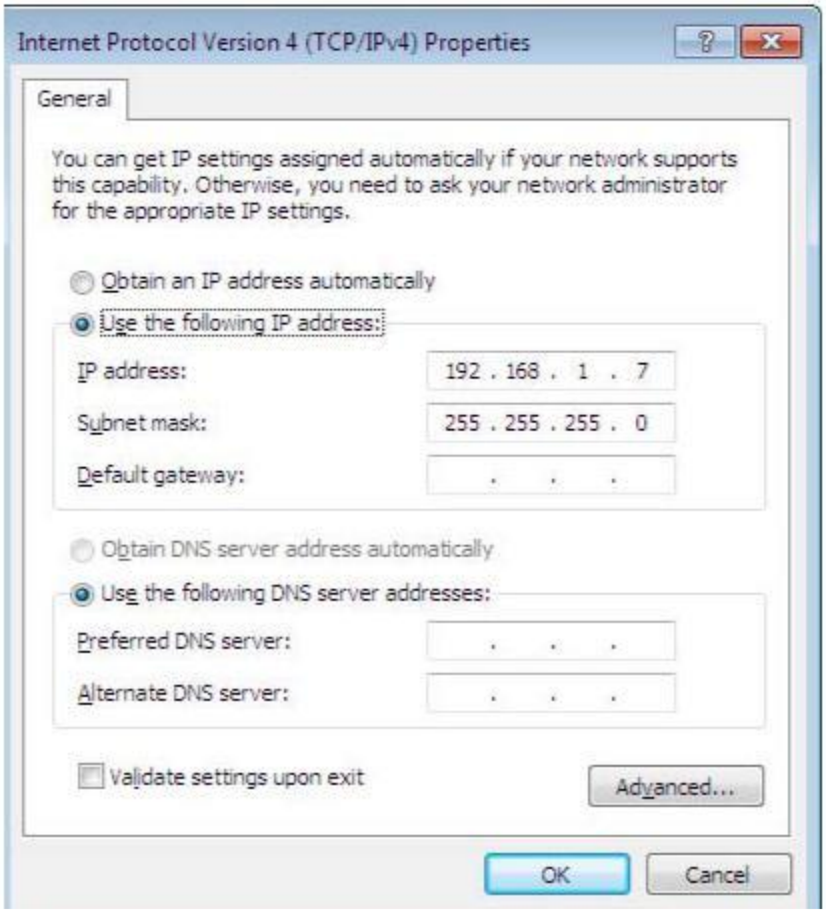
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

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

6 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.



Internet Protocol Version 4 (TCP/IPv4) 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 . 7

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: . . .

□ Validate settings upon exit

7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided. Click **Advanced** if you want to configure advanced settings for IP, DNS and WINS.

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

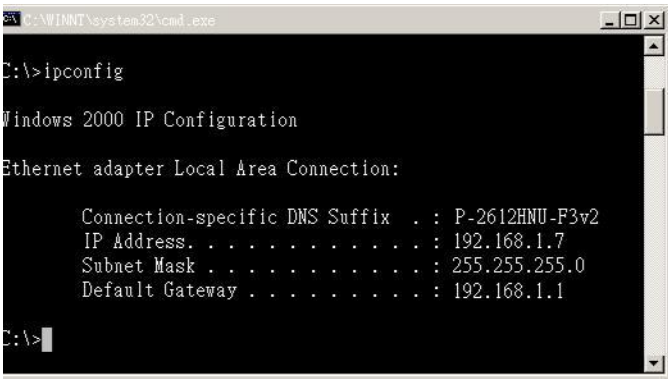
9 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

3 The IP settings are displayed as follows.



```
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : P-2612HNU-F3v2
        IP Address. . . . . . . . . . . . : 192.168.1.7
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\>
```

Wireless LANs

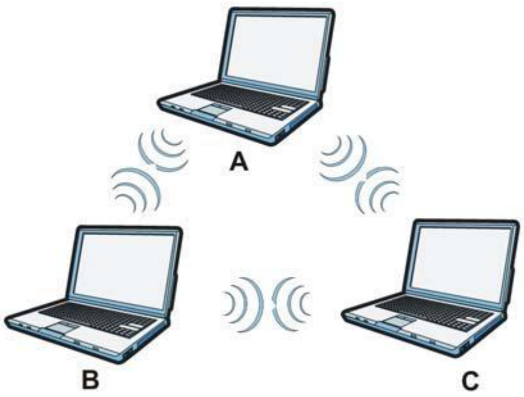
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 136 Peer-to-Peer Communication in an Ad-hoc Network

