ZYXEL
Your Networking Ally

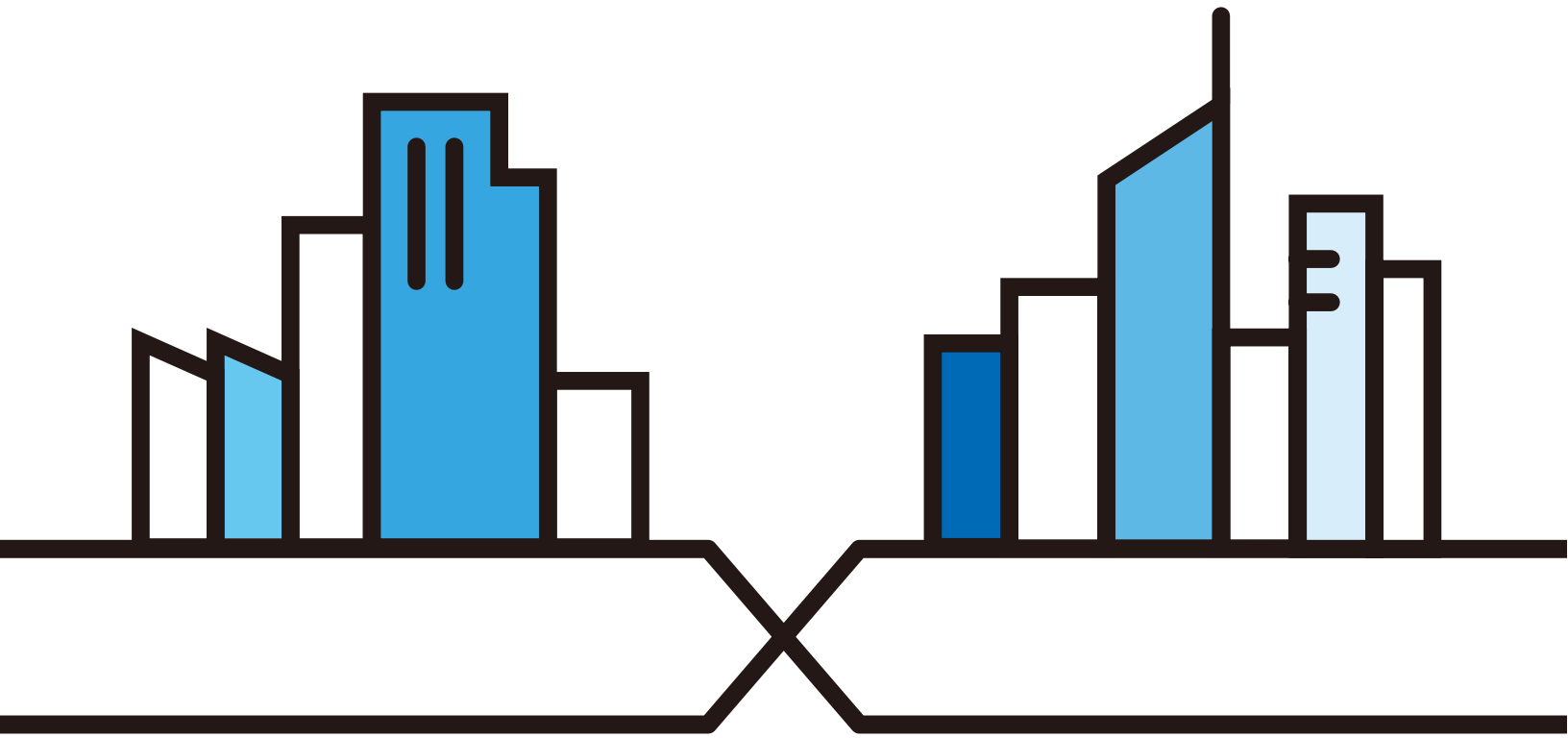
User's Guide

WAP3205 v3

Wireless N300 Access Point

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

Version 1.00 Edition 3, 07/2018



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from what you see due to differences in release versions 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 managed device.

- More Information

  Go to **support.zyxel.com** to find other information on the WAP3205 v3.

Contents Overview

Table of Contents

PART I
User's Guide

CHAPTER 1
Introduction

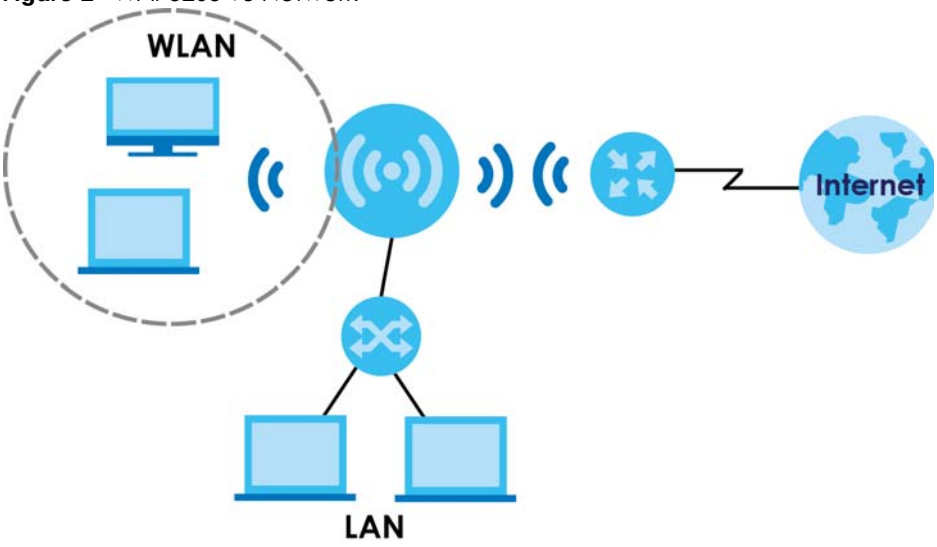
1.1 Overview

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

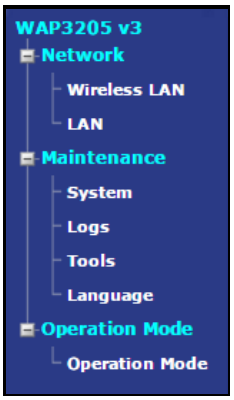


You can set up the WAP3205 v3 with other IEEE 802.11b/g/n compatible devices in one of the following device modes:

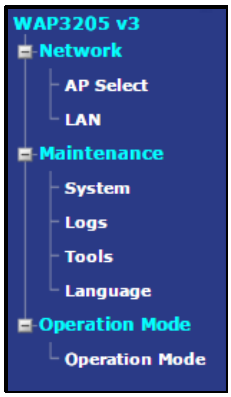
- Access Point
- Universal Repeater
- Client Bridge

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

AP or Universal Repeater Mode



Client Bridge Mode



See Chapter 4 on page 33 for more information on these modes.

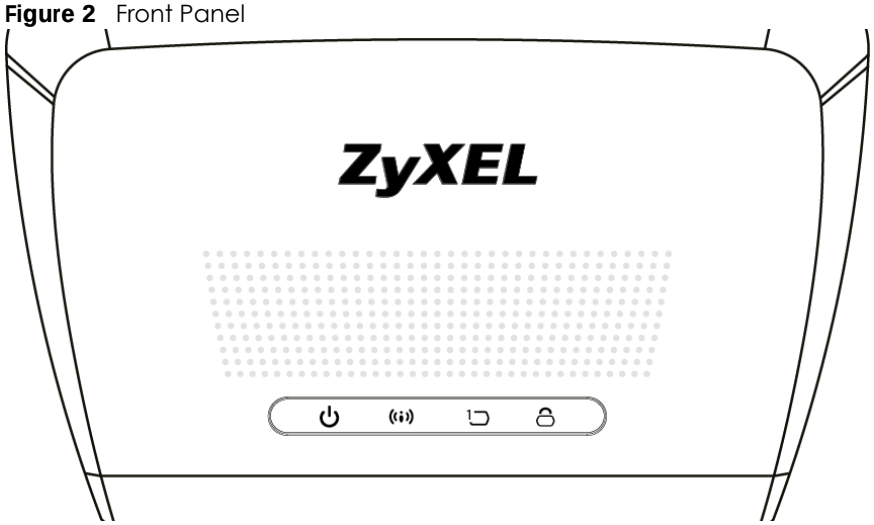
1.2 Securing the WAP3205 v3

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.

Table 1 Front Panel LEDs and WPS Button

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The WAP3205 v3 is receiving power and functioning properly.
		Off	The WAP3205 v3 is not receiving power.
WLAN 2.4G	Green	On	The WAP3205 v3 is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The WAP3205 v3 is sending/receiving data through the wireless LAN. The WAP3205 v3 is negotiating a WPS connection with a wireless client.
		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 a router or client device.
		Off	The WAP3205 v3 LAN port (any of 5 ports) is not connected with a router or client device.
WPS	Green	On	WPS status is configured.
		Blinking	The WAP3205 v3 is negotiating a WPS connection with a wireless client.
		Off	The WPS status is not configured or disabled.

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 Wi-Fi 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 reset the WAP3205 v3 back to its factory-default configurations.

   For more information on using **WPS/RESET**, see Section 5.3 on page 45.

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

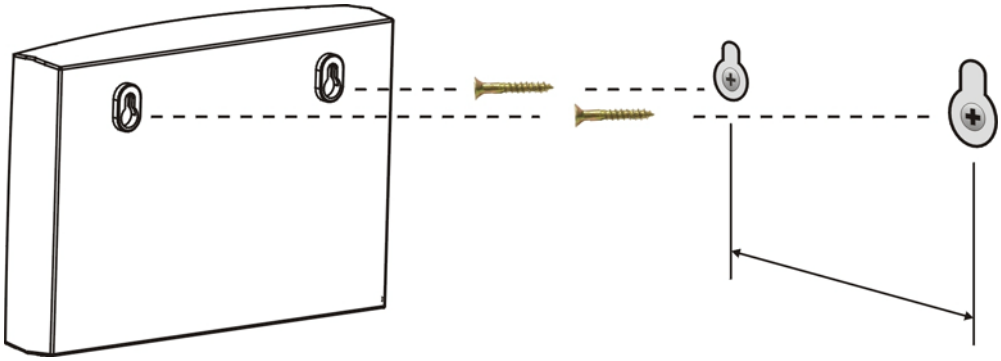
1. Select a position free of obstructions on a wall strong enough to hold the weight of the device.
2. Mark two holes on the wall at the appropriate distance apart for the screws.

   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



CHAPTER 2
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.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Refer to Chapter 13 Troubleshooting to see how to make sure these functions are allowed in Internet Explorer.

2.2 Preparing your Computer to Access the Web Configurator

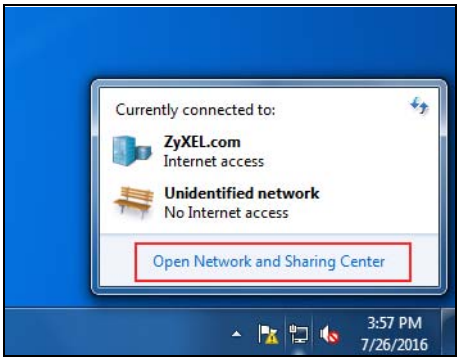
This section shows you how to assign a static IP address to your computer.

In order to access the web configurator your computer needs to be in the same subnet as the WAP3205 v3. Below you will find the steps to set a static IP on both Windows 7 (Section 2.2.1 on page 14) and MAC OS X 10.11(Section 2.2.2 on page 17) operating systems. For other operating systems go to Appendix C on page 108.

2.2.1 Static IP Configuration in Microsoft Windows

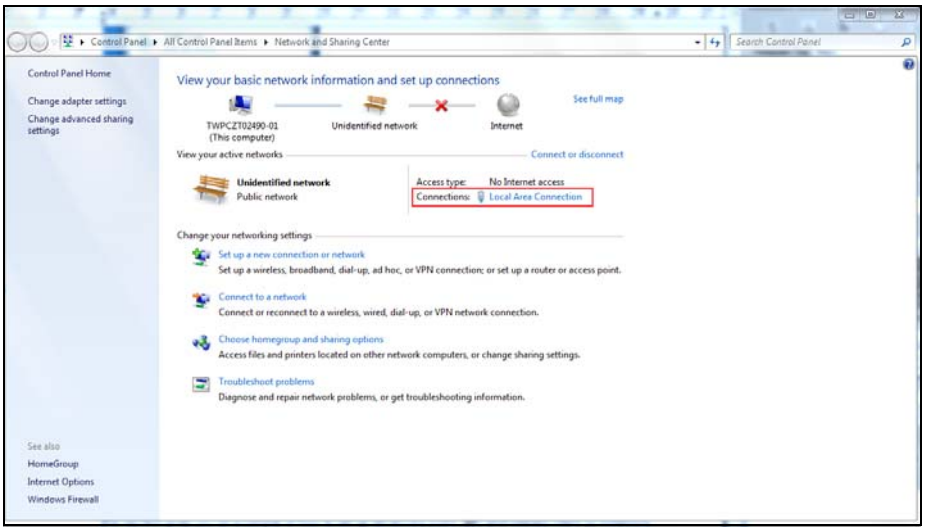
Follow these steps to change your computer's IP address in Windows 7 operating system.

1 Click on the **Network** Icon  located in the System Tray of your Task Bar. After you have clicked the icon a small message window will appear, select **Open Network and Sharing Center.**

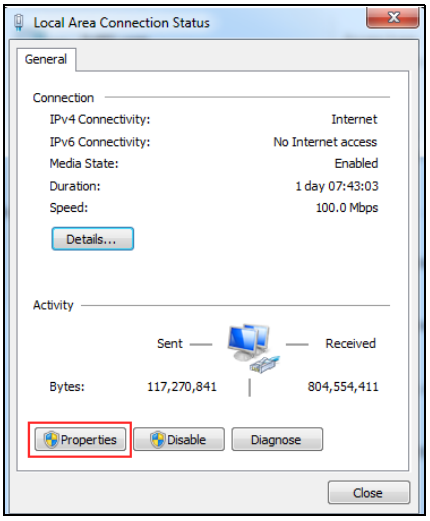


Note: You can also access the **Network and Sharing Center** by going to the **Control Panel** in the **Start Menu** and clicking on **Network and Sharing Center**.

2 Once you have accessed the **Network and Sharing Center**, click on **Local Area Connection** to access the adapter's settings.

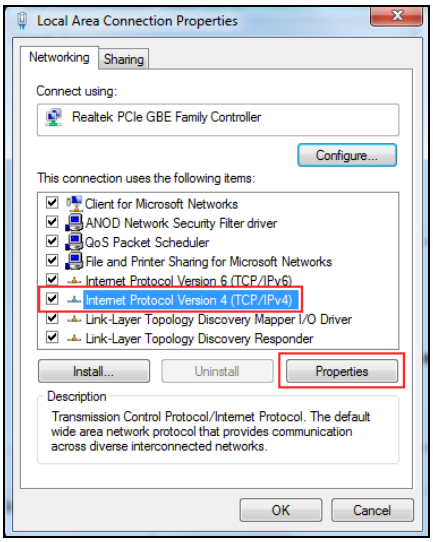


3 After accesing the connection's general settings, click on the **Properties** button.

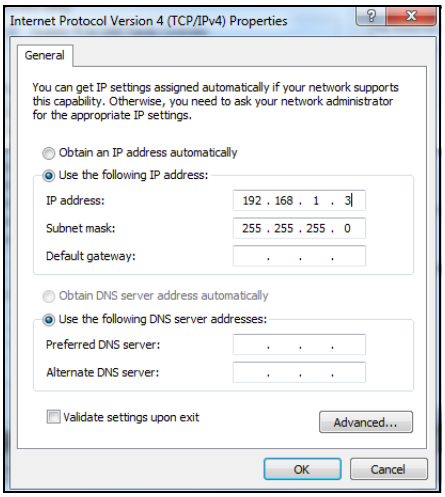


Note: You can also access the adapter's settings by clicking on **Change adapter settings** located on the left side bar. Then right-clicking on the **Local Area Connection** icon and selecting **Properties**.

4 In the connection's properties select the **Internet Protocol Version 4 (TCP/IPv4)** item, then click on the **Properties** button.



5 Once you have accessed the **Internet Protocol Version 4 (TCP/IPv4)** properties, click on the **Use the following IP address** radio button and type your new IP address. Your computer must be in the same subnet in order to access this website address.You must give it a fixed IP address in the range between 192.168.1.3 and 192.168.1.254. Then type 255.255.255.0 as your subnet mask, click **OK** to close the **Internet Protocol Version 4 (TCP/IPv4) Properties** window. Then click **OK** to close the **Local Area Connection**

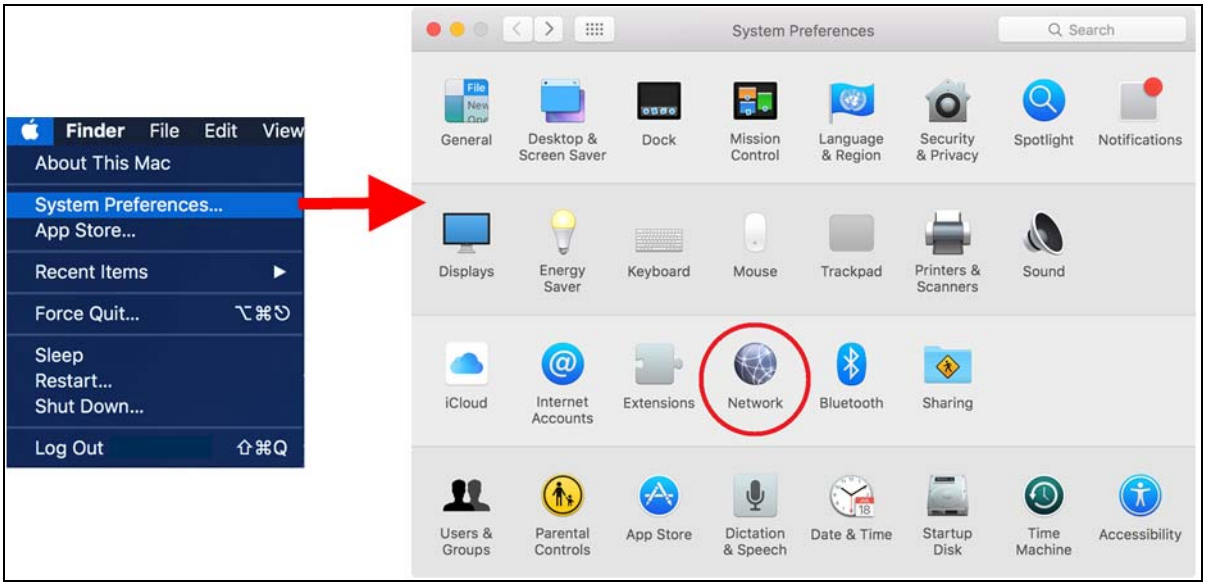


Note: After you have configured your WAP3205 v3, you must remember to change your static IP back to automatic to be able to access the Internet. If you want to change the IP address to automatic (default) then repeat steps 1 to 4, for step 5 select the **Obtain an IP address automatically** radio button, and click **OK**.

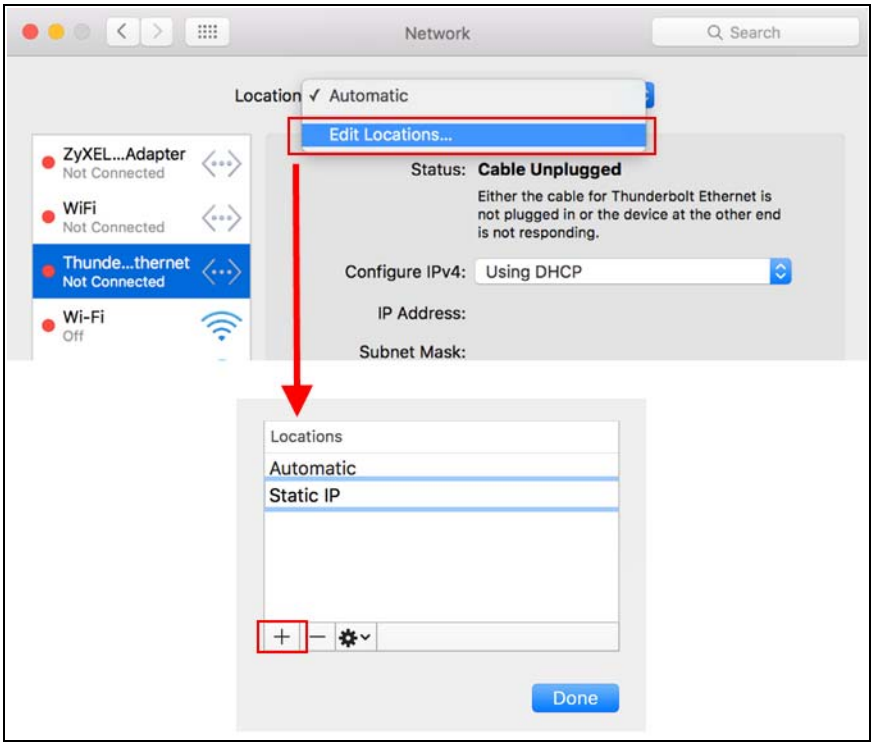
2.2.2 Static IP Configuration in MAC OS X

Follow these steps to change your computer's IP address in MAC OS X 10.11 operating system.