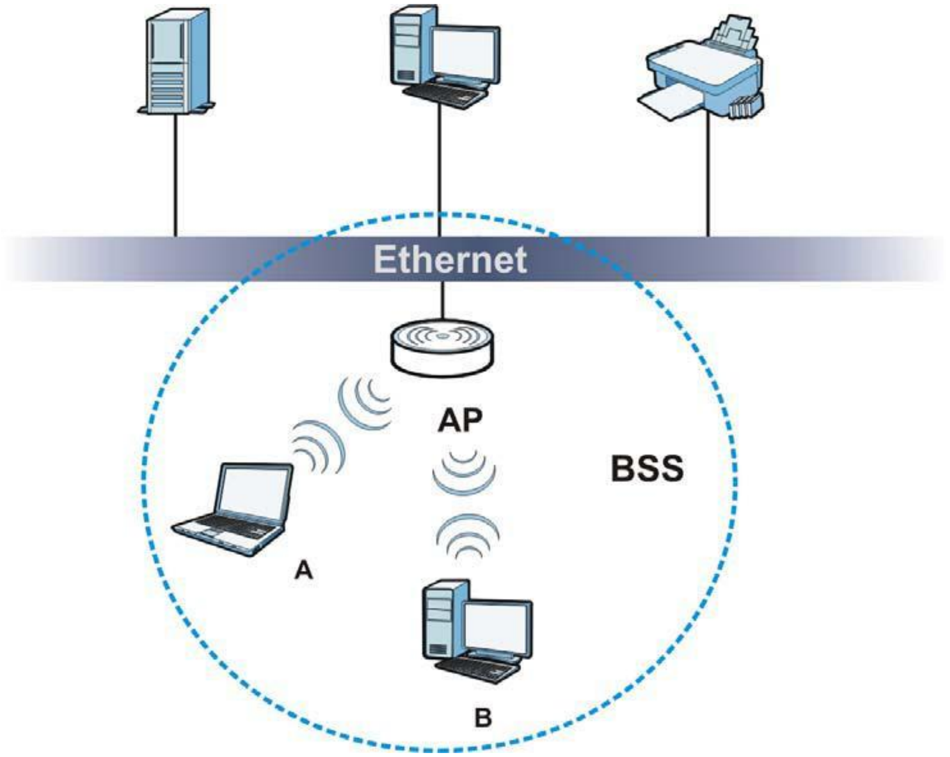


BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 137 Basic Service Set



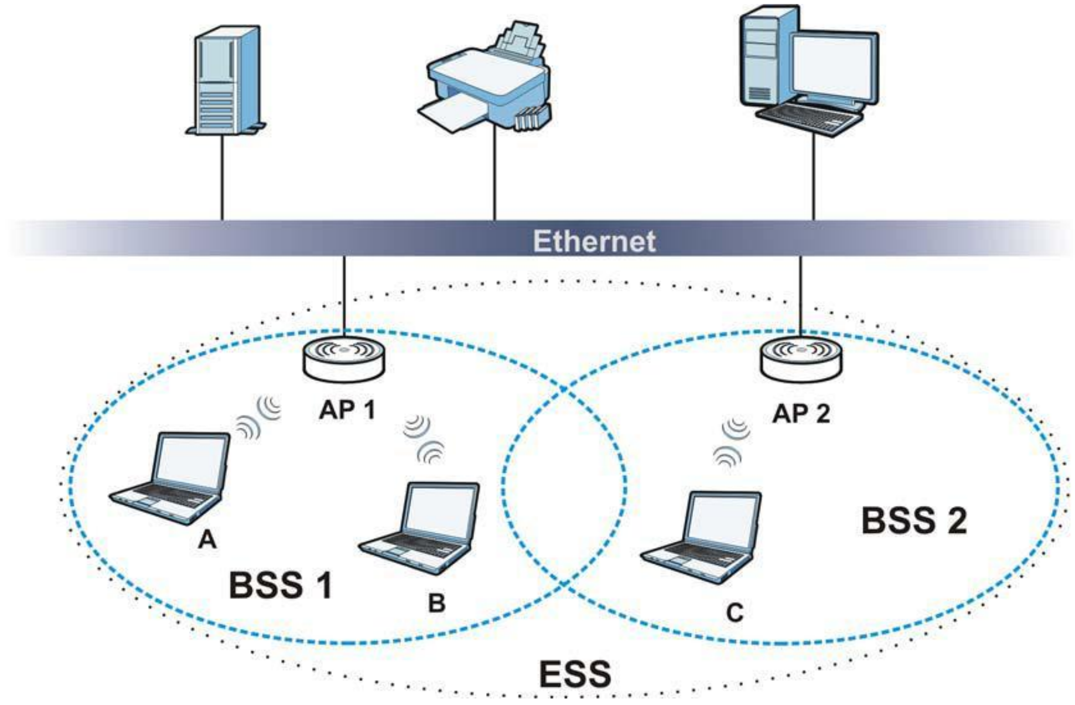
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 138 Infrastructure WLAN



Channel

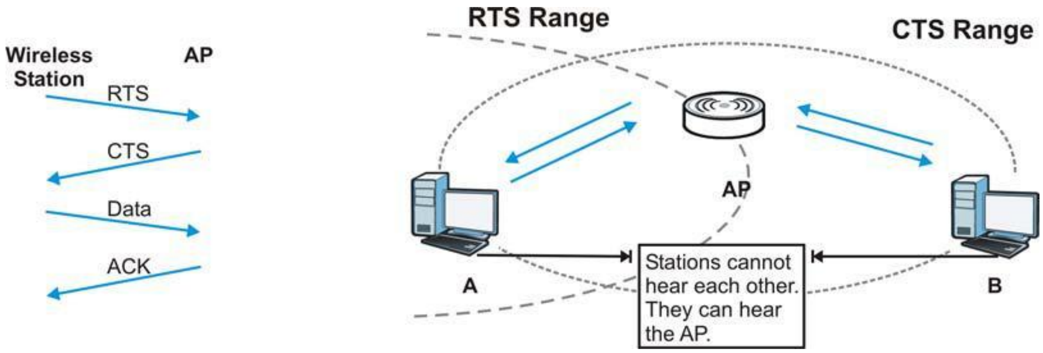
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 139 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the WAP3205 v3 uses long preamble.

Note: The wireless devices MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 70 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/ 54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the WAP3205 v3 are data encryption, wireless client authentication, restricting access by device MAC address and hiding the WAP3205 v3 identity.

The following figure shows the relative effectiveness of these wireless security methods available on your WAP3205 v3.

Table 71 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

Note: You must enable the same wireless security settings on the WAP3205 v3 and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client’s network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.
- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client ‘proves’ that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender’s identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or re-authentication times out. A new WEP key is generated each time re-authentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 72 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it’s still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

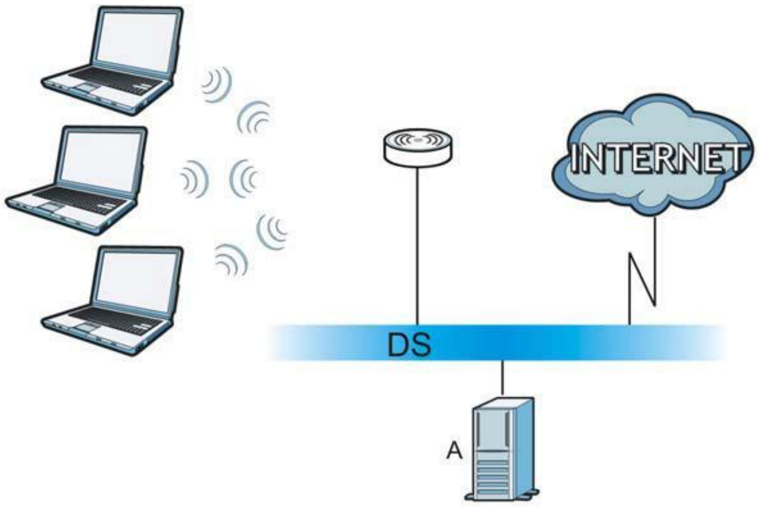
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
4. The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 140 WPA(2) with RADIUS Application Example