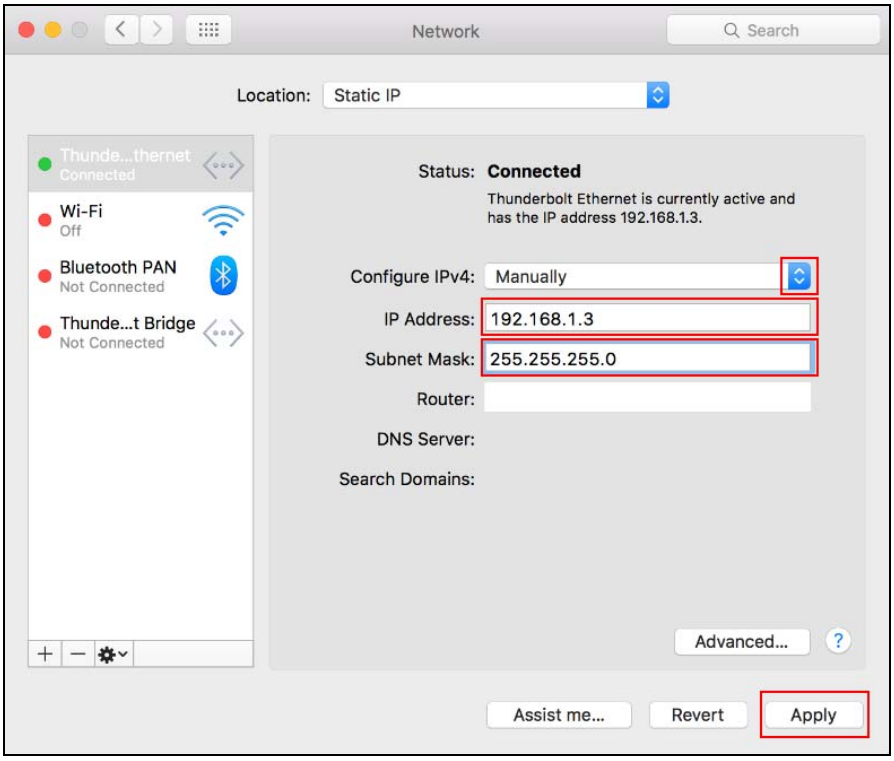
1 Open your **System Preferences**, then click on **Network**.



2 Once the **Network** screen is open, it is recommended you click on **Location** > **Edit Locations** to create a new profile. Use the **+** button to add a new profile, in this case it is called **Static IP**. This will easily help you change from static IP address to automatic.



3 After creating your **Static IP** profile, make sure it is selected, then click on the **Configure IPv4** scroll button and select **Manually**. Then modify your IP Address, your computer must be in the same subnet in order to access this website address.You must give it a fixed IP address in the range between 192.168.1.3 and 192.168.1.254. Then type 255.255.255.0 as your subnet mask, and click **Apply** to save your changes.



Note: After you have configured your WAP3205 v3, you must remember to change your static IP back to obtaining it automatically to be able to access the Internet. If you want to change the IP address to automatic (default) repeat step 1, then on **Location** select **Automatic** or a different profile you have configured.

2.3 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).

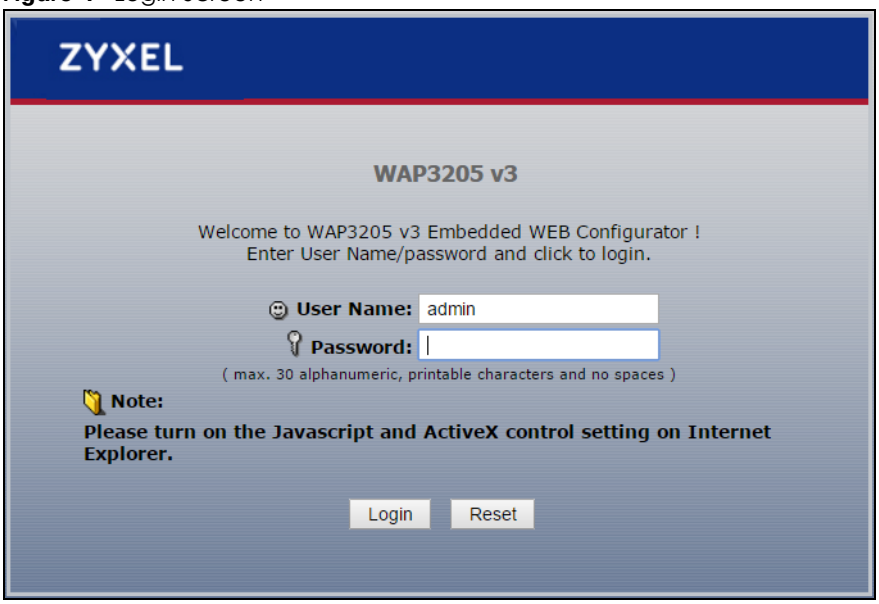
2 Launch your web browser.

3 Type the WAP3205 v3's default address "http://192.168.1.2 to access any of the modes.

Your computer must be in the same subnet in order to access this website address.You must give it a fixed IP address in the range between 192.168.1.3 and 192.168.1.254 (see Section 2.2 on page 14).

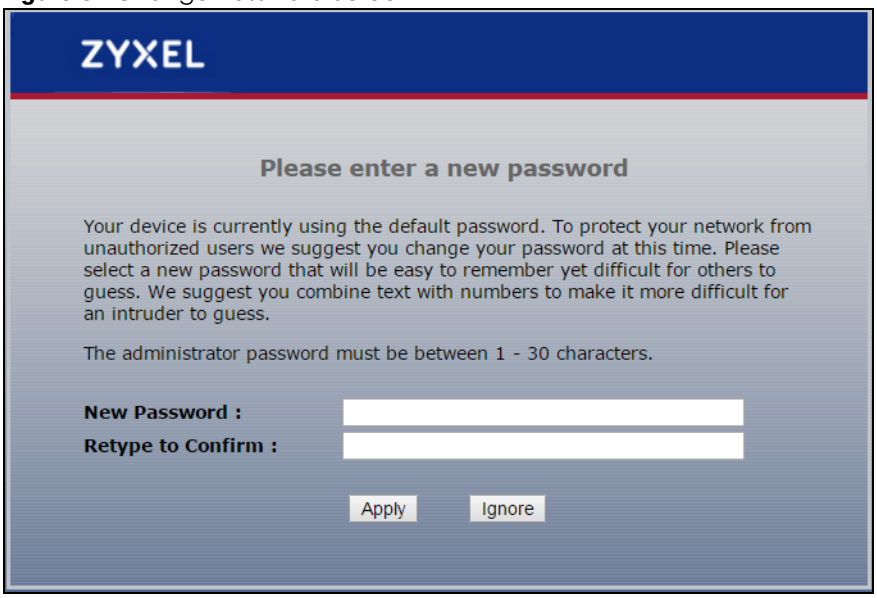
4 Type **admin** (default) as the user name and **1234** (default) as the password and click **Login**.

Figure 4 Login Screen



5 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password. Click **Apply** to save your changes. Click **Ignore** if you do not want to change the password this time.

Figure 5 Change Password Screen

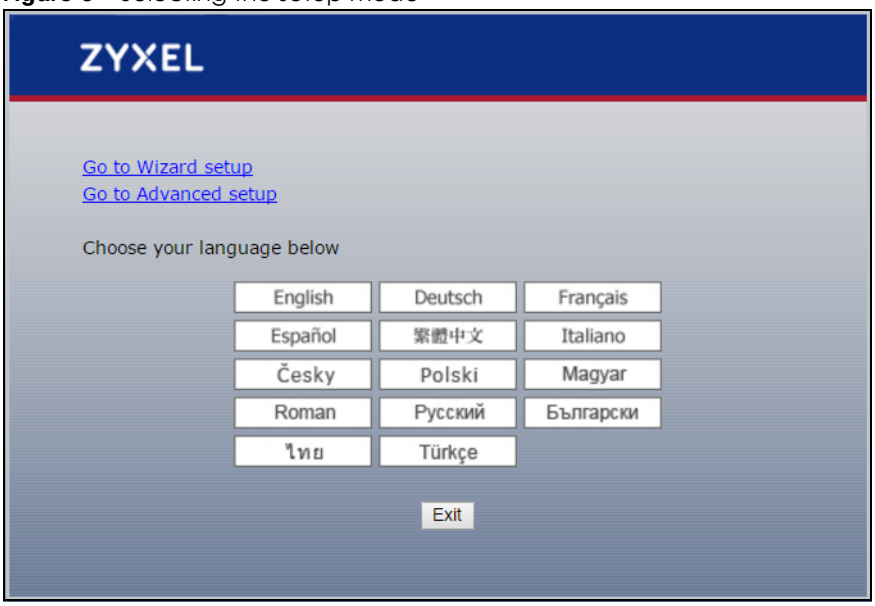


Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the WAP3205 v3 if this happens.

6 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 11 on page 82.

Figure 6 Selecting the setup mode



2.4 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 "192.168.1.2".

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.

CHAPTER 3
Connection Wizard

3.1 Overview

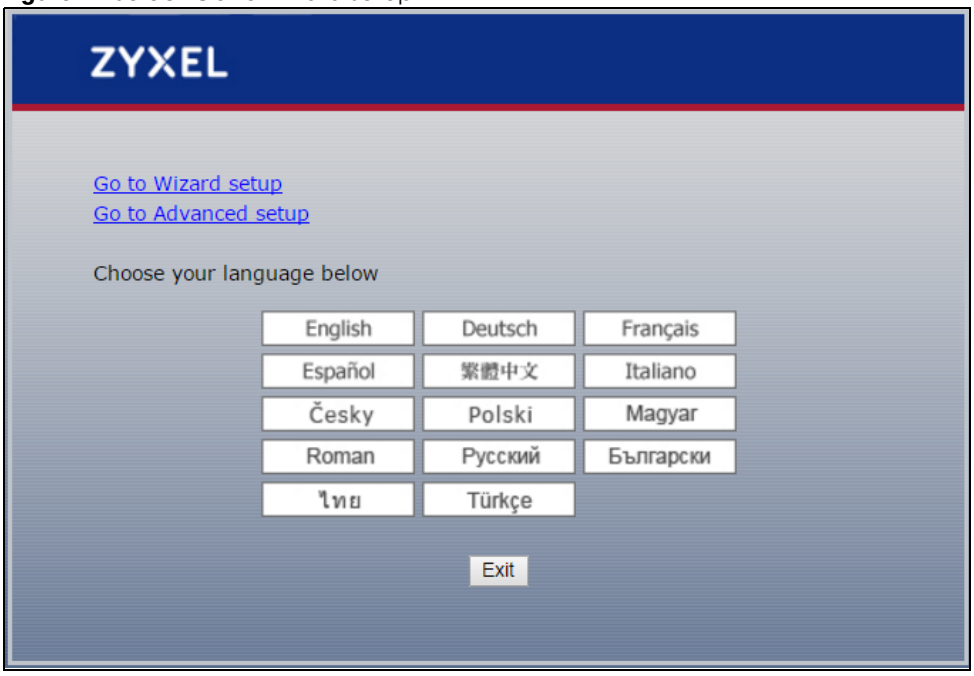
This chapter provides information on the wizard setup screens in the Web Configurator.

The Web Configurator's wizard setup helps you configure your device to access the Internet. Leave a field blank if you don't have that information.

3.2 Accessing the Wizard

1 After you access the WAP3205 v3 Web Configurator, click **Go to Wizard setup**.

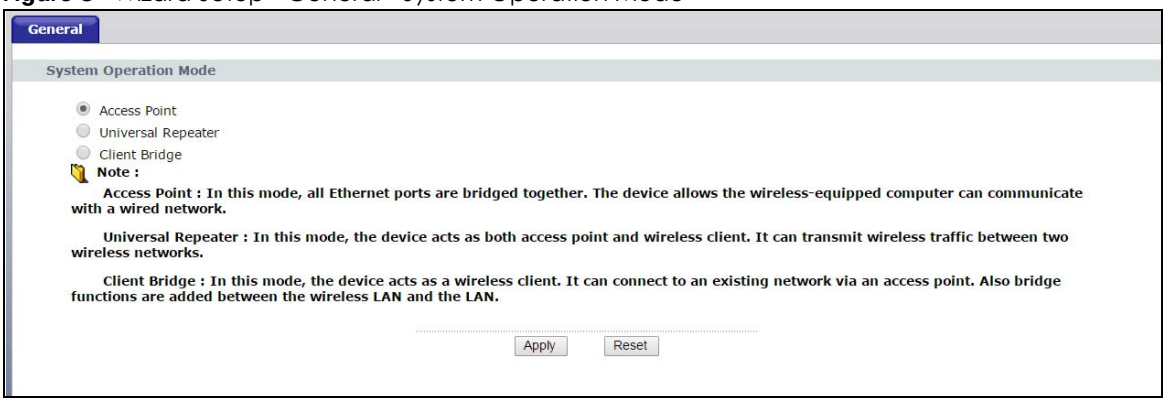
Figure 7 Select Go to Wizard setup



3.3 Choosing a System Operation Mode

The WAP3205 v3 offers three different system operation modes: Access Point mode, Universal Repeater mode and Client Bridge mode. To learn more about each mode refer to Chapter 4 on page 33. When you click on the Wizard Setup the following screen opens.

Figure 8 Wizard Setup - General> System Operation Mode



The following table describes the labels in this screen.

Table 3 Wizard Setup - General> System Operation Mode

LABEL	DESCRIPTION
Access Point	Select **Access Point** to allow wireless devices to communicate with a wired network.
Universal Repeater	Select **Universal Repeater** to transmit traffic between two wireless networks.
Client Bridge	Select **Client Bridge** to connect your WAP3205 v3 to an existing network via an access point.
Apply	Click **Apply** to save the changes to your WAP3205 v3.
Reset	Click **Reset** to reload the previous configuration of this screen.

Note: After choosing an operating mode, the next screen will vary according to the mode you have selected. If you have selected an operating mode different than the current mode, your WAP3205 v3 will restart.

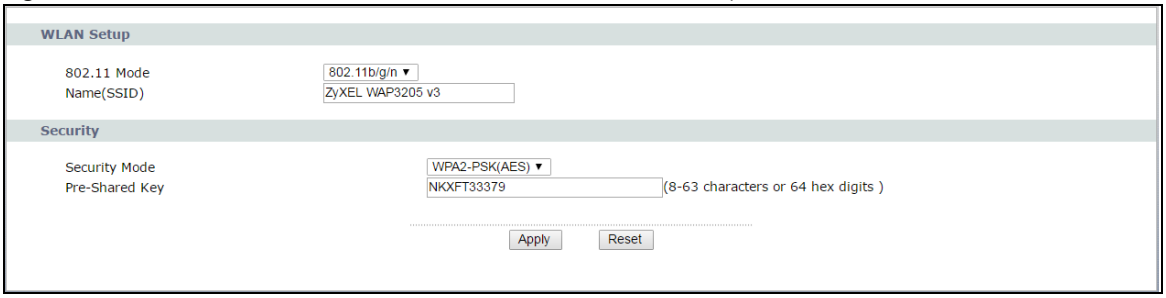
3.4 Connection Wizard - Access Point Mode

The WAP3205 v3's system operation mode is set to access point mode by default. In this mode your WAP3205 v3 bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet.

3.4.1 WLAN Setup

The following screen will open. Use this screen to configure the WAP3205 v3's wireless network settings.

Figure 9 Connection Wizard - Access Point Mode> WLAN Setup



The following table describes the labels in this screen.

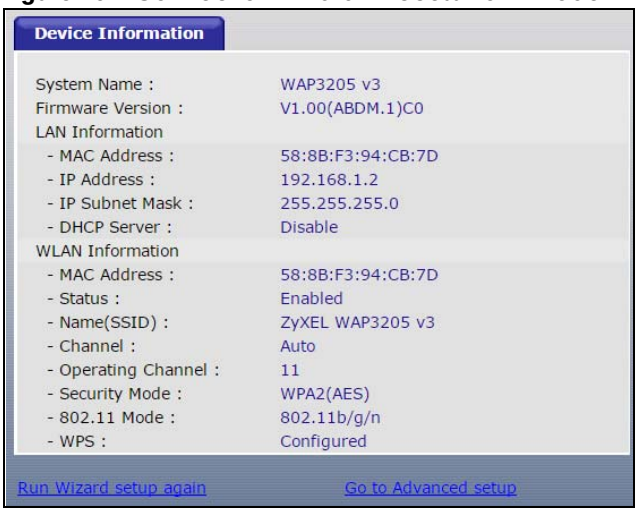
Table 4 Connection Wizard - Access Point Mode> WLAN Setup

LABEL	DESCRIPTION
WLAN Setup	
802.11 Mode	Select the wireless standard the WAP3205 v3 uses.
Name (SSID)	Type the descriptive name used to identify the WAP3205 v3 in the wireless LAN.
Security	
Security Mode	Select the data encryption method the WAP3205 v3 uses for wireless connection. When you select to use a security, the **Pre-Shared Key** field appears in this screen. You can also select **None** to allow any client to associate this network without any data encryption or authentication.
Pre-Shared Key	Enter the password that lets you connect to the WAP3205 v3. Your password should be in a string of ASCII characters between 8 and 63 or hexadecimal characters between 8 and 64.
Apply	Click **Apply** to save the changes to your WAP3205 v3.
Reset	Click **Reset** to reload the previous configuration of this screen.

3.4.2 Device Information

After configuring the general settings for your WAP3205 v3's wireless network. The following screen displays, showing all the details about your device.

Figure 10 Connection Wizard - Access Point Mode> Device Information



The following table describes the labels in this screen.

Table 5 Connection Wizard - Access Point Mode> Device Information

LABEL	DESCRIPTION
System Name	This is the WAP3205 v3's model name.
Firmware Version	This is the current firmware version of the WAP3205 v3.
LAN Information	
- MAC Address	This shows the LAN Ethernet MAC Address of your device.

Table 5 Connection Wizard - Access Point Mode> Device Information

LABEL	DESCRIPTION
- IP Address	This shows the LAN port's IP Address.
- IP Subnet Mask	This shows the LAN port's IP 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 - **Enabled** or **Disabled**.
- 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 **Auto** when the WAP3205 v3 automatically scans and selects the Wireless Lan's channel.
- Operating Channel	This shows the current channel number the WAP3205 v3 uses over the wireless LAN.
- Security Mode	This shows the data encryption method the WAP3205 v3 uses for the wireless connection.
- 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.
- WPS	This displays **Configured** when the WPS (Wi-Fi Protected Setup) has been set up. This displays **Unconfigured** if the WPS has not been set up.
Run Wizard setup again	Click here to run the Wizard setup one more time.
Go to advanced settings	Click here to go to your WAP3205 v3's advanced settings.

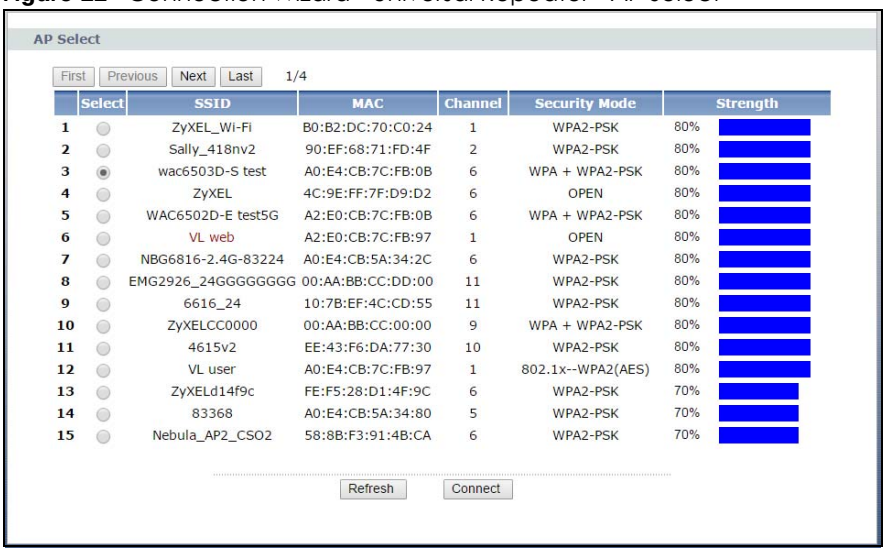
3.5 Connection Wizard - Universal Repeater Mode

In Universal Repeater mode, your WAP3205 v3 can act as an access point and wireless client at the same time.

3.5.1 AP Select

The following screen will open. Use this screen to connect the WAP3205 v3 to a wireless network.

Figure 11 Connection Wizard - Universal Repeater> AP Select



The following table describes the labels in this screen.

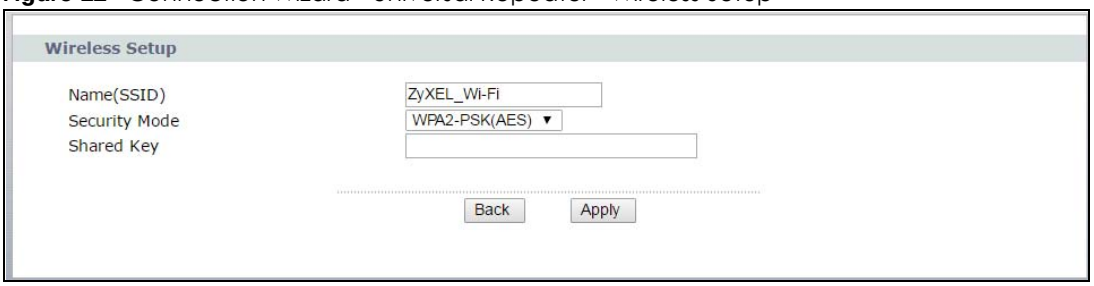
Table 6 Connection Wizard - Universal Repeater> AP Select

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** to go to the last page of the AP select table.
Select	Click to choose the wireless device your WAP3205 v3 will connect to.
SSID	This displays 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 shows the channel number used by the wireless device.
Security Mode	This shows 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.