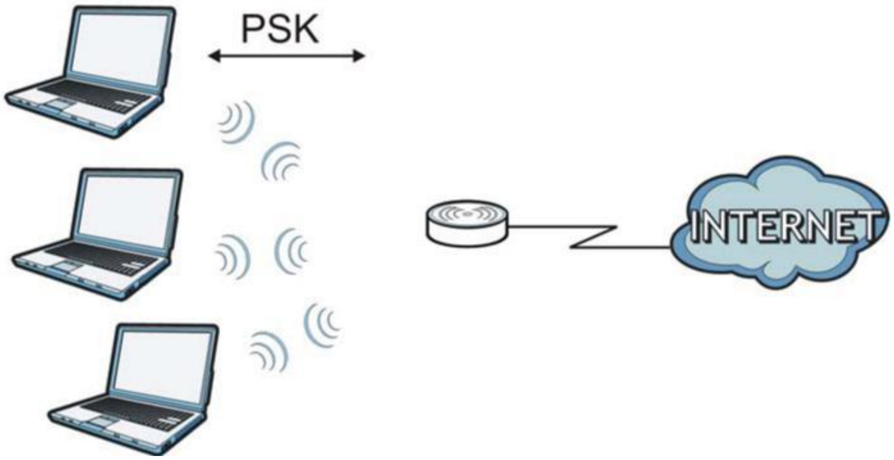
WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
2. The AP checks each wireless client's password and allows it to join the network only if the password matches.
3. The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 141 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 73 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTIO N METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz or 5GHz is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

A

Legal Information

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

UNITED STATES of AMERICA

The following information applies if you use the product within USA area.

FCC EMC Statement

- The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this device does cause harmful interference to radio or television reception, which is found by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna
  - Increase the separation between the devices
  - Connect the equipment to an outlet other than the receiver's
  - Consult a dealer or an experienced radio/TV technician for assistance

FCC Radiation Exposure Statement

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.

EUROPEAN UNION

The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive)

Compliance information for 2.4GHz and/or 5GHz wireless products relevant to the EU and other Countries following the EU Directive 1999/5/EC (R&TTE)

Български (Bulgarian)	С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/ЕС.
Español (Spanish)	Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Čeština (Czech)	ZyXEL tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
Dansk (Danish)	Undertegnede ZyXEL erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch (German)	Hiermit erklärt ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ZyXEL ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EC.
English	Hereby, ZyXEL declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Français (French)	Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.
Hrvatski (Croatian)	ZyXEL ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 1999/5/EC.
Íslenska (Icelandic)	Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.
Italiano (Italian)	Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviešu valoda (Latvian)	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių kalba (Lithuanian)	Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EK irányelv egyéb elõírásainak.
Malti (Maltese)	Hawnhekk, ZyXEL, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Nederlands (Dutch)	Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
Polski (Polish)	Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português (Portuguese)	ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.
Română (Romanian)	Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 1999/5/EC.
Slovenčina (Slovak)	ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.
Slovenščina (Slovene)	ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
Suomi (Finnish)	ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

Svenska (Swedish)	Härmed intygar ZyXEL att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
Norsk (Norwegian)	Erklærer herved ZyXEL at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 1999/5/EF.

This device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

National Restrictions

This product may be used in all EU countries (and other countries following the EU Directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttiva 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der Richtlinie 1999/5/CE folgen) mit Außnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2.4GHz and 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable.

The requirements for any country may evolve. ZyXEL recommends that you check with the local authorities for the latest status of their national regulations for both the 2.4GHz and 5GHz wireless LANs.

The following countries have restrictions and/or requirements in addition to those given in the table labeled "*Overview of Regulatory Requirements for Wireless LANs*":.

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.

Denmark

In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.

Latvia

The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.

2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.

2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used(specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do not obstruct the device ventilation slots, as insufficient airflow may harm your device.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,
  - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;
  - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

Environment Statement

ErP (Energy-related Products)

ZyXEL products put on the EU market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

Network standby power consumption < 12W, and/or

Off mode power consumption < 0.5W, and/or

Standby mode power consumption < 0.5W.

Wireless setting, please refer to "Wireless" chapter for more detail.

European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

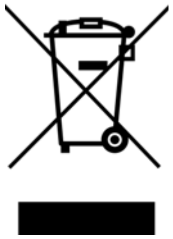
Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

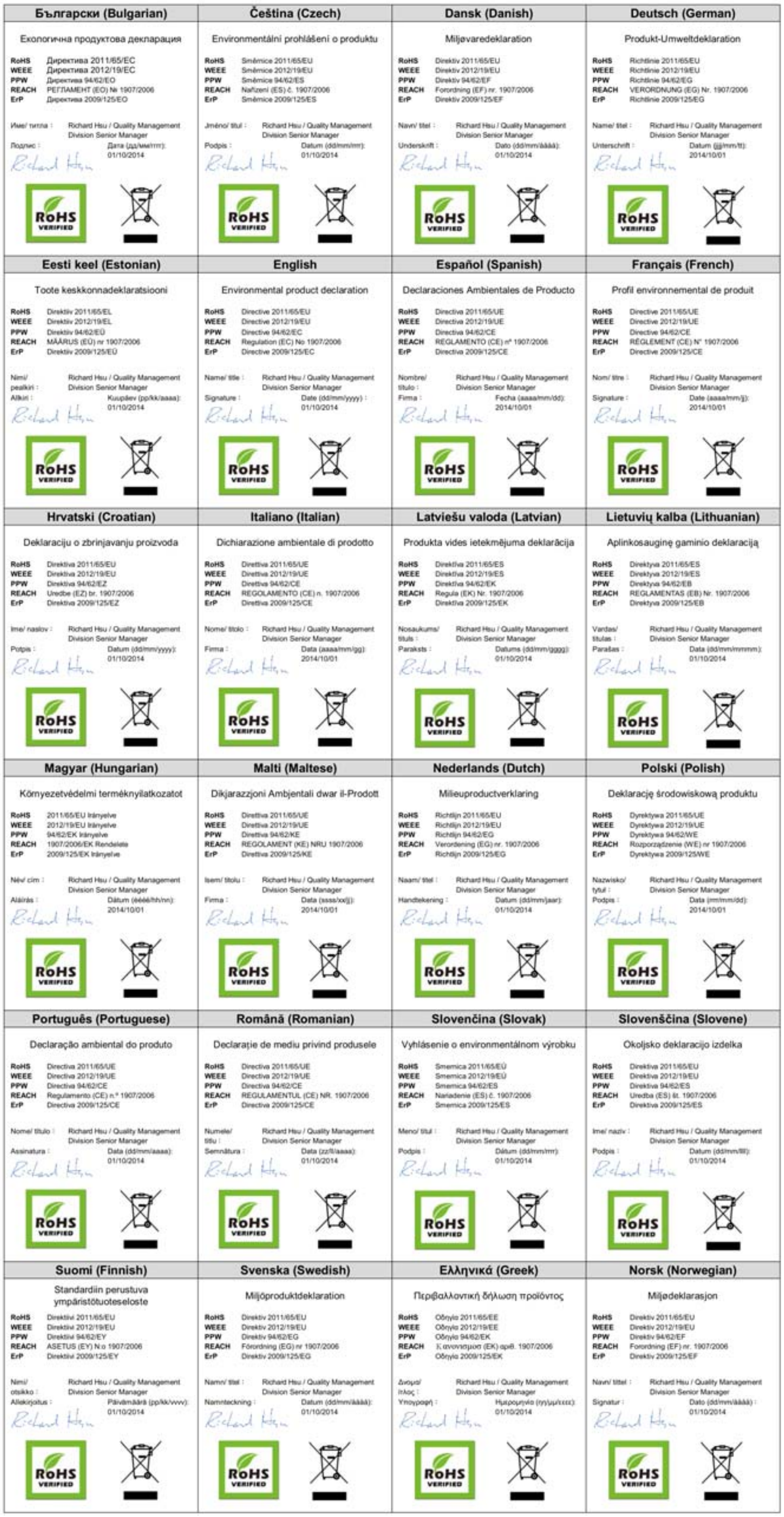
Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



Environmental Product Declaration



Български (Bulgarian)

Екологична продуктова декларация

RoHS	Директива 2011/65/EC
WEEE	Директива 2012/19/EC
PPW	Директива 94/62/EO
REACH	РЕГЛАМЕНТ (EO) № 1907/2006
ErP	Директива 2009/125/EO