3.5.2 Wireless Setup

After you click **Connect** the following screen will open. Use this screen to enter the Wi-FI key if wireless security is enabled on the selected AP.

Figure 12 Connection Wizard - Universal Repeater> Wireless Setup



The following table describes the labels in this screen.

Table 7 Connection Wizard - Universal Repeater> Wireless Setup

LABEL	DESCRIPTION
Wireless Setup	
Name (SSID)	This shows the descriptive name of the wireless device you want the WAP3205 v3 to connect to.
Security Mode	This shows the type of security configured on the wireless device.
Shared Key	Type the wireless device's password to connect.
Back	Click **Back** to return to the list of wireless devices.
Apply	Click **Apply** to associate with the selected wireless device.

3.5.3 WLAN Information

After your WAP3205 v3 has connected to a wireless device, use the following screen to configure the wireless settings between the WAP3205 v3 and its wireless clients.

Figure 13 Connection Wizard - Universal Repeater> WLAN Information

The following table describes the labels in this screen.

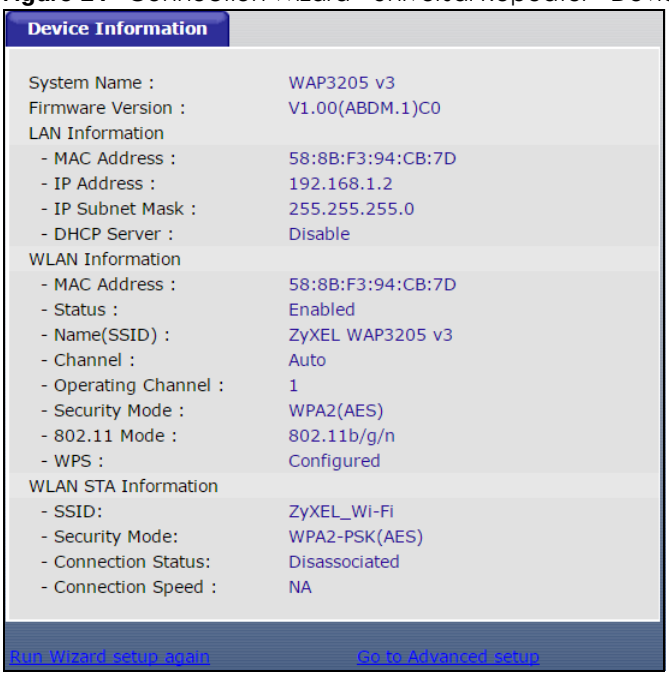
Table 8 Connection Wizard - Universal Repeater> WLAN Information

LABEL	DESCRIPTION
WLAN STA Information	
SSID	This is the name of the selected AP the WAP3205 v3 is associating with.
Security Mode	This shows the type of security configured on the wireless device.
Operating Channel	This shows the channel the WAP3205 v3 is using to connect to the wireless device.
WLAN AP Information	
802.11 Mode	Select the wireless standard the WAP3205 v3's wireless LAN uses.
Name (SSID)	Type the descriptive name used to identify the WAP3205 v3 in the wireless LAN.
Security	
Security Mode	Select the data encryption method the WAP3205 v3 uses for wireless connection. Choose **WPA2-PSK (AES)** security to configure a Pre-Shared Key in the box below.
Pre-Shared Key	Enter the password that lets you connect to the WAP3205 v3. Your password should be in a string of ASCII characters between 8 and 63 or hexadecimal characters between 8 and 64.
Apply	Click **Apply** to save the changes to your WAP3205 v3.
Reset	Click **Reset** to reload the previous configuration of this screen.

3.5.4 Device Information

After connecting to an AP and configuring the WAP3205 v3's wireless LAN, the following screen will open, providing detailed information about your device.

Figure 14 Connection Wizard - Universal Repeater> Device Information



The following table describes the labels in this screen.

Table 9 Connection Wizard - Universal Repeater> Device Information

LABEL	DESCRIPTION
System Name	This is the WAP3205 v3's model name.
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 IP 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 - **Enabled** or **Disabled**.
- 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 **Auto** when the WAP3205 v3 automatically scans and selects the Wireless Lan's channel.
- Operating Channel	This shows the current channel number the WAP3205 v3 uses over the Wireless LAN.
- Security Mode	This shows the data encryption method the WAP3205 v3 uses for the wireless connection.
- 802.11 Mode	This shows the wireless standard the WAP3205 v3 uses.

Table 9 Connection Wizard - Universal Repeater> Device Information

LABEL	DESCRIPTION
- WPS	This displays **Configured** when the WPS has been set up. This displays **Unconfigured** if the WPS has not been set up.
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 wireless device.
- Connection Status	This shows whether the WAP3205 v3 is currently associated with the selected AP.
- Connection Speed	This shows the connection speed between the WAP3205 v3 and the selected AP.
Run Wizard setup again	Click here to run the Wizard setup one more time.
Go to Advanced setup	Click here to go to your WAP3205 v3's advanced settings.

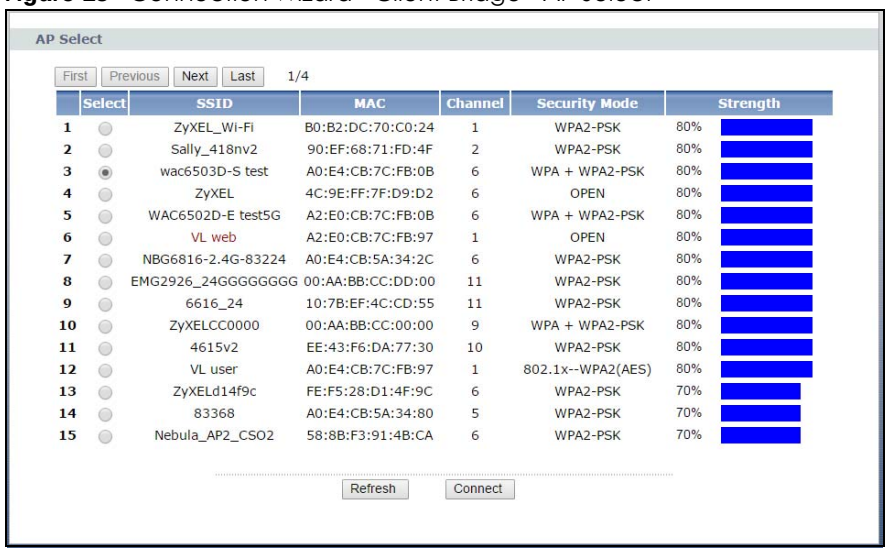
3.6 Connection Wizard - Client Bridge Mode

The WAP3205 v3's system operation mode is now Client Bridge, your WAP3205 v3 can act as a wireless client to connect to an existing network via an access point.

3.6.1 AP Select

The **AP Select** screen will open. Use this screen to connect your WAP3205 v3 to an access point in the area.

Figure 15 Connection Wizard - Client Bridge> AP Select



The following table describes the labels in this screen.

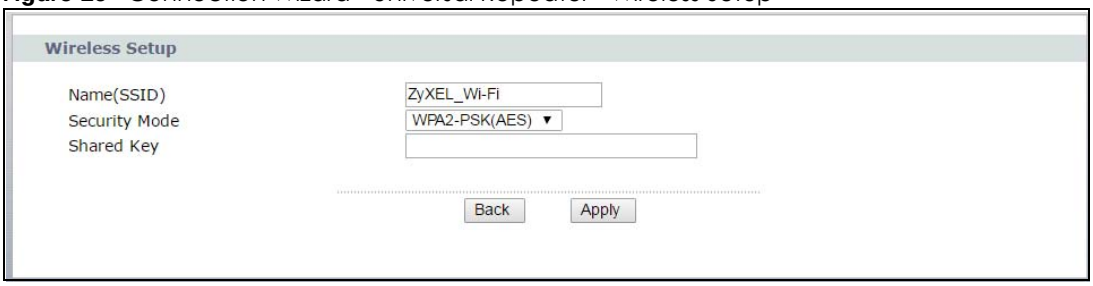
Table 10 Connection Wizard - Client Bridge> AP Select

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** to go to the last page of the AP select table.
Select	Click to choose the wireless device your WAP3205 v3 will connect to.
SSID	This displays 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 shows the channel number used by the wireless device.
Security Mode	This shows 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.

3.6.2 Wireless Setup

After you click **Connect** the following screen will open. Use this screen to enter the Wi-FI key if wireless security is enabled on the selected AP.

Figure 16 Connection Wizard - Universal Repeater> Wireless Setup



The following table describes the labels in this screen.

Table 11 Connection Wizard - Universal Repeater> Wireless Setup

LABEL	DESCRIPTION
Wireless Setup	
Name (SSID)	This shows the descriptive name of the wireless device you want the WAP3205 v3 to connect to.

Table 11 Connection Wizard - Universal Repeater> Wireless Setup

LABEL	DESCRIPTION
Security Mode	This shows the type of security configured on the wireless device.
Shared Key	Type the wireless device's password to connect.
Back	Click **Back** to return to the list of wireless devices.
Apply	Click **Apply** to associate with the selected wireless device.

3.6.3 Device Information

After connecting to an AP, the following screen will open.

Figure 17 Connection Wizard- Client Bridge> Device Information

The following table describes the labels in this screen.

Table 12 Connection Wizard - Client Bridge> Device Information

LABEL	DESCRIPTION
System Name	This is the WAP3205 v3's model name.
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 IP Subnet Mask.
- DHCP Server	This shows the LAN port's DHCP server status.
WLAN STA Information	
- SSID	This shows a descriptive name used to identify the WAP3205 v3 in the wireless LAN.
- Security Mode	This shows the wireless security the WAP3205 v3 is using to connect to the wireless device.
- Connection Status	This shows whether the WAP3205 v3 is currently associated with the selected AP.

Table 12 Connection Wizard - Client Bridge> Device Information

LABEL	DESCRIPTION
Run Wizard setup again	Click here to run the Wizard setup one more time.
Go to Advanced setup	Click here to go to your WAP3205 v3's advanced settings.

CHAPTER 4
Modes

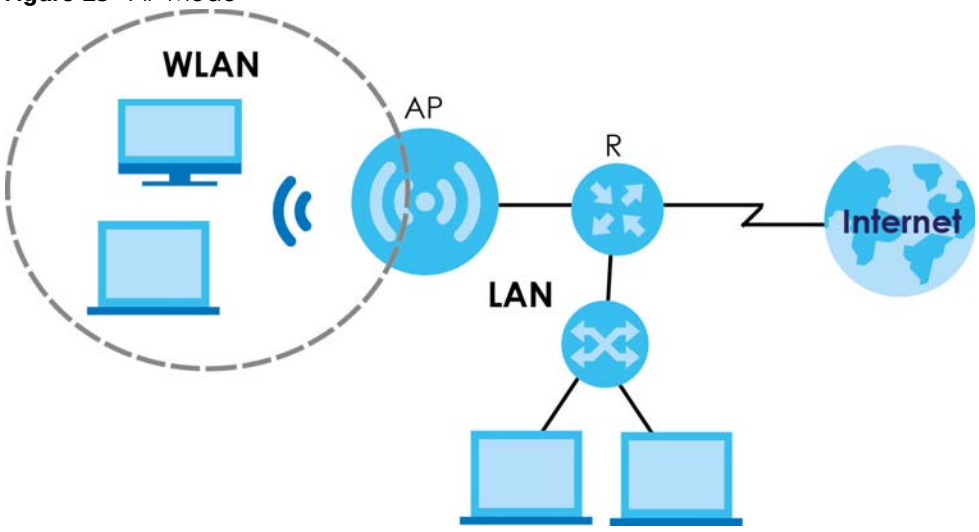
4.1 Overview

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.

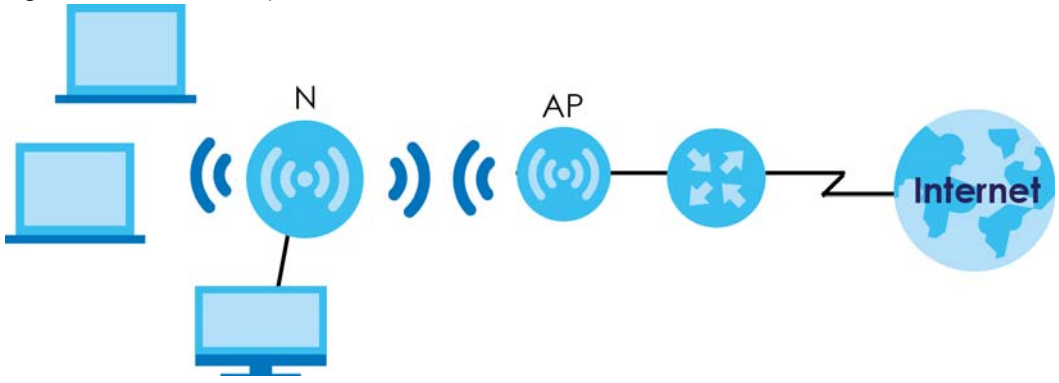
- **Access Point**: Use this mode if you already have a Router (R) in your network and you want to set up a wireless network and bridge the wired and wireless connections on the WAP3205 v3.

Figure 18 AP Mode



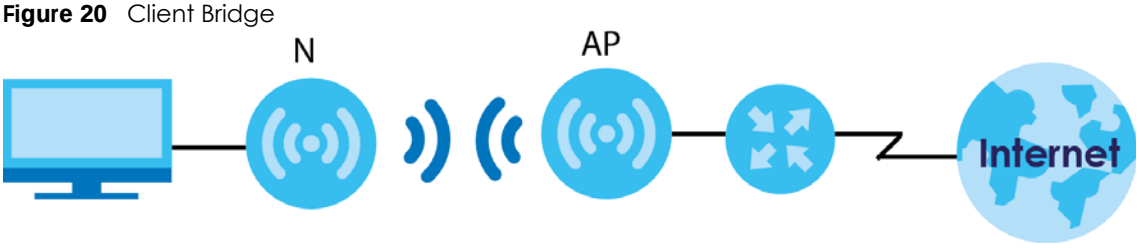
- **Universal Repeater**: In this mode, the WAP3205 v3 (N) can be an access point and a wireless client at the same time. Use this mode if there is an existing wireless router or access point in your network and you want the WAP3205 v3 (N) to wirelessly relay communications from its wireless clients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

Figure 19 Universal Repeater



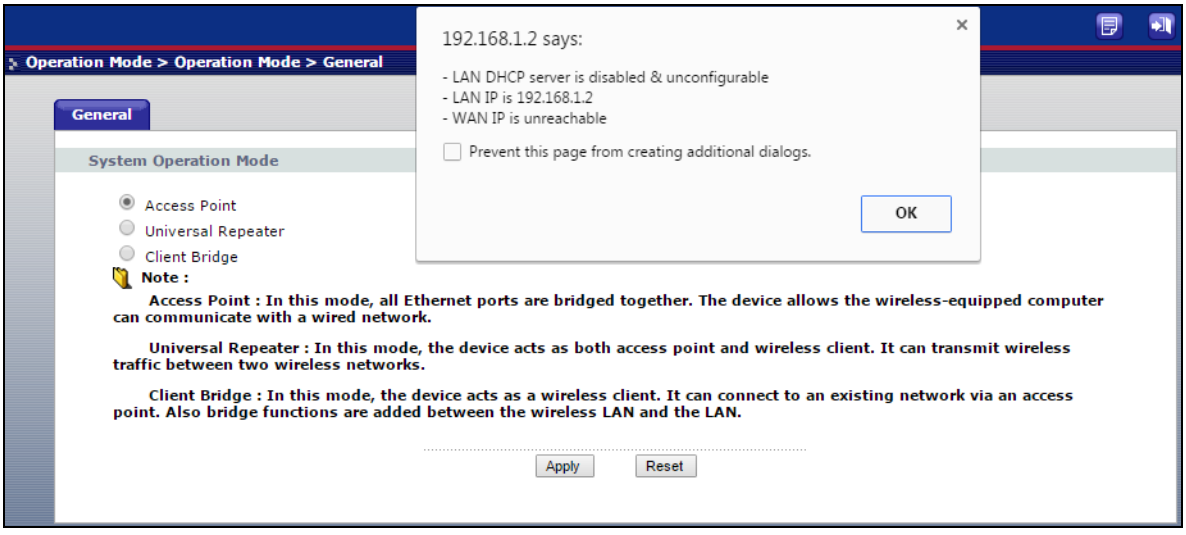
- **Client Bridge**: Use this mode to have the WAP3205 v3 (N) work only as a wireless client if there is an existing wireless router or access point in the network to which you want to connect your local network wirelessly. In this mode, you should know the SSID and wireless security details of the access point to which you want to connect.

Figure 20 Client Bridge



4.2 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 192.168.1.2. The WAP3205 v3 cannot assign your computer an IP address, so you must give it a fixed IP address in the range between 192.168.1.3 and 192.168.1.254 (Section 2.2 on page 14).
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 14 for instructions on how to do this.
5. Go to **Operation Mode > General** and select **Access Point**.



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.

4.2.1 Status Screen (AP Mode)

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

Figure 21 Status Screen (AP Mode)

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

Table 13 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 - **Enabled** or **Disabled**.
- 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 **Auto** when the WAP3205 v3 automatically scans and selects the Wireless Lan's channel.
- Operating Channel	This shows the current channel number the WAP3205 v3 uses for the wireless connection.
- Security Mode	This shows the data encryption method the WAP3205 v3 uses.
- 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 13 Status Screen (AP Mode) (continued)

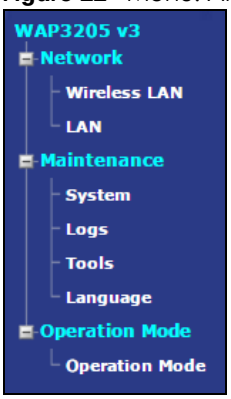
LABEL	DESCRIPTION
- WPS	This displays **Configured** when the WPS (Wi-Fi Protected Setup) has been set up. This displays **Unconfigured** if the WPS has not been set up.
System Status	
Operation Mode	This field shows the device operating mode: **Access Point**, **Universal Repeater** or **Client Bridge**.
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.
Interface Status	
Interface	This displays the WAP3205 v3 port types.
Status	For the LAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected). For the WLAN, it displays **Up** when the WLAN is enabled or **Down** when the WLAN is disabled.
Rate	For the LAN ports, this displays the port speed or **N/A** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **N/A** when the WLAN is disabled.
Summary	
Client Table	Use this screen to view current client information. Click "**Details...**" to see the screen.
Packet Statistics	Use this screen to view port status and packet specific statistics. Click "**Details...**" to see the screen.
Message	Use this screen to view the status of the WAP3205 v3.

4.2.2 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 22 Menu: AP Mode



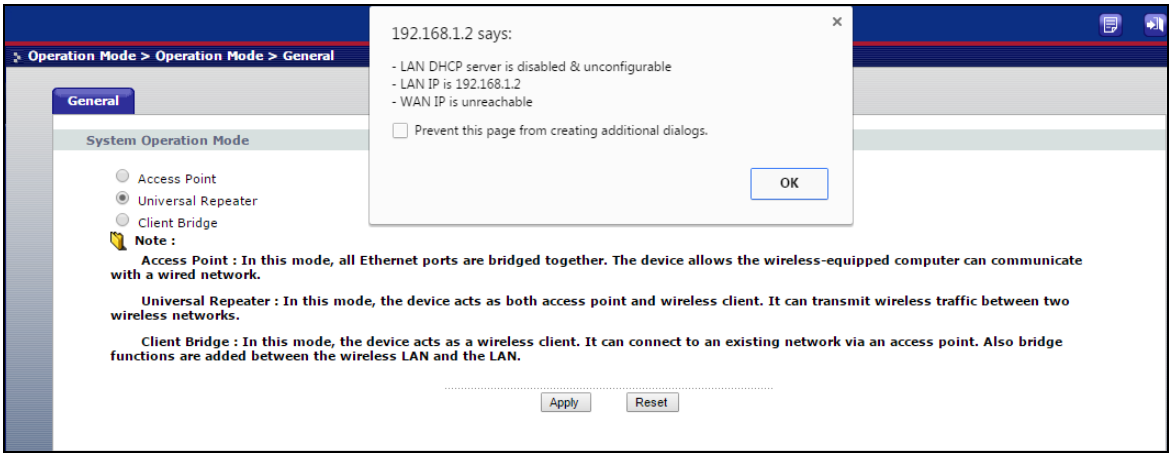
The following table describes the sub-menus.

Table 14 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.
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.
	Language	This screen allows you to select the language you prefer.
Operation Mode	General	This screen allows you to select the device operating mode: **Access Point**, **Universal Repeater** or **Client Bridge**.

4.3 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 give your computer a fixed IP address in the range between 192.168.1.3 and 192.168.1.254 (Section 2.2 on page 14).
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 14 for instructions on how to do this.
5. Go to **Operation Mode > General** and select **Universal Repeater**.



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.

4.3.1 Status Screen (Universal Repeater Mode)

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

Figure 23 Status Screen (Universal Repeater Mode)

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

Table 15 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 - **Enabled** or **Disabled**.
- 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 **Auto** when the WAP3205 v3 automatically scans and selects the Wireless LAN's channel.
- Operating Channel	This shows the current channel number the WAP3205 v3 uses over the Wireless LAN.
- Security Mode	This shows the data encryption method the WAP3205 v3 uses for the wireless connection.
- 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.
- WPS	This displays **Configured** when the WPS has been set up. This displays **Unconfigured** if the WPS has not been set up.
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 wireless device.
- Connection Status	This shows whether the WAP3205 v3 is currently associated with the selected AP.
System Status	
Operation Mode	This field shows the device operating mode: **Access Point**, **Universal Repeater** or **Client Bridge**.
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.
Interface Status	
Interface	This displays the WAP3205 v3 port types.
Status	For the LAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected). For the WLAN, it displays **Up** when the WLAN is enabled or **Down** when the WLAN is disabled.