Име/ титла : Richard Hsu / Quality Management Division Senior Manager

Подпис : Дата (дд/мм/гггг): 01/10/2014

Richard Hsu

RoHS VERIFIED

Čeština (Czech)

Environmentální prohlášení o produktu

RoHS	Směrnice 2011/65/EU
WEEE	Směrnice 2012/19/EU
PPW	Směrnice 94/62/ES
REACH	Nařízení (ES) č. 1907/2006
ErP	Směrnice 2009/125/ES

Jméno/ titul : Richard Hsu / Quality Management Division Senior Manager

Podpis : Datum (dd/mm/rrrr): 01/10/2014

Richard Hsu

RoHS VERIFIED

Dansk (Danish)

Miljøvaredeklaration

RoHS	Direktiv 2011/65/EU
WEEE	Direktiv 2012/19/EU
PPW	Direktiv 94/62/EF
REACH	Forordning (EF) nr. 1907/2006
ErP	Direktiv 2009/125/EF

Navn/ titel : Richard Hsu / Quality Management Division Senior Manager

Underskrift : Dato (dd/mm/åååå): 01/10/2014

Richard Hsu

RoHS VERIFIED

Deutsch (German)

Produkt-Umweltdeklaration

RoHS	Richtlinie 2011/65/EU
WEEE	Richtlinie 2012/19/EU
PPW	Richtlinie 94/62/EG
REACH	VERORDNUNG (EG) Nr. 1907/2006
ErP	Richtlinie 2009/125/EG

Name/ titel : Richard Hsu / Quality Management Division Senior Manager

Unterschrift : Datum (jj/mm/tt): 2014/10/01

Richard Hsu

RoHS VERIFIED

Eesti keel (Estonian)

Toote keskkonnadeklaratsiooni

RoHS	Direktiiv 2011/65/EL
WEEE	Direktiiv 2012/19/EL
PPW	Direktiiv 94/62/EÜ
REACH	MÄÄRUS (EÜ) nr 1907/2006
ErP	Direktiiv 2009/125/EÜ

Nimi/ pealkiri : Richard Hsu / Quality Management Division Senior Manager

Allkiri : Kuupäev (pp/kk/aaaa): 01/10/2014

Richard Hsu

RoHS VERIFIED

English

Environmental product declaration

RoHS	Directive 2011/65/EU
WEEE	Directive 2012/19/EU
PPW	Directive 94/62/EC
REACH	Regulation (EC) No 1907/2006
ErP	Directive 2009/125/EC

Name/ title : Richard Hsu / Quality Management Division Senior Manager

Signature : Date (dd/mm/yyyy) : 01/10/2014

Richard Hsu

RoHS VERIFIED

Español (Spanish)

Declaraciones Ambientales de Producto

RoHS	Directiva 2011/65/UE
WEEE	Directiva 2012/19/UE
PPW	Directiva 94/62/CE
REACH	REGLAMENTO (CE) nº 1907/2006
ErP	Directiva 2009/125/CE

Nombre/ título : Richard Hsu / Quality Management Division Senior Manager

Firma : Fecha (aaaa/mm/dd): 2014/10/01

Richard Hsu

RoHS VERIFIED

Français (French)

Profil environnemental de produit

RoHS	Directive 2011/65/UE
WEEE	Directive 2012/19/UE
PPW	Directive 94/62/CE
REACH	RÉGLEMENT (CE) N° 1907/2006
ErP	Directive 2009/125/CE

Nom/ titre : Richard Hsu / Quality Management Division Senior Manager

Signature : Date (aaaa/mm/jj): 2014/10/01

Richard Hsu

RoHS VERIFIED

Hrvatski (Croatian)

Deklaraciju o zbrinjavanju proizvoda

RoHS	Direktiva 2011/65/EU
WEEE	Direktiva 2012/19/EU
PPW	Direktiva 94/62/EZ
REACH	Uredbe (EZ) br. 1907/2006
ErP	Direktiva 2009/125/EZ

Ime/ naslov : Richard Hsu / Quality Management Division Senior Manager

Potpis : Datum (dd/mm/yyyy): 01/10/2014

Richard Hsu

RoHS VERIFIED

Italiano (Italian)

Dichiarazione ambientale di prodotto

RoHS	Direttiva 2011/65/UE
WEEE	Direttiva 2012/19/UE
PPW	Direttiva 94/62/CE
REACH	REGOLAMENTO (CE) n. 1907/2006
ErP	Direttiva 2009/125/CE

Nome/ titolo : Richard Hsu / Quality Management Division Senior Manager

Firma : Data (aaaa/mm/gg): 2014/10/01

Richard Hsu

RoHS VERIFIED

Latviešu valoda (Latvian)

Produkta vides ietekmējuma deklarācija

RoHS	Direktīva 2011/65/ES
WEEE	Direktīva 2012/19/ES
PPW	Direktīva 94/62/EK
REACH	Regula (EK) Nr. 1907/2006
ErP	Direktīva 2009/125/EK

Nosaukums/ tituls : Richard Hsu / Quality Management Division Senior Manager

Paraksts : Datums (dd/mm/gggg): 01/10/2014

Richard Hsu

RoHS VERIFIED

Lietuvių kalba (Lithuanian)

Aplinkosauginę gaminio deklaraciją

RoHS	Direktyva 2011/65/ES
WEEE	Direktyva 2012/19/ES
PPW	Direktyva 94/62/EB
REACH	REGLAMENTAS (EB) Nr. 1907/2006
ErP	Direktyva 2009/125/EB

Vardas/ titulas : Richard Hsu / Quality Management Division Senior Manager

Parašas : Data (dd/mm/mmmm): 01/10/2014

Richard Hsu

RoHS VERIFIED

Magyar (Hungarian)

Környezetvédelmi terméknyilatkozatot

RoHS	2011/65/EU Irányelve
WEEE	2012/19/EU Irányelve
PPW	94/62/EK Irányelve
REACH	1907/2006/EK Rendelete
ErP	2009/125/EK Irányelve

Név/ cím : Richard Hsu / Quality Management Division Senior Manager

Aláírás : Dátum (éééé/hh/nn): 2014/10/01

Richard Hsu

RoHS VERIFIED

Malti (Maltese)

Dikjarazzjoni Ambjentali dwar il-Prodott

RoHS	Direttiva 2011/65/UE
WEEE	Direttiva 2012/19/UE
PPW	Direttiva 94/62/KE
REACH	REGOLAMENT (KE) NRU 1907/2006
ErP	Direttiva 2009/125/KE

Isem/ titolu : Richard Hsu / Quality Management Division Senior Manager

Firma : Data (ssss/xx/jj): 2014/10/01

Richard Hsu

RoHS VERIFIED

Nederlands (Dutch)

Milieuproductverklaring

RoHS	Richtlijn 2011/65/EU
WEEE	Richtlijn 2012/19/EU
PPW	Richtlijn 94/62/EG
REACH	Verordening (EG) nr. 1907/2006
ErP	Richtlijn 2009/125/EG

Naam/ titel : Richard Hsu / Quality Management Division Senior Manager

Handtekening : Datum (dd/mm/jaar): 01/10/2014

Richard Hsu

RoHS VERIFIED

Polski (Polish)

Deklarację środowiskową produktu

RoHS	Dyrektywa 2011/65/UE
WEEE	Dyrektywa 2012/19/UE
PPW	Dyrektywa 94/62/WE
REACH	Rozporządzenie (WE) nr 1907/2006
ErP	Dyrektywa 2009/125/WE

Nazwisko/ tytuł : Richard Hsu / Quality Management Division Senior Manager

Podpis : Data (rrrr/mm/dd): 2014/10/01

Richard Hsu

RoHS VERIFIED

Português (Portuguese)

Declaração ambiental do produto

RoHS	Directiva 2011/65/UE
WEEE	Directiva 2012/19/UE
PPW	Directiva 94/62/CE
REACH	Regulamento (CE) n.º 1907/2006
ErP	Directiva 2009/125/CE

Nome/ título : Richard Hsu / Quality Management Division Senior Manager

Assinatura : Data (dd/mm/aaaa): 01/10/2014

Richard Hsu

RoHS VERIFIED

Română (Romanian)

Declarație de mediu privind produsele

RoHS	Directiva 2011/65/UE
WEEE	Directiva 2012/19/UE
PPW	Directiva 94/62/CE
REACH	REGULAMENTUL (CE) NR. 1907/2006
ErP	Directiva 2009/125/CE