Table 15 Status Screen (Universal Repeater Mode) (continued)

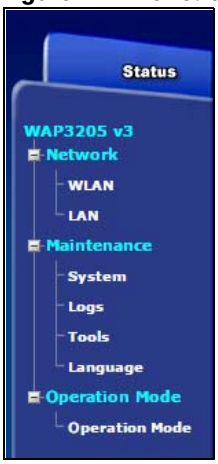
LABEL	DESCRIPTION
Rate	For the LAN ports, this displays the port speed or **N/A** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **N/A** when the WLAN is disabled.
Summary	
Client table	Use this screen to view current client information. Click "**Details...**" to see the screen.
Packet Statistics	Use this screen to view port status and packet specific statistics. Click "**Details...**" to see the screen.
Message	Use this screen to view the status of the WAP3205 v3.

4.3.2 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 24 Menu: Universal Repeater Mode



The following table describes the sub-menus.

Table 16 Menu: Universal Repeater Mode

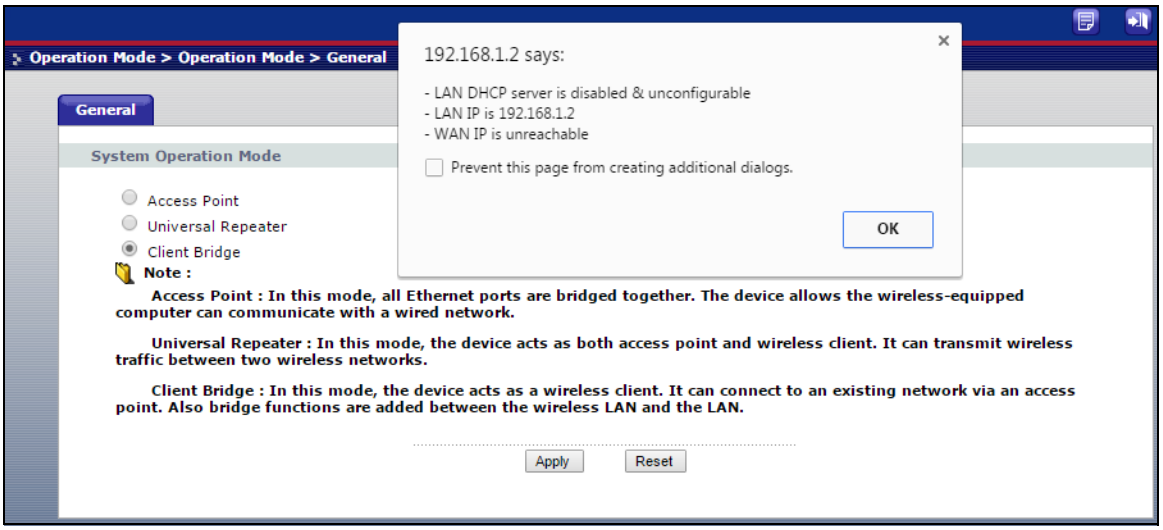
LINK	TAB	FUNCTION
Status		This screen shows the WAP3205 v3's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
Network		

Table 16 Menu: Universal Repeater Mode (continued)

LINK	TAB	FUNCTION
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.
	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.
	Language	This screen allows you to select the language you prefer.
Operation Mode	General	This screen allows you to select the device operating mode: **Access Point**, **Universal Repeater** or **Client Bridge**.

4.4 Setting your WAP3205 v3 to Client Bridge 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 give your computer a fixed IP address in the range between 192.168.1.3 and 192.168.1.254 (Section 2.2 on page 14).
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 14 for instructions on how to do this.
5. Go to **Operation Mode > General** and select **Client Bridge**.



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 **Client Bridge** mode.

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

4.4.1 Status Screen (Client Bridge Mode)

Click on **Status**. The screen below shows the status screen in **Client Bridge** mode.

Figure 25 Status Screen (Client Bridge Mode)

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

Table 17 Status Screen (Client Bridge Mode)

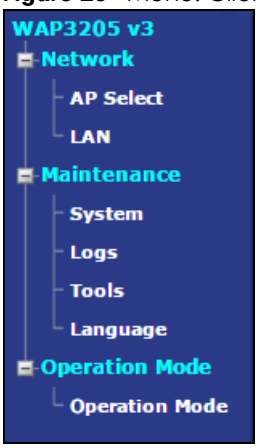
LABEL	DESCRIPTION
Device Information	
System Name	This is the **System Name** you enter in the **Maintenance** > **System** > **General** screen. It is for identification purposes.
Firmware Version	This is the current firmware version of the WAP3205 v3.
LAN Information	
- MAC Address	This shows the LAN 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 status of the LAN port's DHCP server.
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 operating mode: **Access Point**, **Universal Repeater** or **Client Bridge**.
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.
Interface Status	
Interface	This displays the WAP3205 v3 port types.
Status	For the LAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected). For the WLAN, it displays **Up** when the WLAN is enabled or **Down** when the WLAN is disabled.
Rate	For the LAN ports, this displays the port speed or **N/A** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **N/A** when the WLAN is disabled.
Summary	
Client Table	Use this screen to view information of the client that is currently connected to the WAP3205 v3's Ethernet LAN port.
Packet Statistics	Use this screen to view port status and packet specific statistics.

4.4.2 Universal Repeater Navigation Panel

Use the menu in the navigation panel to configure WAP3205 v3 features in **Client Bridge Mode**.

The following screen and table show the features you can configure in **Client Bridge Mode**.

Figure 26 Menu: Client Bridge Mode



The following table describes the sub-menus.

Table 18 Menu: Client Bridge 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		
AP Select	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.
	WLAN Information	Use this screen to view the SSID and security mode of the AP to which the WAP3205 v3 is connecting.
	Advanced	This screen allows you to configure advanced wireless settings.
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.
	Language	This screen allows you to select the language you prefer.
Operation Mode	General	This screen allows you to select the device operating mode: **Access Point**, **Universal Repeater** or **Client Bridge**.

CHAPTER 5
Tutorials

5.1 Overview

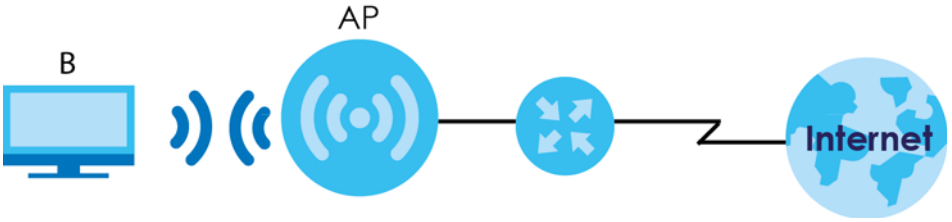
This chapter provides tutorials for your WAP3205 v3 as follows:

- How to Connect to the Internet from an AP
- Configure Wireless Security Using WPS on both your WAP3205 v3 and Wireless Client
- Connecting to the WAP3205 v3's Wi-Fi Network Manually (No WPS)

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 27 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 a wireless network using WPS. This example uses the WAP3205 v3 as the AP and a WPS-enabled Android smartphone as the wireless client.

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 WPS is enabled by default on the WAP3205 v3. If not, log into WAP3205 v3's Web Configurator and turn it on in the **Network > Wireless LAN > WPS** screen. You can either press the WPS button on the WAP3205 v3's panel or press **Push Button** in the **Network** > **Wireless LAN** > **WPS Station** screen.

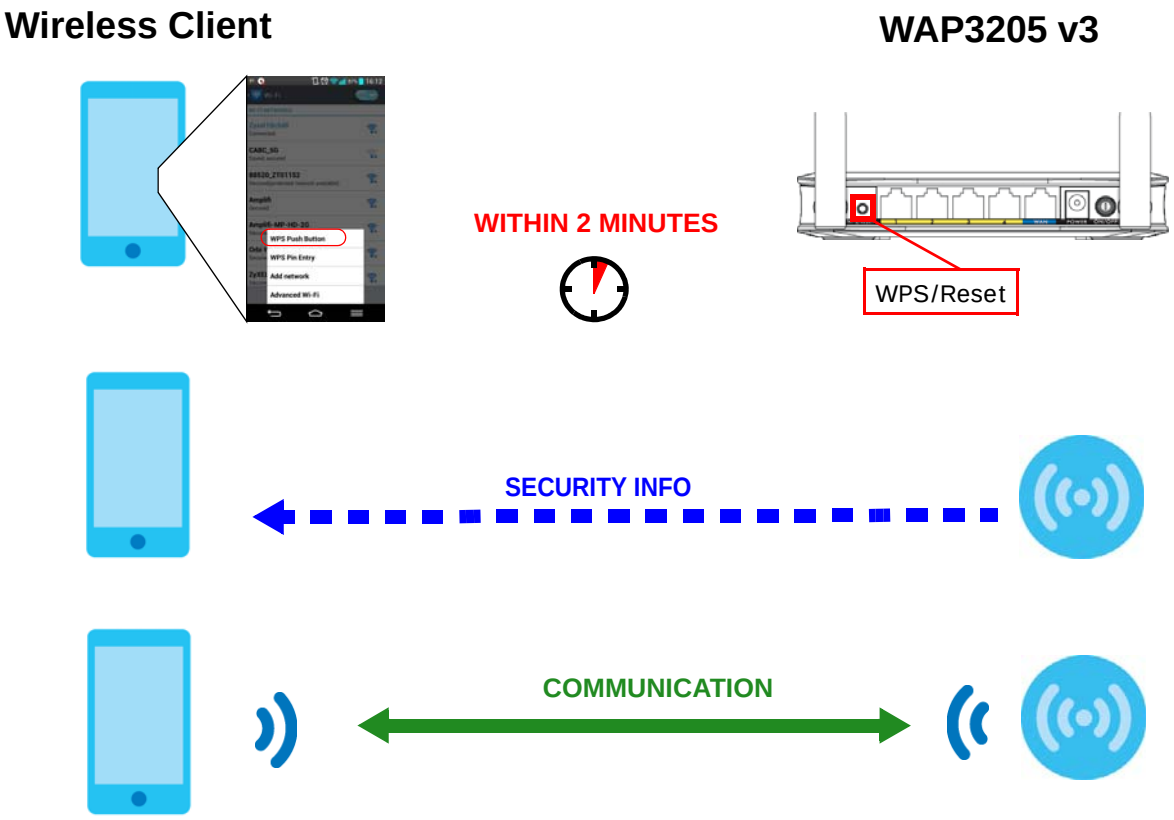
3 Go to your phone settings and turn on Wi-Fi. Open the Wi-Fi networks list and tap WPS Push Button or the WPS icon ( ).

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 Android smartphone in this example).

Figure 28 Example WPS Process: PBC Method



5.3.2 PIN Configuration

When you use the PIN configuration method, you need to check the client's PIN number and use the WAP3205 v3's configuration interface.

1. Go to your phone settings and turn on Wi-Fi. Open the Wi-Fi networks list and tap WPS PIN Entry get a PIN number.

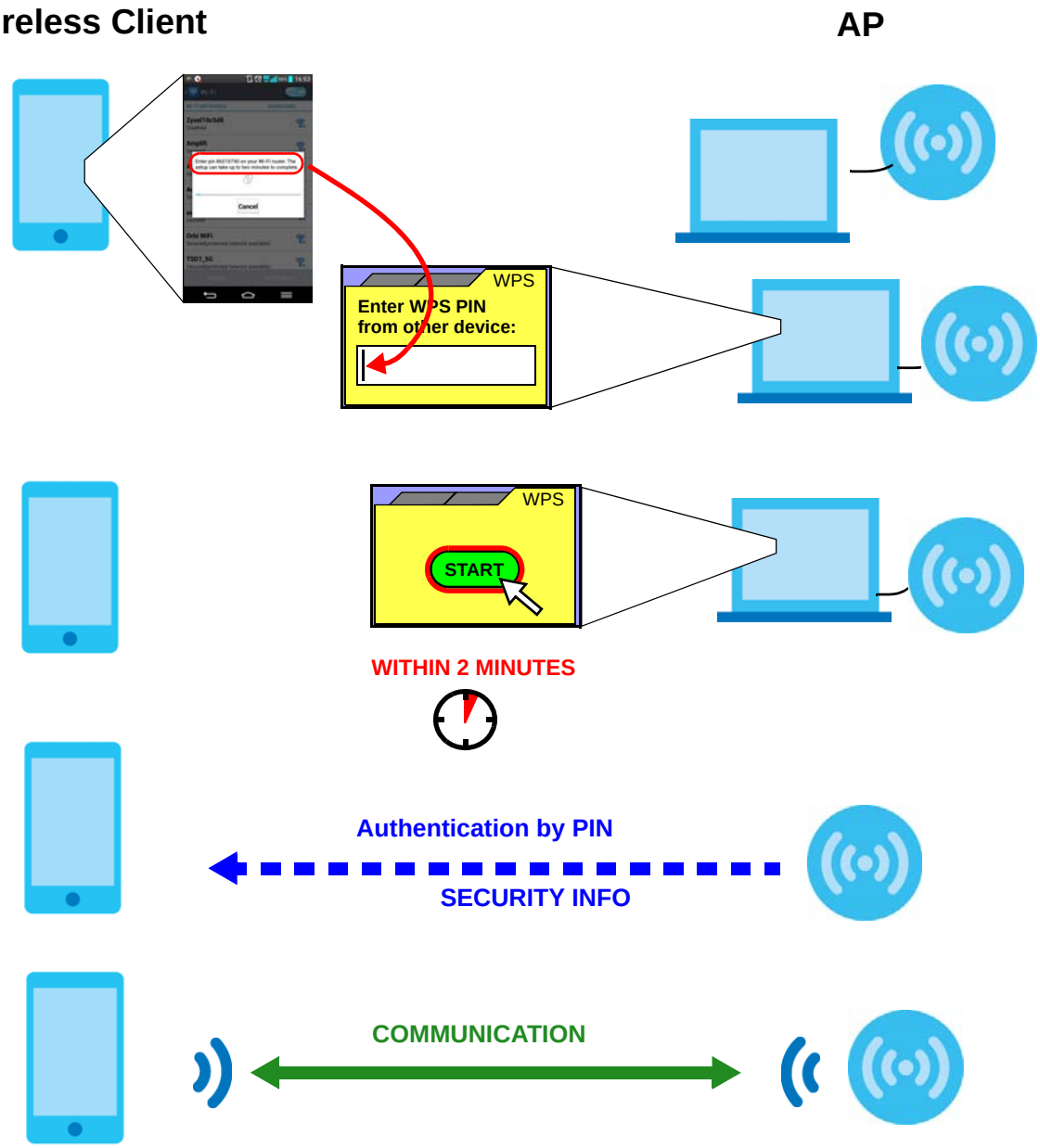
2. Enter the client's PIN number to the **PIN** field in the **Network** > **Wireless LAN** > **WPS Station** screen on the WAP3205 v3.

3. Click the **Start** button (or button next to the PIN field) on 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. the Android smartphone in this example) by using PIN method.

Figure 29 Example WPS Process: PIN Method



5.4 Connecting to the WAP3205 v3's Wi-Fi Network Manually (No WPS)

In this example, we change the WAP3205 v3's wireless settings, and then manually select the WAP3205 v3's new SSID and enter the Wi-Fi key to connect a wireless client to the WAP3205 v3.

5.4.1 Configuring Wireless Security on the WAP3205 v3

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

SSID	SSID_Example
Channel	Auto
Security	WPA2-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 2.3 on page 18).

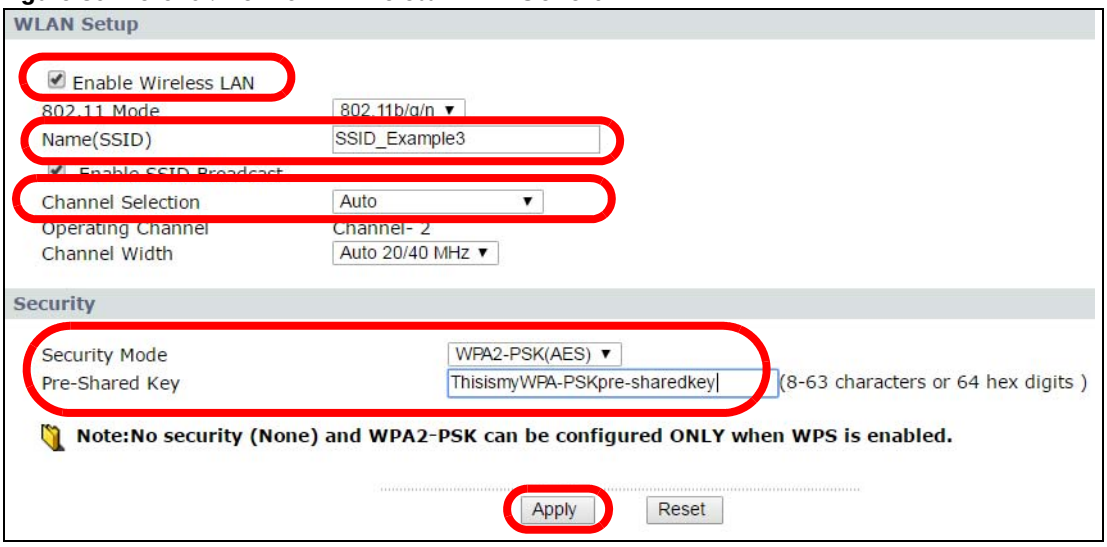
1 Open the **Network > Wireless LAN > General** screen in the WAP3205 v3's Web Configurator.

2 Make sure the **Enable Wireless LAN** check box is selected.

3 Enter **SSID_Example3** as the SSID and select **Auto** in the **Channel Selection** field to have the WAP3205 v3 scans for and select an available channel automatically.

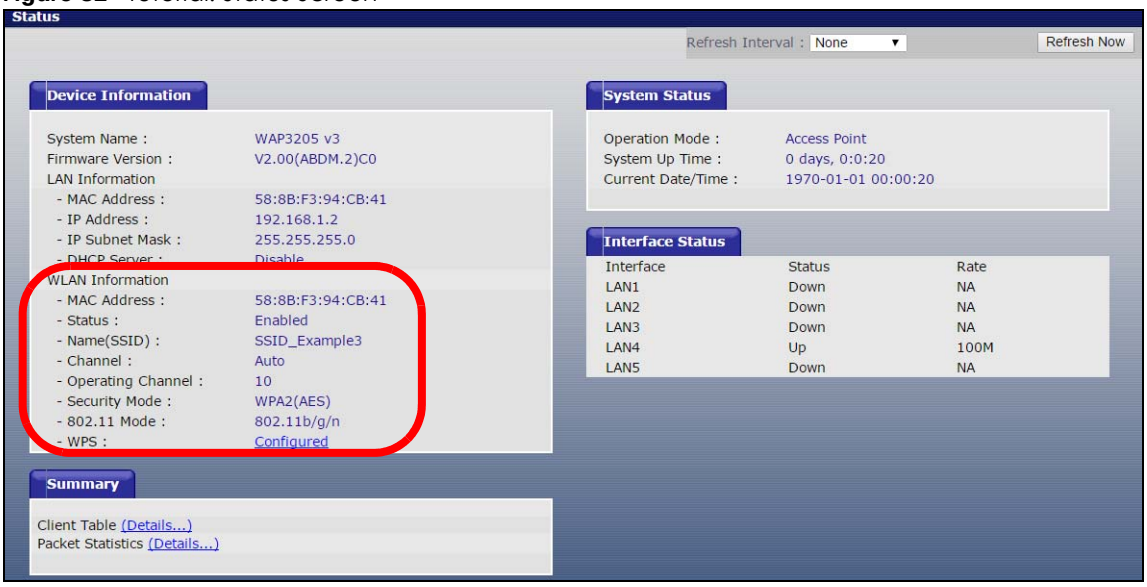
4 Set security mode to **WPA2-PSK(AES)** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.

Figure 30 Tutorial: Network > Wireless LAN > General



5 Open the **Status** screen. Verify your wireless and wireless security settings under **Device Information**.

Figure 31 Tutorial: Status Screen

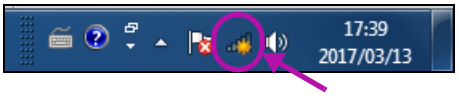


5.4.2 Configure Your Notebook

Note: In this example, we use a Windows 7 laptop that has a built-in wireless adapter as the wireless client.

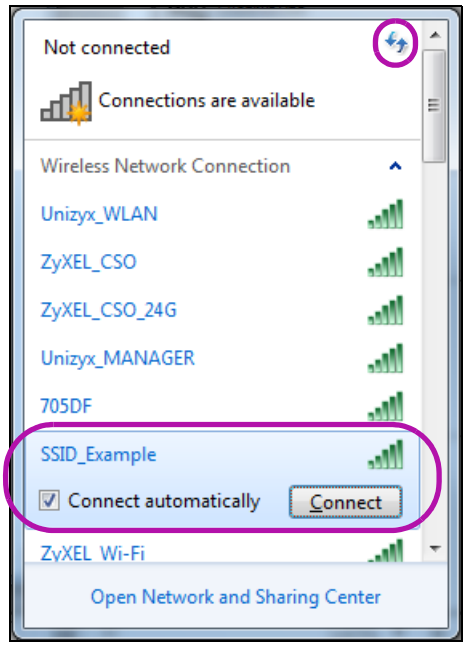
1 The WAP3205 v3 supports IEEE 802.11b, IEEE 802.11g and IEEE 802.11n wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

2 Click the Wi-Fi icon in your computer's system tray.

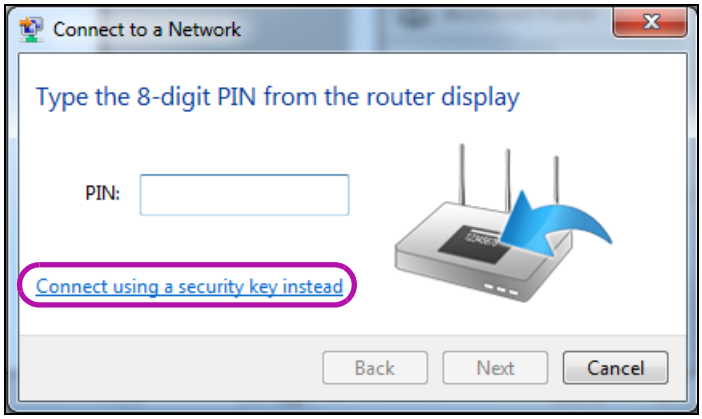


3 The **Wireless Network Connection** screen displays. Click the refresh button to update the list of the available wireless APs within range.

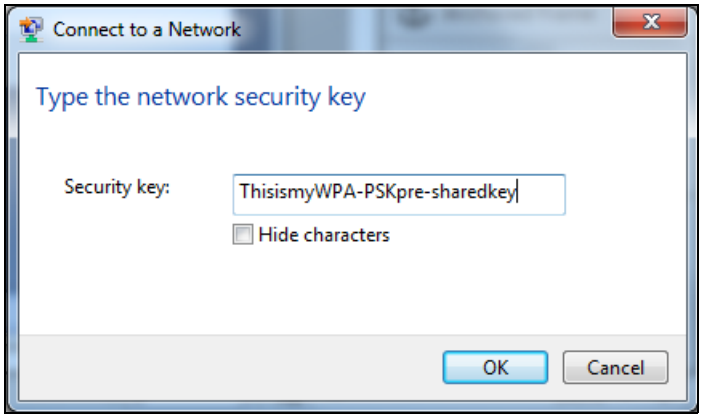
4 Select **SSID_Example3** and click **Connect**.



5 The following screen displays if WPS is enabled on the WAP3205 v3 but you didn't press the WPS button. Click **Connect using as security key instead**.



6 Type the security key in the following screen. Click **OK**.



7 Check the status of your wireless connection in the screen below.

8 If the wireless client keeps trying to connect to or acquiring an IP address from the WAP3205 v3, make sure you entered the correct security key.

If the connection has limited or no connectivity, make sure the WAP3205 v3 is connected to a router with the DHCP server enabled.

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.

PART II
Technical Reference

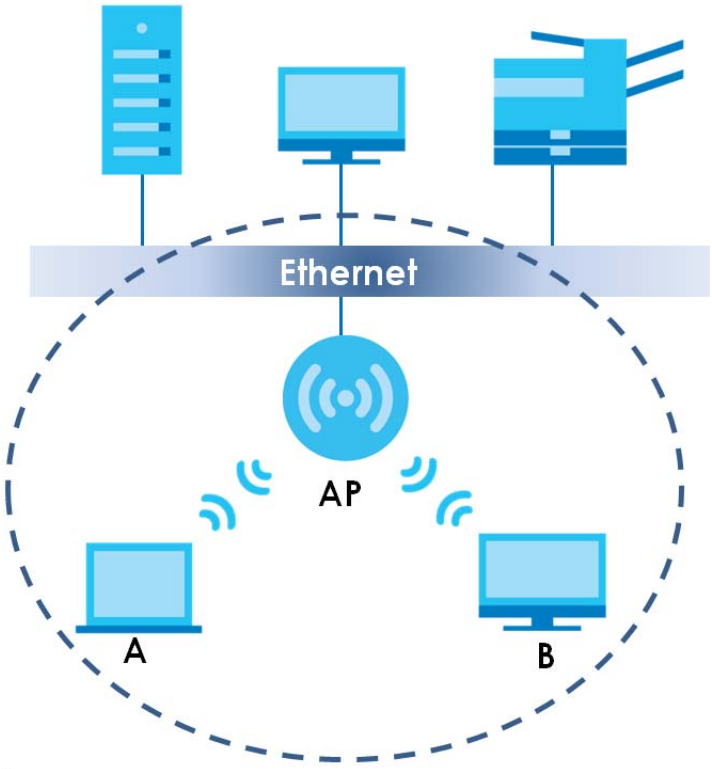
CHAPTER 6
Wireless LAN

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 32 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	Client Bridge
General	✔	✔	
MAC Filter	✔	✔	
Advanced	✔	✔	✔
WPS	✔	✔	
WPS Station	✔	✔	
Scheduling	✔	✔	
AP Select		✔	✔
WLAN Information			✔

See Chapter 4 on page 33 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 57).
- 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 61).
- Use the **Advanced** screen to allow intra-BSS networking and set the RTS/CTS Threshold (Section 6.6 on page 62).
- 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 63).
- Use the **WPS Station** screen to add a wireless station using WPS (Section 6.8 on page 64).
- Use the **Scheduling** screen to set the times your wireless LAN is turned on and off (Section 6.9 on page 65).
- 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 6.10 on page 66).
- Use the **WLAN Information** screen to view the SSID and security of the selected AP wireless network (Section 6.11 on page 67).

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 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.

6.3.3 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 19 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, WEP, WPA-PSK, or WPA2-PSK.

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.

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 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.

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.

6.3.4 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 45.

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 33 Network > Wireless LAN > General (Access Point Mode)

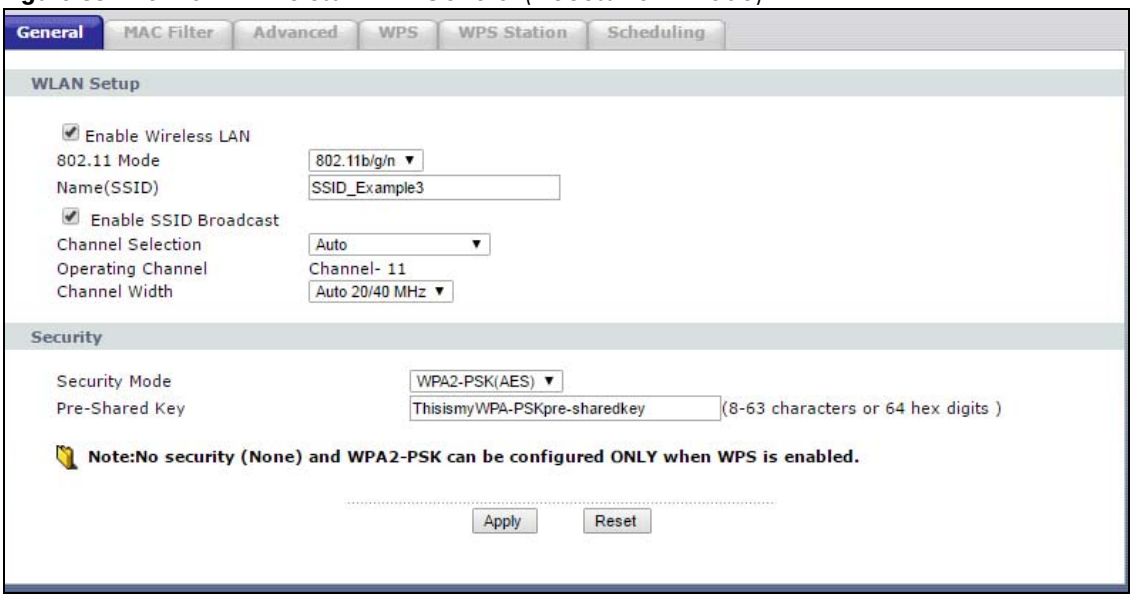
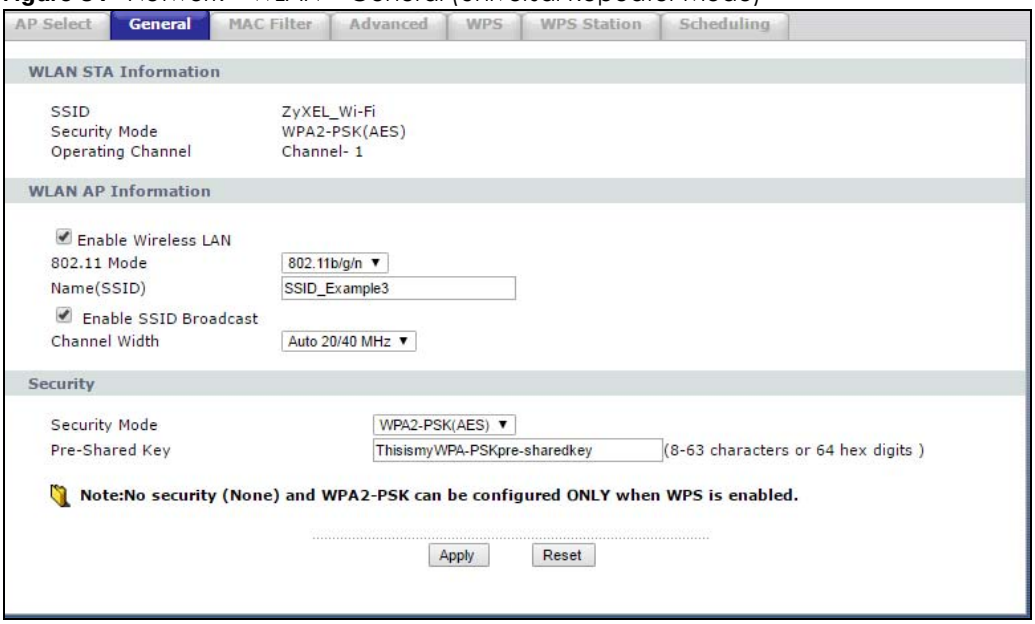


Figure 34 Network > WLAN > General (Universal Repeater Mode)



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

Table 20 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 v3 and 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.

Table 20 Network > Wireless LAN > General (continued)

LABEL	DESCRIPTION
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 **WEP**, **WPA-PSK(TKIP)**, **WPA-PSK(AES)**, **WPA2-PSK(TKIP)**, **WPA2-PSK(AES)** or **WPA-PSK/WPA2-PSK AES** 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 **None** to allow any client to associate this network without authentication.
Pre-Shared Key	Enter the password that lets you connect to the WAP3205 v3. Your password should be in a string of ASCII characters between 8 and 63 or hexadecimal characters between 8 and 64.
Apply	Click **Apply** to save your changes back to the WAP3205 v3.
Reset	Click **Reset** to reload the previous configuration for this screen.

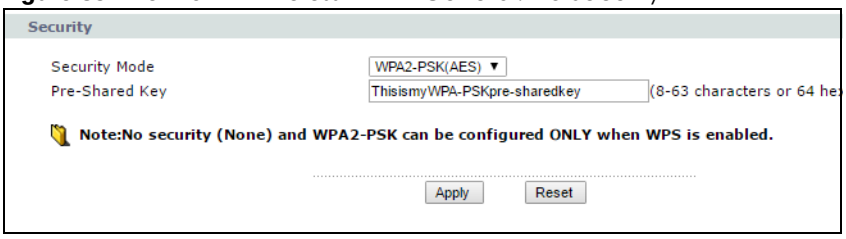
See the rest of this chapter for information on the other labels in this screen.

6.4.1 No Security

Select **None** 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 35 Network > Wireless LAN > General: No Security



The following table describes the labels in this screen.

Table 21 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.

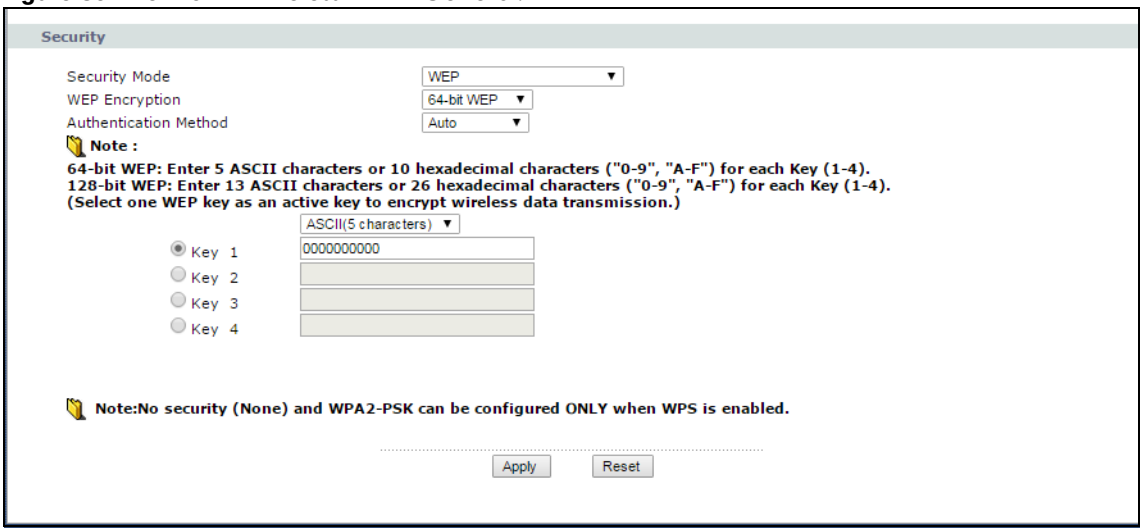
6.4.2 WEP Encryption

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 **WEP** from the **Security Mode** list.

Figure 36 Network > Wireless LAN > General: WEP



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

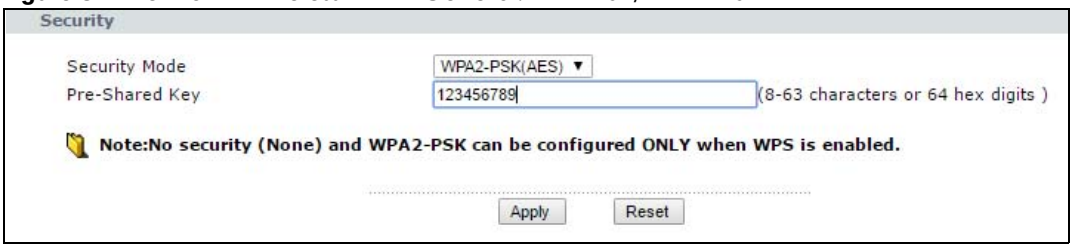
Table 22 Network > Wireless LAN > General: WEP

LABEL	DESCRIPTION
Security Mode	Choose **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** 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** unless you want to force a key verification before communication between the wireless client and the WAP3205 v3 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.
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 37 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK



The following table describes the labels in this screen.

Table 23 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK (AES)

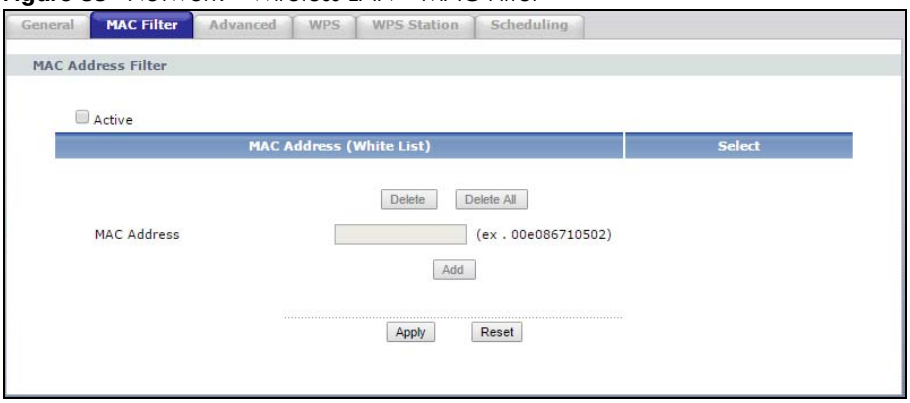
LABEL	DESCRIPTION
Security Mode	Choose **WPA-PSK** or **WPA2-PSK** from the drop downli Select **WPA-PSK/WPA2-PSK** to have both WPA2 and WPA wireless clients be able to communicate with the WAP3205 v3 even when the WAP3205 v3 is using WPA2-PSK.
Pre-Shared Key	**WPA-PSK/WPA2-PSK** uses a simple common 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").
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 38 Network > Wireless LAN > MAC Filter



The following table describes the labels in this menu.

Table 24 Network > Wireless LAN > MAC Filter

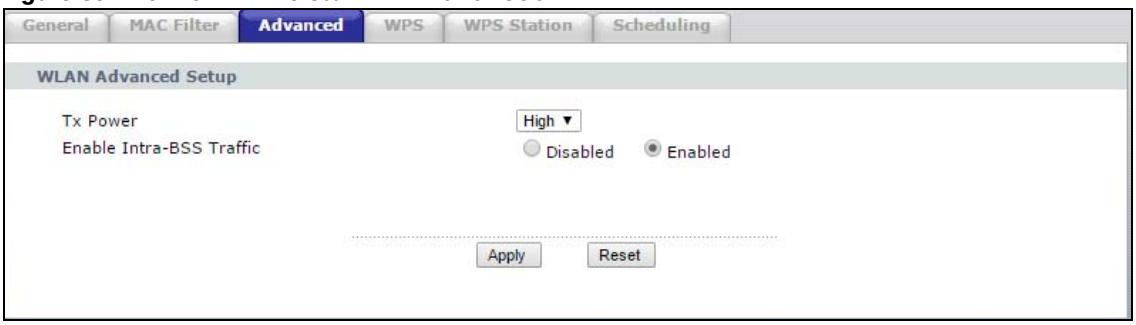
LABEL	DESCRIPTION
Active	Click **Active** check box to enable MAC address filtering.
MAC Address (White List)	This field shows the MAC addresses of the wireless station that are allowed or denied access to the WAP3205 v3 in these address fields. Enter the MAC addresses in a valid MAC address format, 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 39 Network > Wireless LAN > Advanced



The following table describes the labels in this screen.

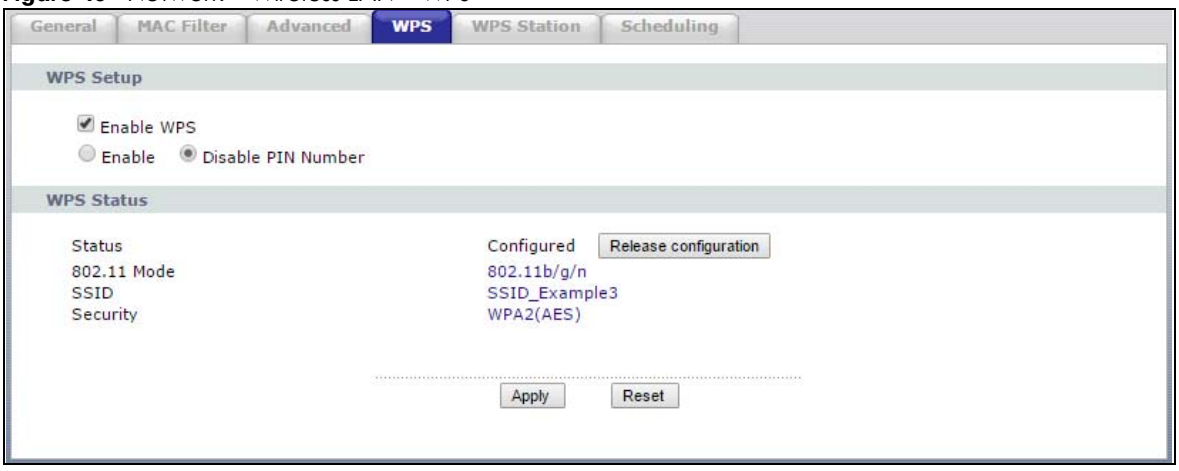
Table 25 Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
Wireless Advanced Setup	
Tx Power	This field controls the transmission power of the WAP3205 v3. If there is a high density of APs in an area, decrease the output power of the WAP3205 v3 to reduce interference with other APs.
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 40 Network > Wireless LAN > WPS



The following table describes the labels in this screen.

Table 26 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	

Table 26 Network > Wireless LAN > WPS (continued)

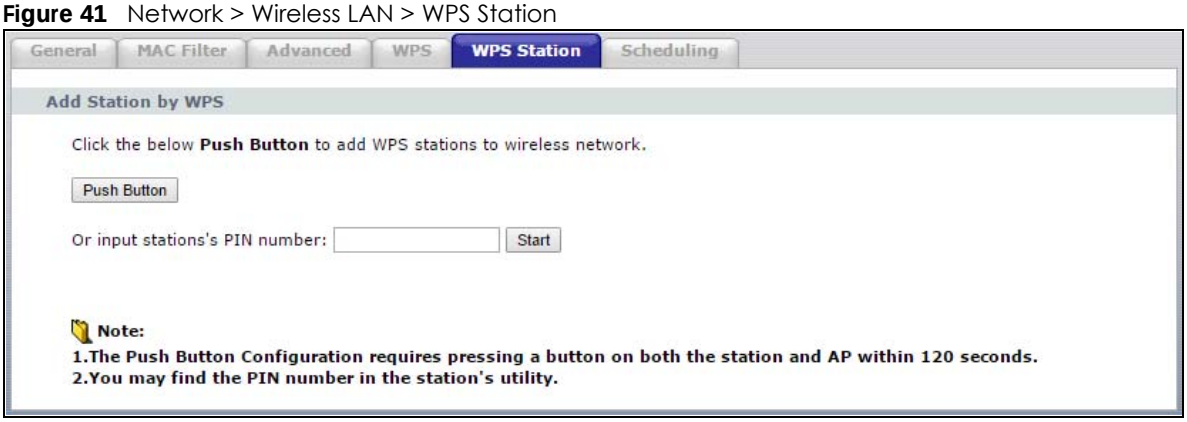
LABEL	DESCRIPTION
Status	This displays **Configured** when the WAP3205 v3 has connected to a wireless network using WPS or when **Enable WPS** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This 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.
802.11 Mode	This shows the wireless LAN's standard.
SSID	This shows the descriptive name used to identify the WAP3205 v3 in the wireless LAN.
Security	This shows the level of wireless security the WAP3205 v3 is using.
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 41 Network > Wireless LAN > WPS Station



The following table describes the labels in this screen.