Numele/ titlu : Richard Hsu / Quality Management Division Senior Manager

Semnătura : Data (zz/ll/aaaa): 01/10/2014

Richard Hsu

RoHS VERIFIED

Slovenčina (Slovak)

Vyhlásenie o environmentálnom výrobku

RoHS	Smernica 2011/65/EÚ
WEEE	Smernica 2012/19/EÚ
PPW	Smernica 94/62/ES
REACH	Nariadenie (ES) č. 1907/2006
ErP	Smernica 2009/125/ES

Meno/ titul : Richard Hsu / Quality Management Division Senior Manager

Podpis : Dátum (dd/mm/rrrr): 01/10/2014

Richard Hsu

RoHS VERIFIED

Slovenščina (Slovene)

Okoljsko deklaracijo izdelka

RoHS	Direktiva 2011/65/EU
WEEE	Direktiva 2012/19/EU
PPW	Direktiva 94/62/ES
REACH	Uredba (ES) št. 1907/2006
ErP	Direktiva 2009/125/ES

Ime/ naziv : Richard Hsu / Quality Management Division Senior Manager

Podpis : Datum (dd/mm/llll): 01/10/2014

Richard Hsu

RoHS VERIFIED

Suomi (Finnish)

Standardiin perustuva ympäristötuoteseloste

RoHS	Direktiivi 2011/65/EU
WEEE	Direktiivi 2012/19/EU
PPW	Direktiivi 94/62/EY
REACH	ASETUS (EY) N:o 1907/2006
ErP	Direktiivi 2009/125/EY

Nimi/ otsikko : Richard Hsu / Quality Management Division Senior Manager

Allekirjoitus : Päivämäärä (pp/kk/vvvv): 01/10/2014

Richard Hsu

RoHS VERIFIED

Svenska (Swedish)

Miljöproduktdeklaration

RoHS	Direktiv 2011/65/EU
WEEE	Direktiv 2012/19/EU
PPW	Direktiv 94/62/EG
REACH	Förordning (EG) nr 1907/2006
ErP	Direktiv 2009/125/EG

Namn/ titel : Richard Hsu / Quality Management Division Senior Manager

Namnteckning : Datum (dd/mm/åååå): 01/10/2014

Richard Hsu

RoHS VERIFIED

Ελληνικά (Greek)

Περιβαλλοντική δήλωση προϊόντος

RoHS	Οδηγία 2011/65/ΕΕ
WEEE	Οδηγία 2012/19/ΕΕ
PPW	Οδηγία 94/62/ΕΚ
REACH	Κανονισμού (ΕΚ) αριθ. 1907/2006
ErP	Οδηγία 2009/125/ΕΚ

Όνομα/ τίτλος : Richard Hsu / Quality Management Division Senior Manager

Υπογραφή : Ημερομηνία (ηη/μμ/εεεε): 01/10/2014

Richard Hsu

RoHS VERIFIED

Norsk (Norwegian)

Miljødeklarasjon

RoHS	Direktiv 2011/65/EU
WEEE	Direktiv 2012/19/EU
PPW	Direktiv 94/62/EF
REACH	Forordning (EF) nr. 1907/2006
ErP	Direktiv 2009/125/EF

Navn/ tittel : Richard Hsu / Quality Management Division Senior Manager

Signatur : Dato (dd/mm/åååå) : 01/10/2014

Richard Hsu

RoHS VERIFIED

台灣

以下訊息僅適用於產品具有無線功能且銷售至台灣地區
第十二條 經型式認證合格之低功率射頻電機，非經許可，公司，商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。 低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

用 20cm 計算 MPE 能符合 1 mW/cm2
電磁波曝露量 MPE 標準值 1mW/cm2，送測產品實測值為： 0.10 mW/cm2

無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用， 俟無干擾之虞，始得繼續使用。

無線資訊傳設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作， 發射的信號應維持於操作頻帶中

以下訊息僅適用於產品操作於 5.25-5.35 秭赫頻帶內並銷售至台灣地區

- 在 5.25-5.35 秭赫頻帶內操作之無線資訊傳輸設備，限於室內使用。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得 設置使用，且不得直接販售給一般消費者

安全警告
為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
- 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座 (如：北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  - 對永久連接之設備， 在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備， 插座必須接近安裝之地點而且是易於觸及的。

Viewing Certifications

Go to http://www.zyxel.com to view this product’s documentation and certifications.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.