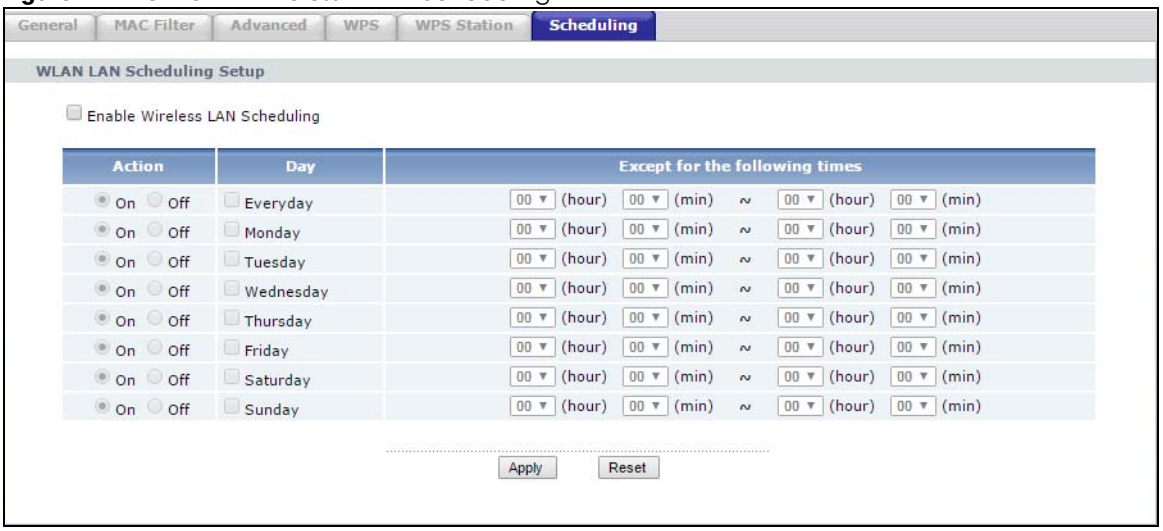
Table 27 Network > Wireless LAN > WPS Station

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 42 Network > Wireless LAN > Scheduling



The following table describes the labels in this screen.

Table 28 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.

Table 28 Network > Wireless LAN > Scheduling (continued)

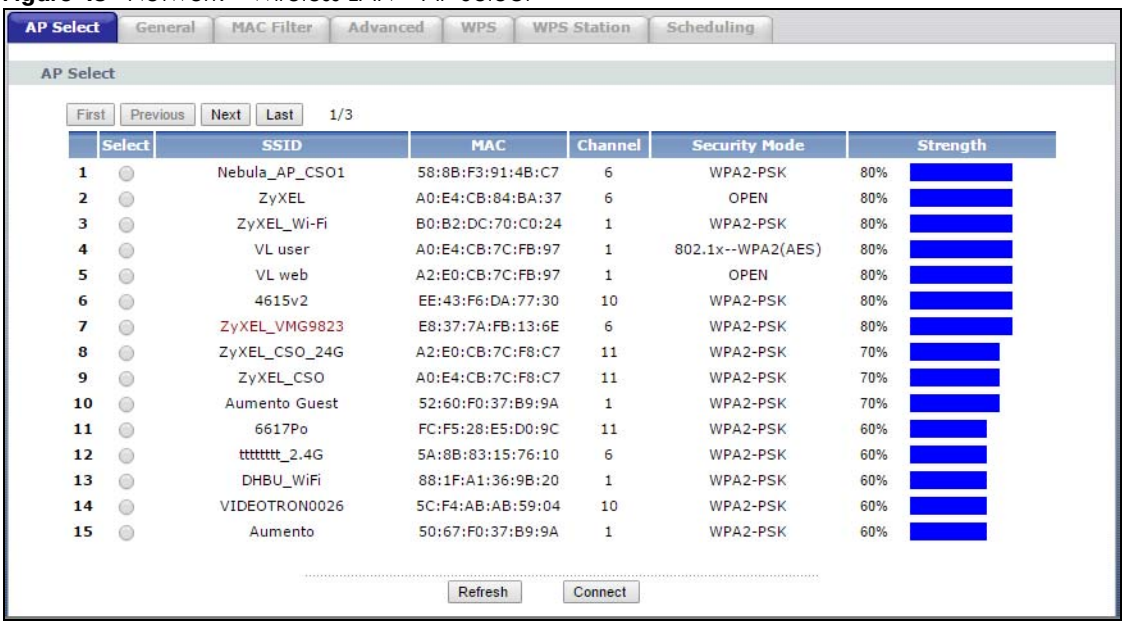
LABEL	DESCRIPTION
Except for the following times	Select a begin time using the first set of **hour** and minute (**min**) drop down boxes and select an end time using the second set of **hour** and minute (**min**) drop down boxes. If you have chosen **On** earlier for the WLAN Status the Wireless LAN 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 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 43 Network > Wireless LAN > AP Select



The following table describes the labels in this screen.

Table 29 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.

Table 29 Network > Wireless LAN > AP Select (continued)

LABEL	DESCRIPTION
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.
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.

6.11 WLAN Information Screen

Use this screen to view the SSID and security of the selected AP wireless network when the WAP3205 v3 is in client bridge mode. To open this screen, click **Network > AP Select > WLAN Info** tab.

Figure 44 Network > AP Select > WLAN Information

The following table describes the labels in this screen.

Table 30 Network > AP Select > WLAN Information

LABEL	DESCRIPTION
SSID	This displays the Service Set IDentity of the AP to which the WAP3205 v3 is connecting.
Security Mode	This displays the type of security configured on the AP to which the WAP3205 v3 is connecting.

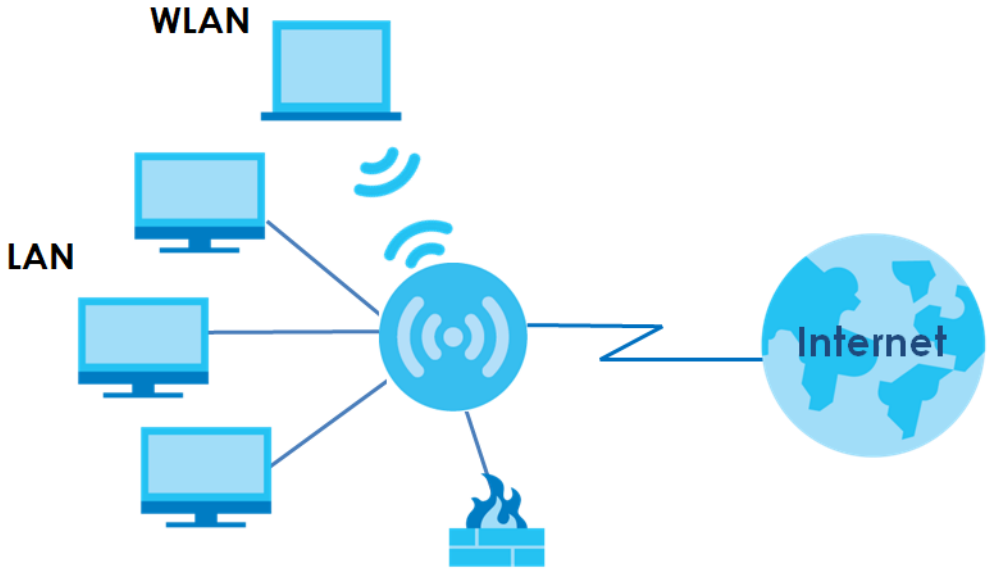
CHAPTER 7
LAN

7.1 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 45 LAN Setup

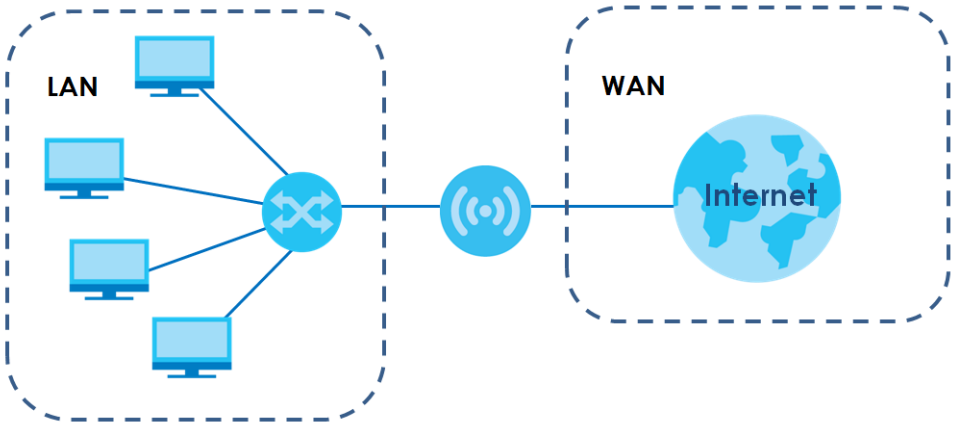


The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

7.2 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 46 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.

7.2.1 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.

7.2.2 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.

7.2.3 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.

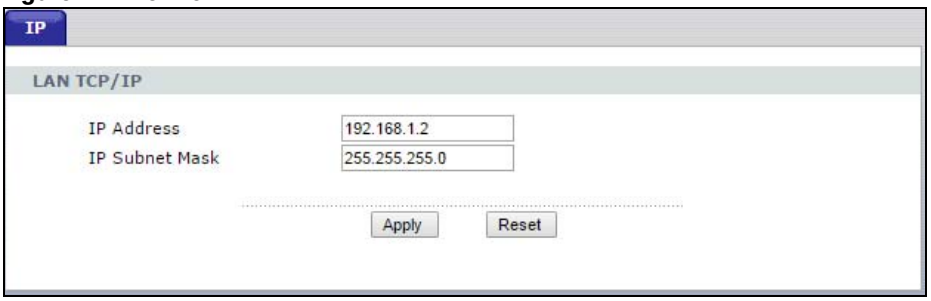
7.2.4 LAN TCP/IP

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

7.3 LAN IP Screen

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

Figure 47 Network > LAN > IP



The following table describes the labels in this screen.

Table 31 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 31 Network > LAN > IP (continued)

LABEL	DESCRIPTION
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your WAP3205 v3 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.

CHAPTER 8
System

8.1 Overview

This chapter provides information on the **System** screens.

See the chapter about wizard setup for more information on the next few screens.

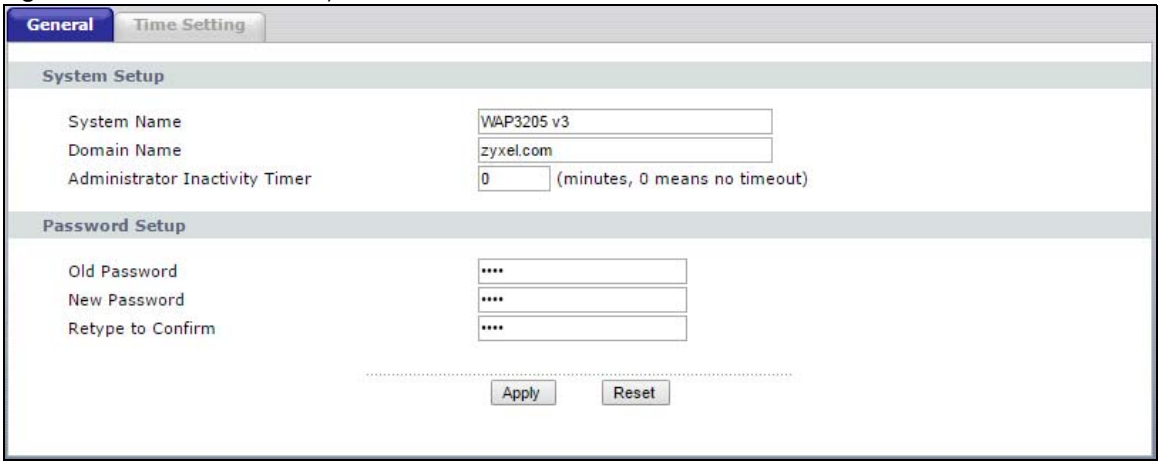
8.2 What You Can Do

- Use the **General** screen to enter a name to identify the WAP3205 v3 in the network and set the password (Section 8.3 on page 72).
- Use the **Time Setting** screen to change your WAP3205 v3's time and date (Section 8.4 on page 73).

8.3 System General Screen

Use this screen to enter a name to identify the WAP3205 v3 in the network and set the password. Click **Maintenance** > **System**. The following screen displays.

Figure 48 Maintenance > System > General



The following table describes the labels in this screen.

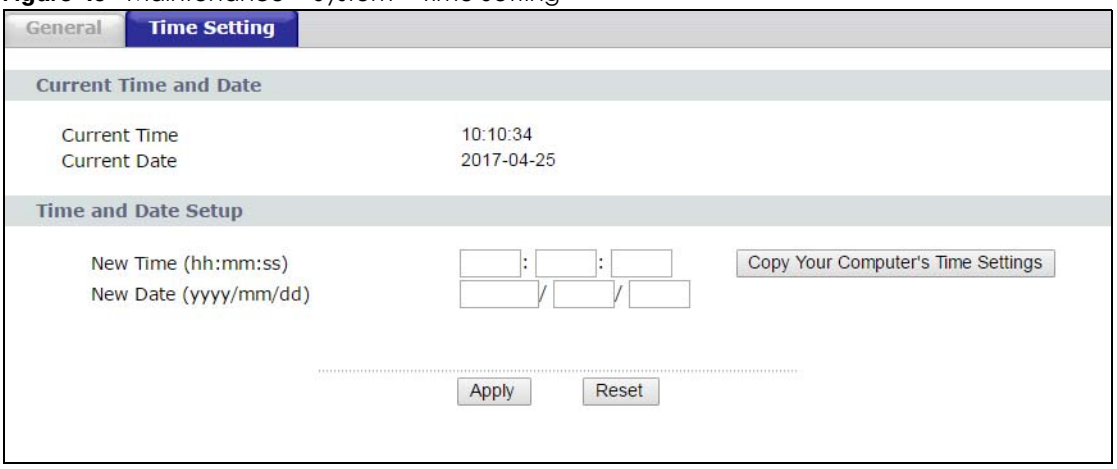
Table 32 Maintenance > System > General

LABEL	DESCRIPTION
System Setup	
System Name	**System Name** is a unique name to identify the WAP3205 v3 in an Ethernet network. It is recommended you enter your computer's "Computer name" in this field (see the chapter about wizard setup for how to find your computer's name). This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the **Domain name** (if you know it) here. This name is propagated to DHCP clients connected to interfaces with the DHCP server enabled.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Password Setup	Change your WAP3205 v3's password (recommended) using the fields as shown.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Apply	Click **Apply** to save your changes back to the WAP3205 v3.
Reset	Click **Reset** to begin configuring this screen afresh.

8.4 Time Setting Screen

To change your WAP3205 v3's time and date, click **Maintenance** > **System** > **Time Setting**. The screen appears as shown. Use this screen to configure the WAP3205 v3's time based on your local time zone.

Figure 49 Maintenance > System > Time Setting



The following table describes the labels in this screen.

Table 33 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your WAP3205 v3. Each time you reload this page, the WAP3205 v3 synchronizes the time with the time server.
Current Date	This field displays the date of your WAP3205 v3. Each time you reload this page, the WAP3205 v3 synchronizes the date with the time server.
Time and Date Setup	
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Copy Your Computer's Time Settings	Click the **Copy Your Computer's Time Settings** button to copy your computer's time settings into the WAP3205 v3's time and date setup.
Apply	Click **Apply** to save your changes back to the WAP3205 v3.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 9
Logs

9.1 Overview

This chapter contains information about configuring general log settings and viewing the WAP3205 v3's logs.

The Web Configurator allows you to look at all of the WAP3205 v3's logs in one location.

9.2 What You Need to Know

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full (see **Log Schedule**). Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

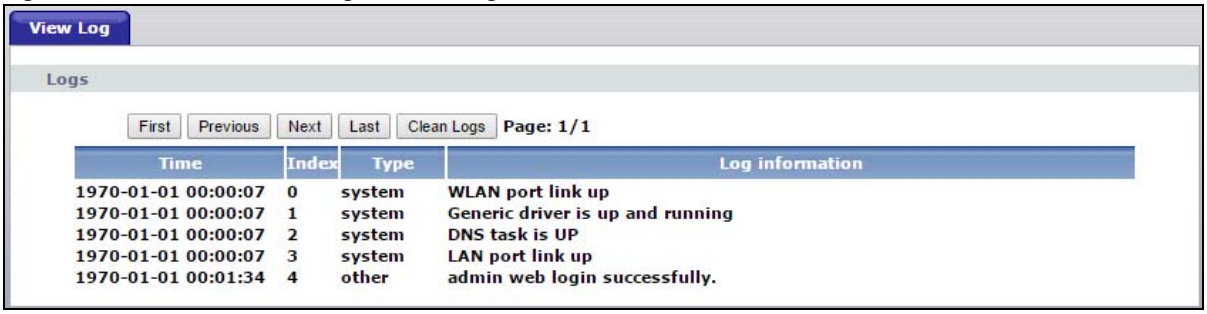
9.3 View Log Screen

Use the **View Log** screen to see the logged messages for the WAP3205 v3. Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, Java and cookies), attacks (such as DoS) and IPSec.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Click **Maintenance** > **Logs** to open the **View Log** screen.

Figure 50 Maintenance > Logs > View Log



The following table describes the labels in this screen.

Table 34 Maintenance > Logs > View Log

LABEL	DESCRIPTION
First	Click **First** button to see the first page of the log.
Previous	Click **Previous** button to go back one page from your current log page.
Next	Click **Next** button to go to the following page from your current log page.
Last	Click **Last** button to go to the last page of the log.
Clear Logs	Click **Clear Logs** to delete all the logs.
Time	This field displays the time the log was recorded.
Index	This is the index number of the log.
Type	This field displays the type of the log.
Log information	This field states the reason for the log.

CHAPTER 10
Tools

10.1 Overview

This chapter shows you how to upload a new firmware, upload or save backup configuration files and restart the WAP3205 v3.

10.2 What You Can Do

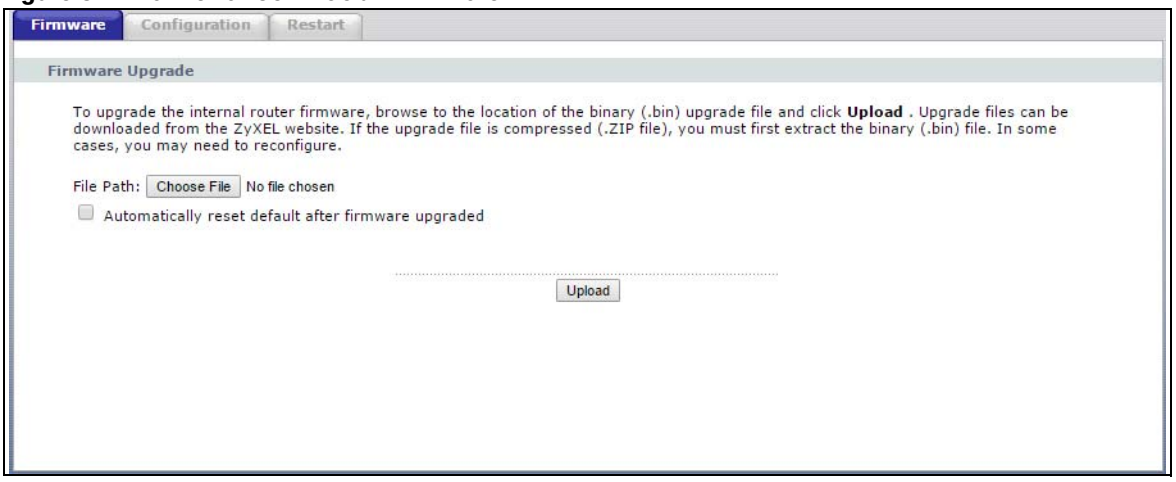
- Use the **Firmware** screen to upload firmware to your WAP3205 v3 (Section 10.3 on page 77).
- Use the **Configuration** screen to view information related to factory defaults, backup configuration, and restoring configuration (Section 10.4 on page 79).
- Use the **Restart** screen to have the WAP3205 v3 reboot (Section 10.5 on page 81).

10.3 Firmware Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "WAP3205 v3.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **Maintenance > Tools**. Follow the instructions in this screen to upload firmware to your WAP3205 v3.

Figure 51 Maintenance > Tools > Firmware



The following table describes the labels in this screen.

Table 35 Maintenance > Tools > Firmware

LABEL	DESCRIPTION
Choose File	Click **Choose File** button to find the.bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Automatically reset default after firmware upgraded	Click the **Automatically reset default after firmware upgraded** check box to have the WAP3205 v3 automatically reset itself after the new firmware is uploaded.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.
Check for Latest Firmware Now	Click **Check for Latest Firmware Now** button to have the WAP3205 v3 search for the latest firmware available online at Zyxel's website.

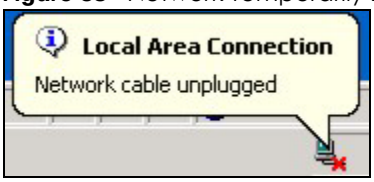
Note: Do not turn off the WAP3205 v3 while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait for several minutes before logging into the WAP3205 v3 again.

Figure 52 Upload Warning

The WAP3205 v3 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 53 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **Status** screen.

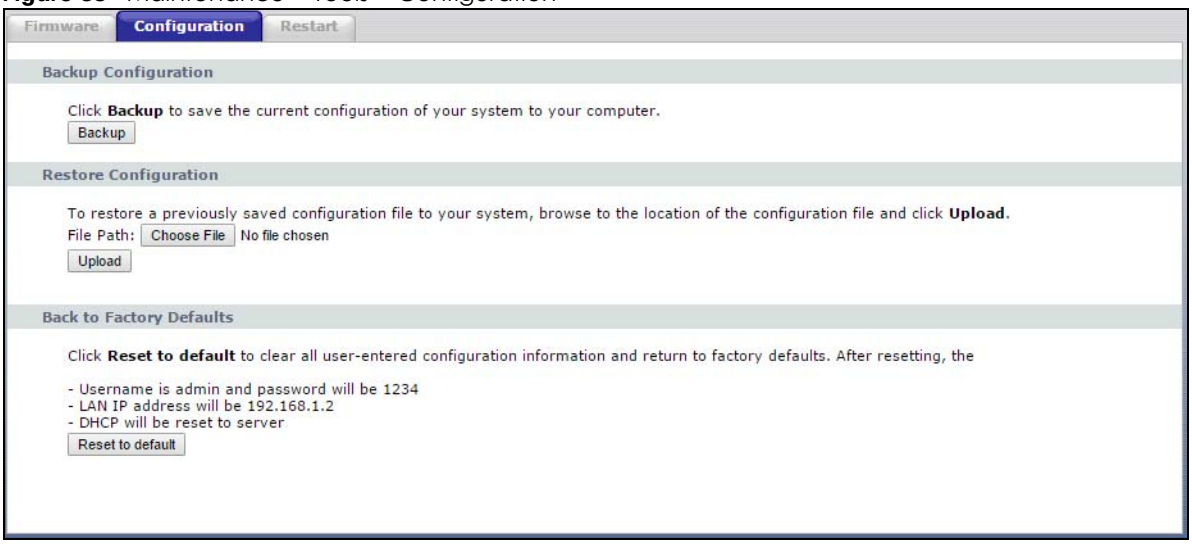
If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Firmware** screen.

Figure 54 Upload Error Message

10.4 Configuration Screen

Click **Maintenance > Tools** > **Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 55 Maintenance > Tools > Configuration



10.4.1 Backup Configuration

Backup configuration allows you to back up (save) the WAP3205 v3's current configuration to a file on your computer. Once your WAP3205 v3 is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the WAP3205 v3's current configuration to your computer.

10.4.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your WAP3205 v3.

Table 36 Maintenance Restore Configuration

LABEL	DESCRIPTION
Choose File	Click **Choose File** button to find the backup file of previous configuration you saved on your computer using the **Backup** button.
Upload	Click **Upload** to begin the upload process.

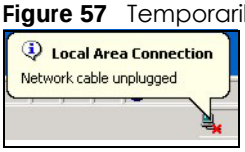
Note: Do not turn off the WAP3205 v3 while configuration file upload is in progress.

After you see a "configuration upload successful" screen, you must then wait one minute before logging into the WAP3205 v3 again.

Figure 56 Configuration Restore Successful

The WAP3205 v3 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 57 Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default WAP3205 v3 IP address (192.168.1.2). See Section 2.2 on page 14 for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

Figure 58 Configuration Restore Error

10.4.3 Back to Factory Defaults

Pressing the **Reset to default** button in this section clears all user-entered configuration information and returns the WAP3205 v3 to its factory defaults.

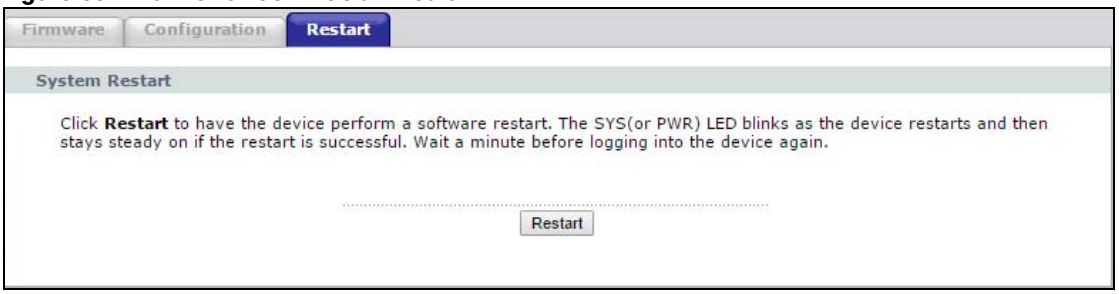
You can also press the **WPS/RESET** button on the rear panel to reset the factory defaults of your WAP3205 v3. Refer to Section 1.4.1 on page 12 for more information on the **WPS/RESET** button.

10.5 Restart Screen

System restart allows you to reboot the WAP3205 v3 without turning the power off.

Click **Maintenance > Tools** > **Restart**. Click **Restart** to have the WAP3205 v3 reboot. This does not affect the WAP3205 v3's configuration.

Figure 59 Maintenance > Tools > Restart



CHAPTER 11
Language

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 60 Language

Figure 61 Language Change Example

CHAPTER 12
Operation Mode

12.1 Overview

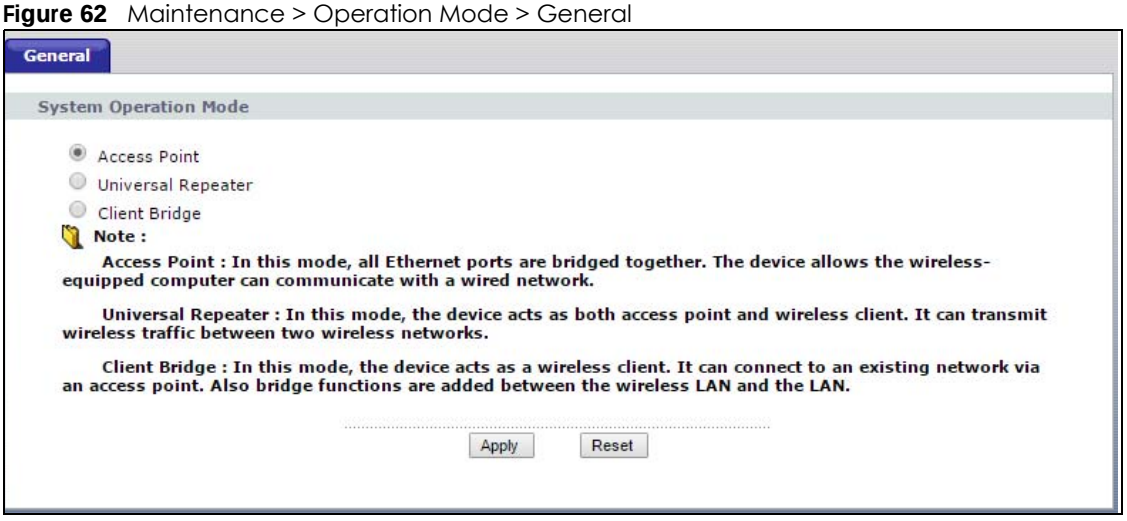
The **Operation Mode** (System Operation Mode) function lets you configure select the device operation mode: **Access Point**, **Universal Repeater**, or **Client Bridge**.

See Chapter 4 on page 33 for more information on which mode to choose.

12.2 General Screen

Use this screen to select how you connect to the Internet.

Figure 62 Maintenance > Operation Mode > General



The following table describes the labels in the **General** screen.

Table 37 Maintenance > Operation Mode > General

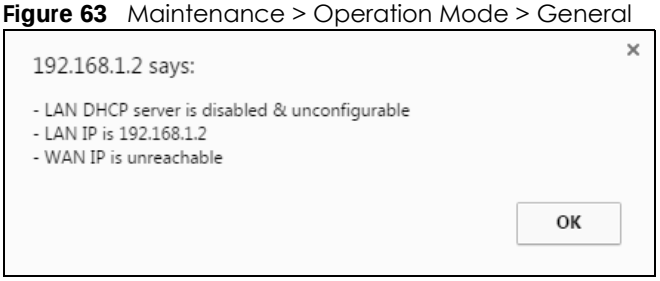
LABEL	DESCRIPTION
System Operation Mode	
Access Point	Use **Access Point** mode if you already have a Router (R) in your network and you want to bridge all wired and wireless network connections.
Universal Repeater	Use **Universal Repeater** mode if there is an existing wireless router or access point in your network and you want the WAP3205 v3 to wirelessly relay communications from its wireless clients to it.
Client Bridge	Use **Client Bridge** mode if your device needs a wireless client to connect to an existing access point.

Table 37 Maintenance > Operation Mode > General (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your settings.
Reset	Click **Reset** to return to the previous screen settings.

If you select a mode (**Access Point**, **Universal Repeater** or **Client Bridge**) the following pop-up message window appears.

Figure 63 Maintenance > Operation Mode > General



- All Ethernet ports have the same IP address.
- All ports on the rear panel of the device are LAN ports. There is no WAN port.
- The DHCP server on your device is disabled. In this mode there must be a device with a DHCP server on your network such as a router which can allocate IP addresses or else you need to manually assign IP addresses to devices on your network.
- The LAN IP address of the WAP3205 v3 is set to 192.168.1.2.

CHAPTER 13
Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

13.1 Power, Hardware Connections, and LEDs

The WAP3205 v3 does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the WAP3205 v3.
2. Make sure the power adaptor or cord is connected to the WAP3205 v3 and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or cord to the WAP3205 v3.
4. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.3 on page 11.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Disconnect and re-connect the power adaptor to the WAP3205 v3.
5. If the problem continues, contact the vendor.

13.2 WAP3205 v3 Access and Login

I don't know the IP address of my WAP3205 v3.

1 The default IP address is **192.168.1.2**

2 If you changed the IP address and have forgotten it, you might need to reset your WAP3205 v3 to change all settings back to their default. This means your current settings are lost. See Section 13.4 on page 88 in the **Troubleshooting** for information on resetting your WAP3205 v3.The default IP address is **192.168.1.2**.

I forgot the username and password.

1 The default username is **admin** and default password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 13.4 on page 88.

I cannot see or access the **Login** screen in the Web Configurator.

1 Make sure you are using the correct IP address.
- The default IP address is 192.168.1.2.
- If you changed the IP address, use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I don't know the IP address of my WAP3205 v3.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See Appendix B on page 99.

4 Make sure your computer is in the same subnet as the WAP3205 v3. (If you know that there are routers between your computer and the WAP3205 v3, skip this step.)
- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address.
- If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the WAP3205 v3.

5 Reset the device to its factory defaults, and try to access the WAP3205 v3 with the default IP address.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- If your computer is connected wirelessly, use a computer that is connected to a **LAN/ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the WAP3205 v3.

1. Make sure you have entered the password correctly. The default username is **admin** and default password is **1234**. This field is case-sensitive, so make sure [Caps Lock] is not on.
2. This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.
3. Disconnect and re-connect the power adaptor or cord to the WAP3205 v3.
4. If this does not work, you have to reset the device to its factory defaults. See Section 13.4 on page 88.

13.3 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
2. If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
3. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
4. Go to **Maintenance > Operation Mode > General**. Check your **System Operation Mode** setting.
5. Check your computer's IP is set to automatic, if your computer has Static IP change it back to automatic to access the Internet. For more information on how to change your computer's IP address see Section 2.2 on page 14.
6. If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the WAP3205 v3), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.3 on page 11.
2. Reboot the WAP3205 v3.
3. If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.3 on page 11. If the WAP3205 v3 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2. Check the signal strength. If the signal strength is low, try moving the WAP3205 v3 closer to the AP if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
3. Reboot the WAP3205 v3.
4. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

13.4 Resetting the WAP3205 v3 to Its Factory Defaults

If you reset the WAP3205 v3, you lose all of the changes you have made. The WAP3205 v3 re-loads its default settings, and the username/password resets to **admin**/**1234**. You have to make all of your changes again.

You will lose all of your changes when you push the **WPS/RESET** button.

To reset the WAP3205 v3,

1. Make sure the power LED is on.
2. Press the **WPS/RESET** button for longer than 10 second to reboot and restore factory-default configurations on the WAP3205 v3.

   If the WAP3205 v3 restarts automatically, wait for the WAP3205 v3 to finish restarting, and log in to the Web Configurator. The username is **admin** and password is **1234**.

   If the WAP3205 v3 does not restart automatically, disconnect and reconnect the WAP3205 v3's power. Then, follow the directions above again.

13.5 Wireless Problems

I cannot access the WAP3205 v3 or ping any computer from the WLAN.

1. Make sure the wireless LAN is enabled on the WAP3205 v3.
2. Make sure the wireless adapter on the wireless station is working properly.
3. Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the WAP3205 v3.
4. Make sure your computer (with a wireless adapter installed) is within the transmission range of the WAP3205 v3.
5. Check that both the WAP3205 v3 and your wireless station are using the same wireless and wireless security settings.
6. Make sure traffic between the WLAN and the LAN is not blocked by the firewall on the WAP3205 v3.
7. Make sure you allow the WAP3205 v3 to be remotely accessed through the WLAN interface. Check your remote management settings.
   - See Chapter 6 Wireless LAN for more information.

APPENDIX A
IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

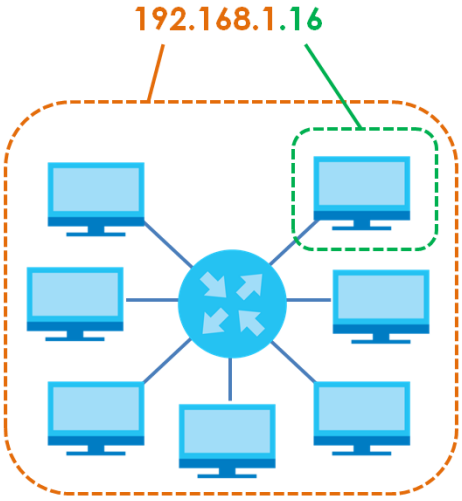
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 64 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 38 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 39 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 40 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} - 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 41 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

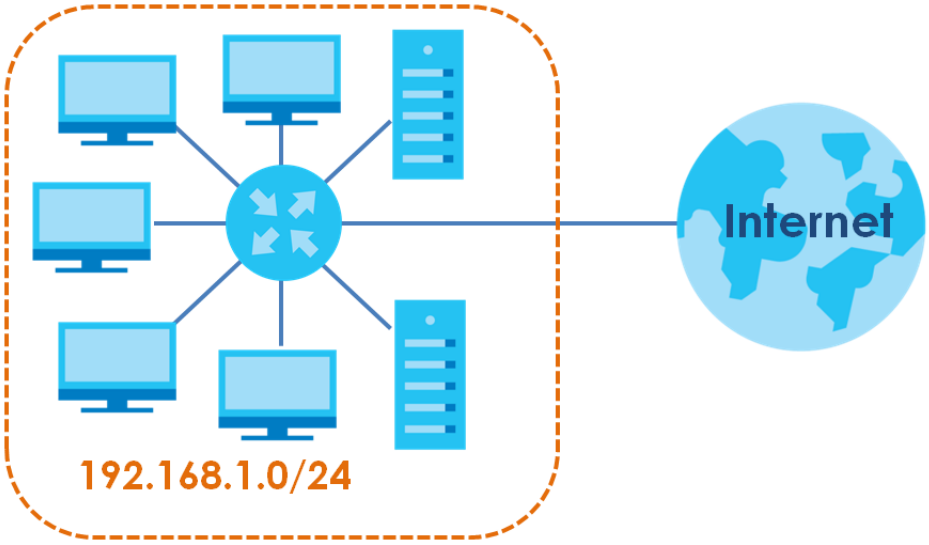
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of 2^{8} – 2 or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 65 Subnetting Example: Before Subnetting

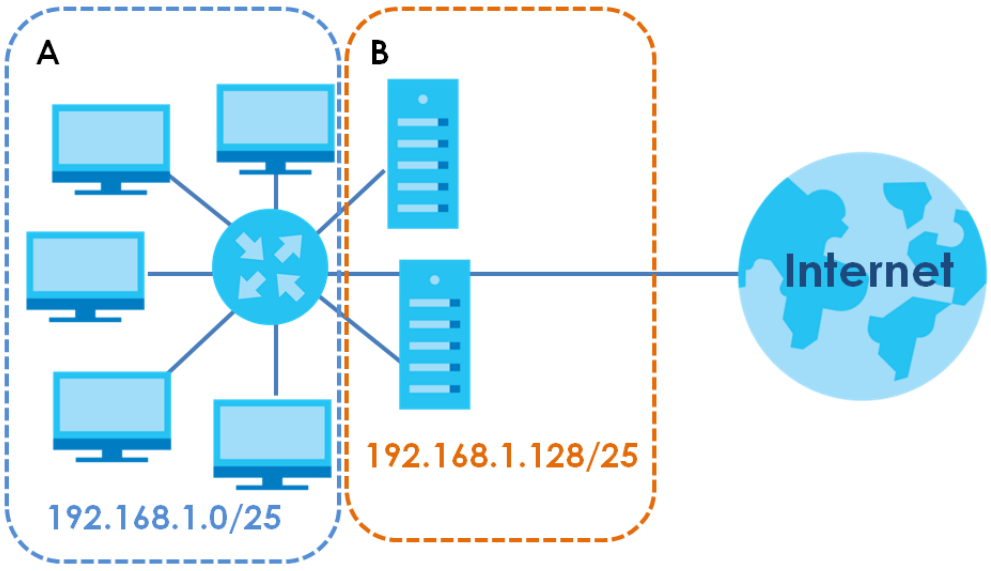


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The "borrowed" host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 66 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 42 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 43 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 44 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 45 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000

Table 45 Subnet 4 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 46 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 47 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 48 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190

Table 48 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

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. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. 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. You must also enable Network Address Translation (NAT) on the WAP3205 v3.

Once you have decided on the network number, pick an IP address for your WAP3205 v3 that is easy to remember (for instance, 192.168.1.1) 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.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet Access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

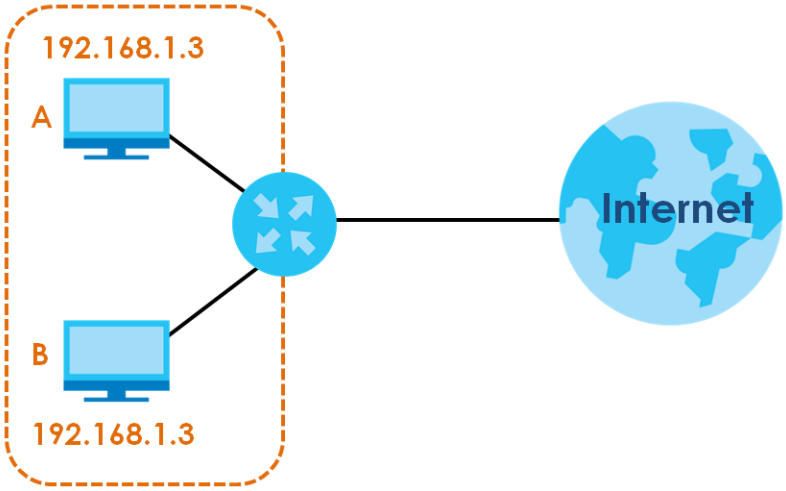
IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

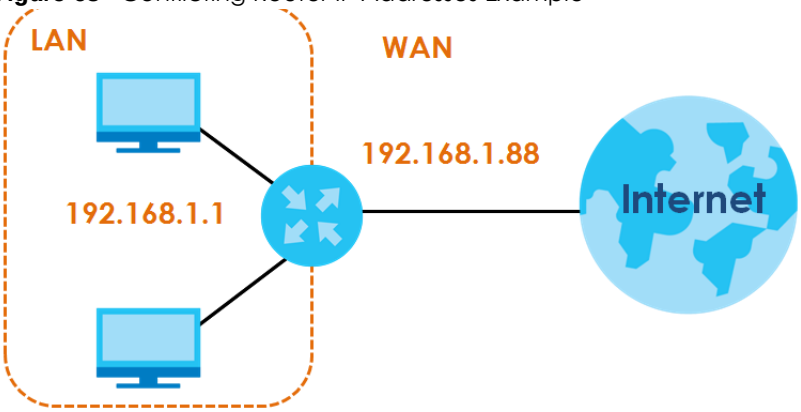
Figure 67 Conflicting Computer IP Addresses Example



Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

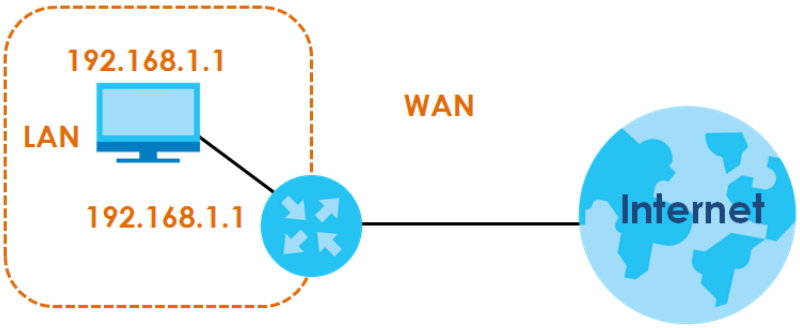
Figure 68 Conflicting Router IP Addresses Example



Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 69 Conflicting Computer and Router IP Addresses Example



APPENDIX B
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

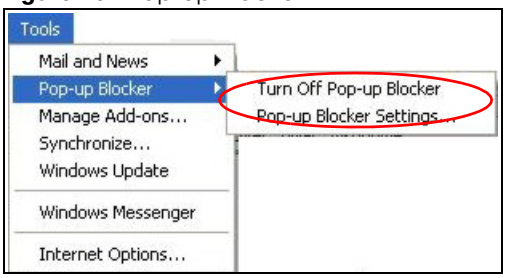
You may have to disable pop-up blocking to log into your device.

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 70 Pop-up Blocker

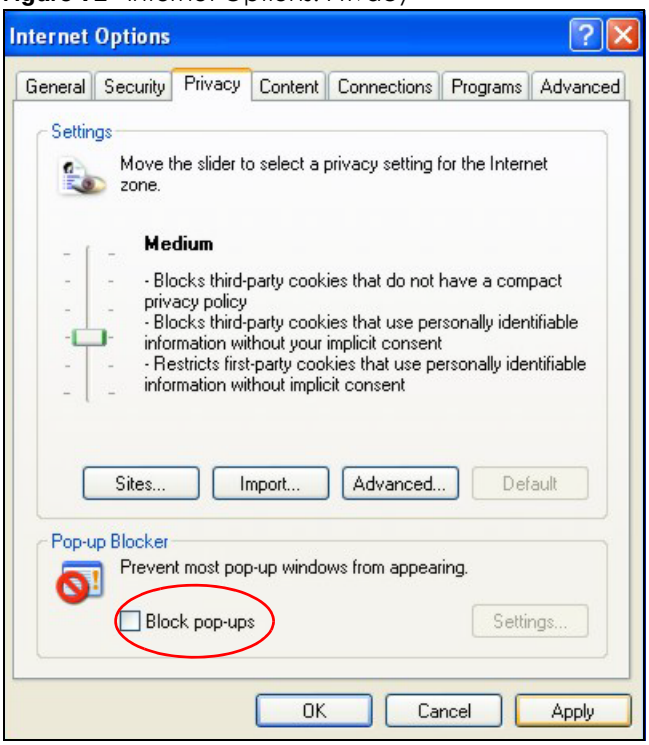


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

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 71 Internet Options: Privacy



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

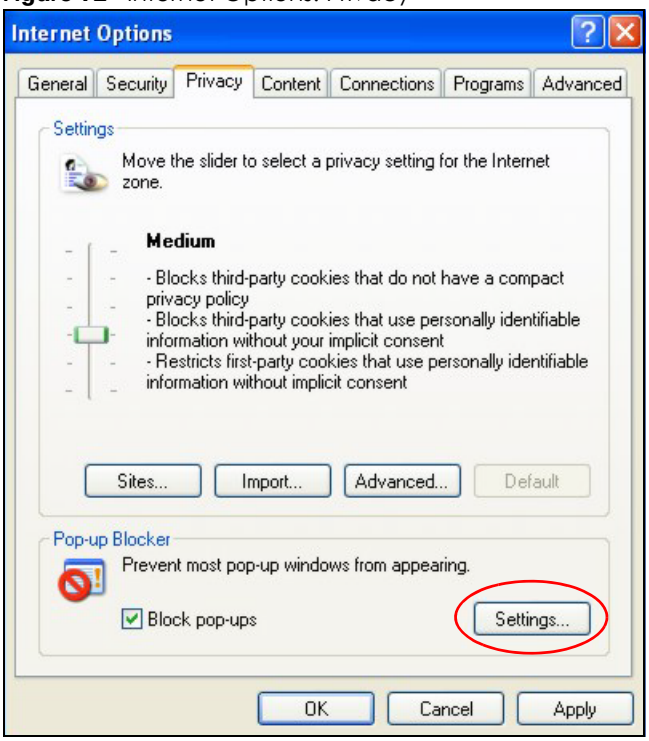
Enable Pop-up Blockers with Exceptions

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.

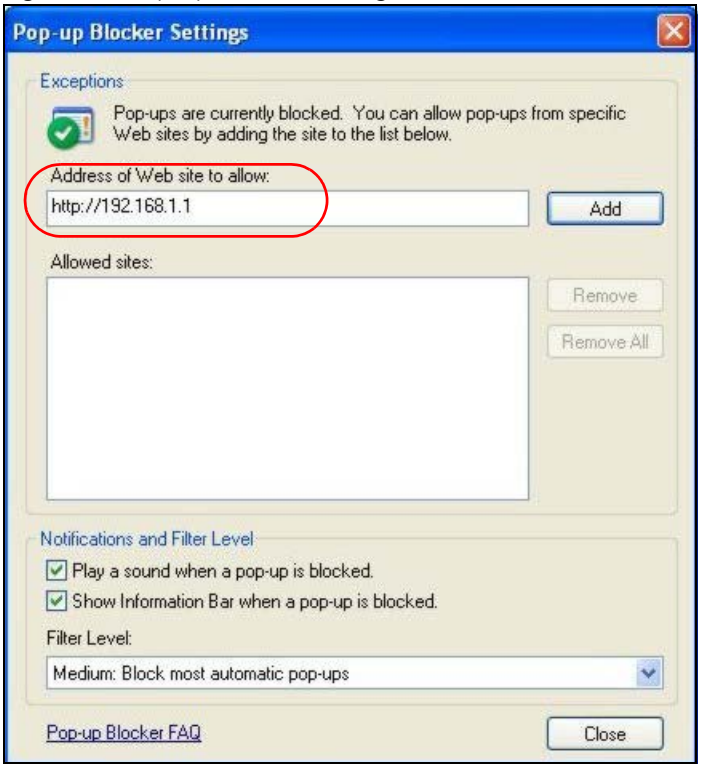
Figure 72 Internet Options: Privacy



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 73 Pop-up Blocker Settings



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

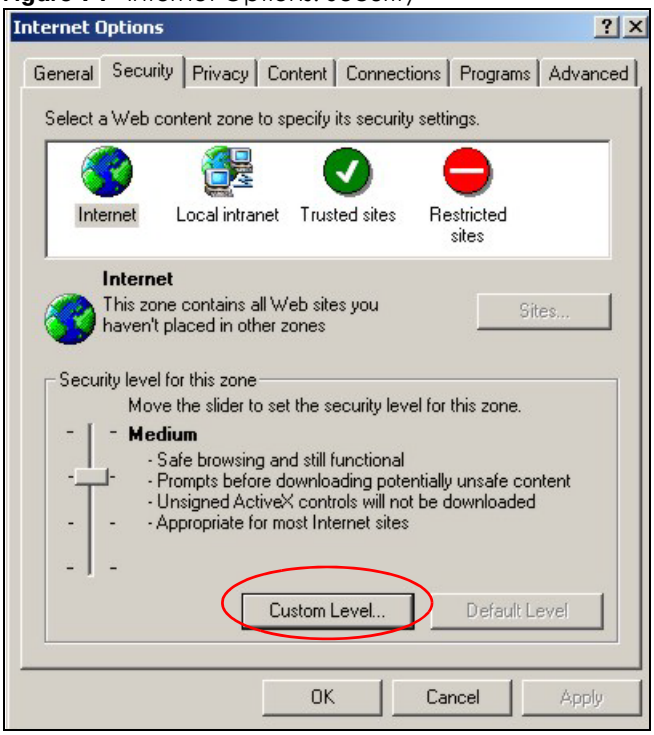
6 Click **Apply** to save this setting.

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 74 Internet Options: Security



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

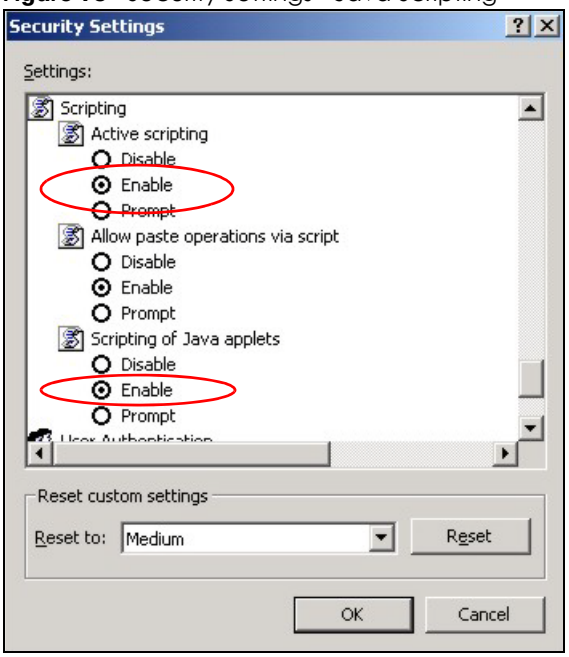
3 Scroll down to **Scripting**.

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 75 Security Settings - Java Scripting



Java Permissions

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

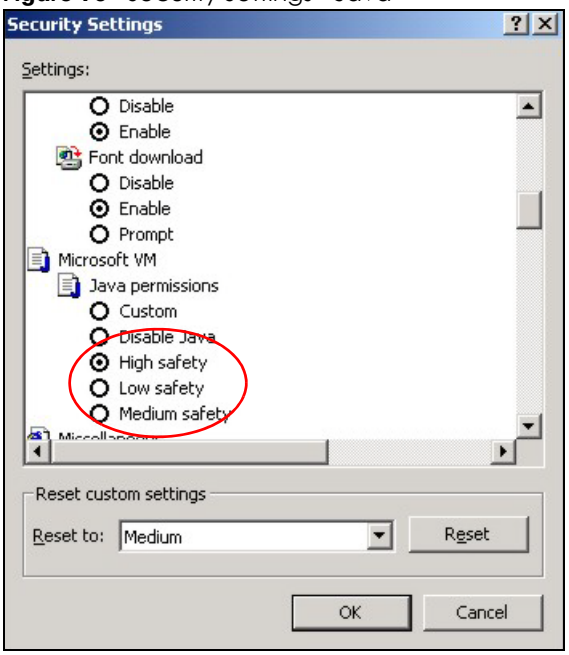
2 Click the **Custom Level...** button.

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 76 Security Settings - Java



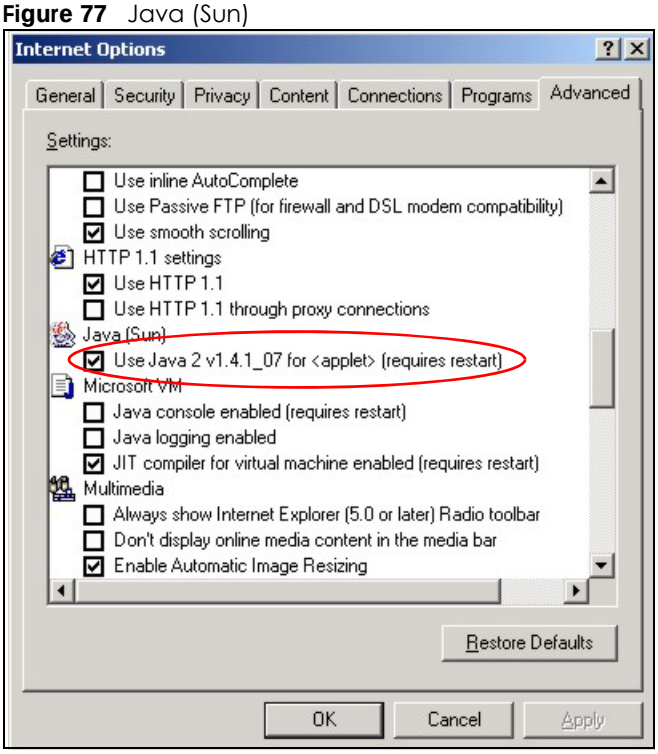
JAVA (Sun)

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 77 Java (Sun)

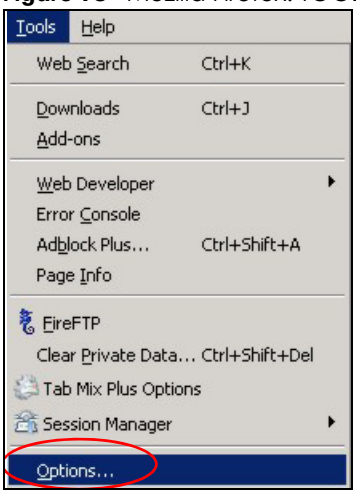


Mozilla Firefox

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.

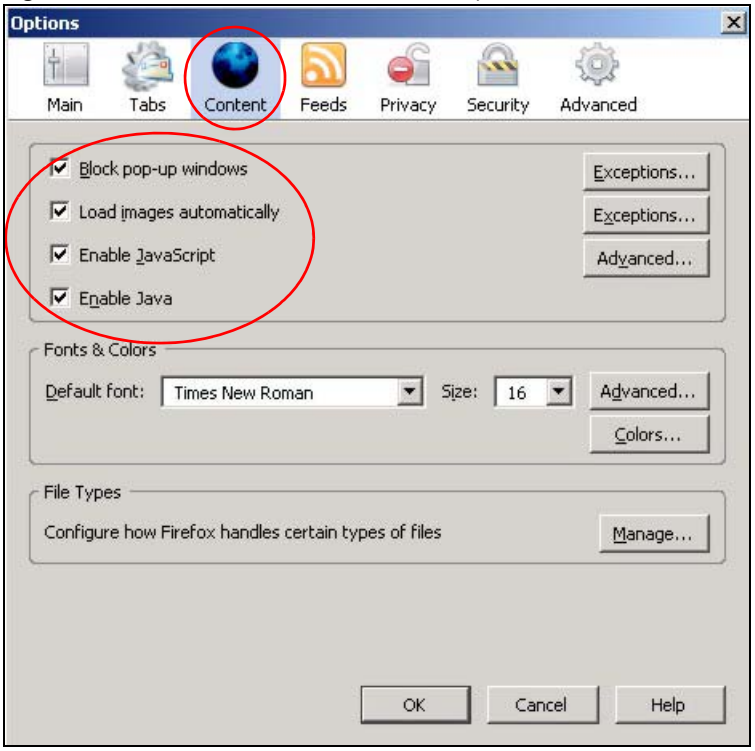
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 78 Mozilla Firefox: TOOLS > Options



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

Figure 79 Mozilla Firefox Content Security



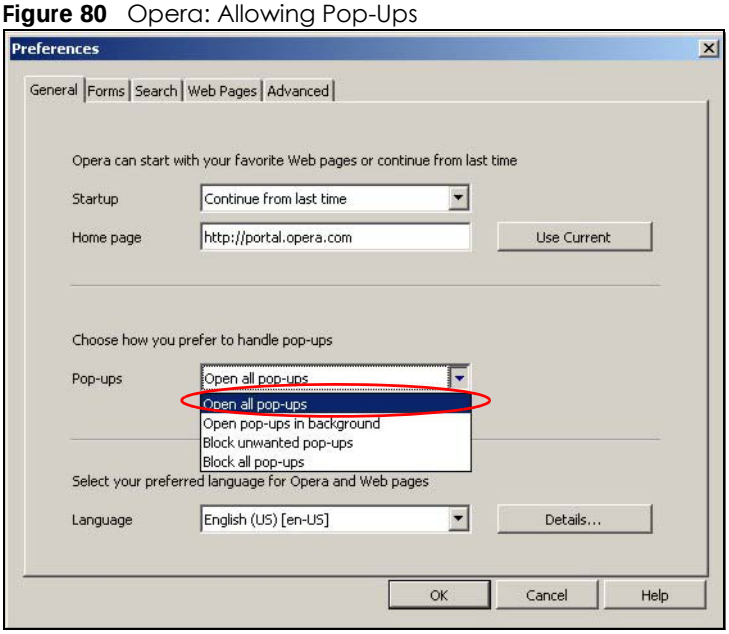
Opera

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**.

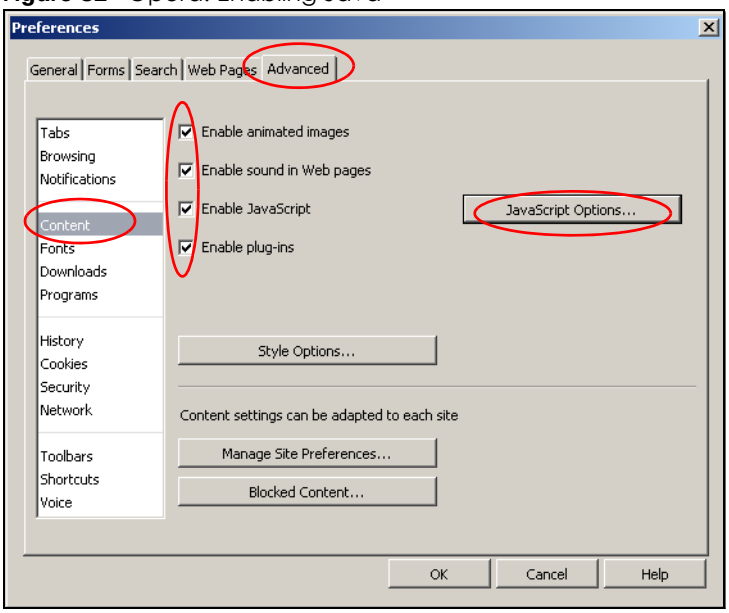
Figure 80 Opera: Allowing Pop-Ups



Enabling Java

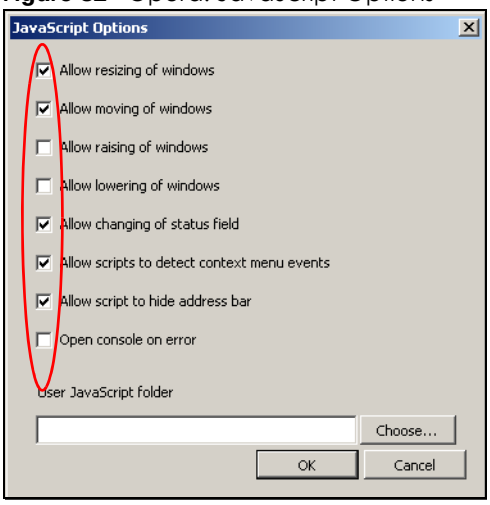
From Opera, click **Tools**, then **Preferences**. In the **Advanced** tab, select **Content** from the left-side menu. Select the check boxes as shown in the following screen.

Figure 81 Opera: Enabling Java



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

Figure 82 Opera: JavaScript Options



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

APPENDIX C
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.

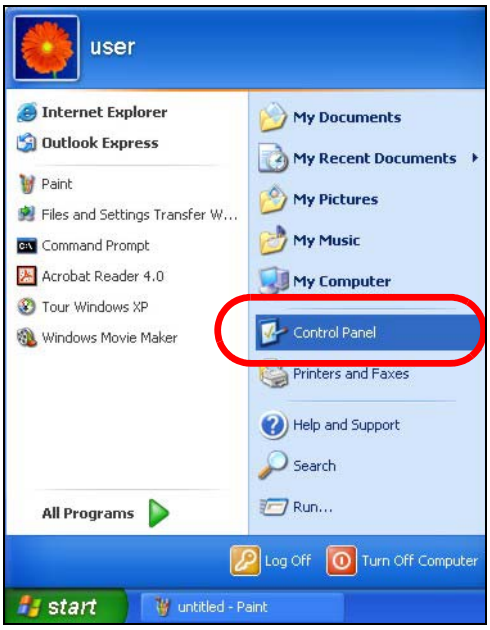
If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

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

Windows XP/NT/2000

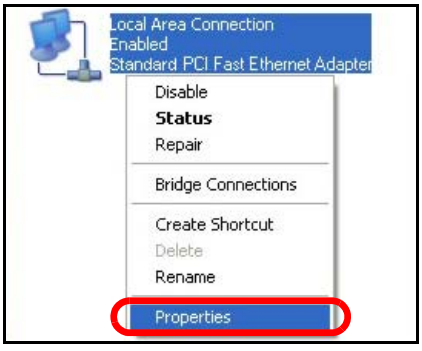
The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

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

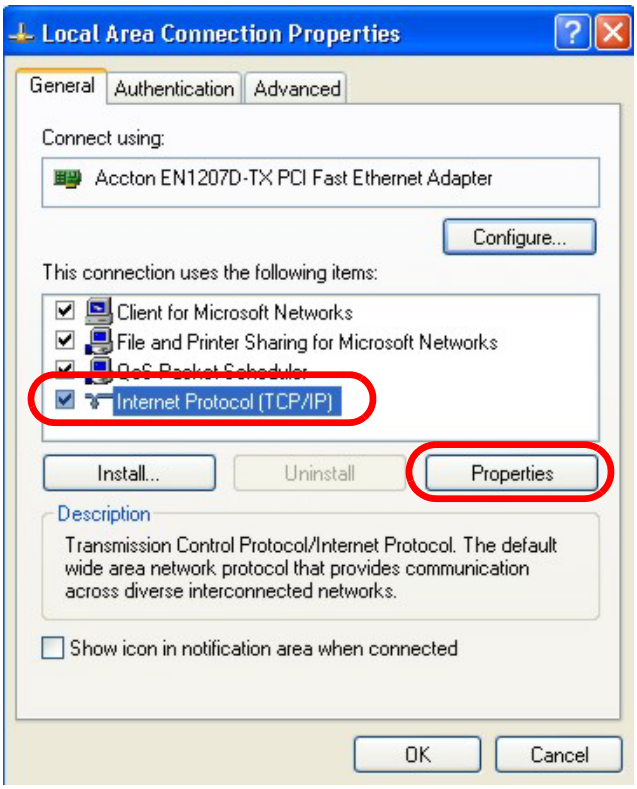


2 In the **Control Panel**, click the **Network Connections** icon.

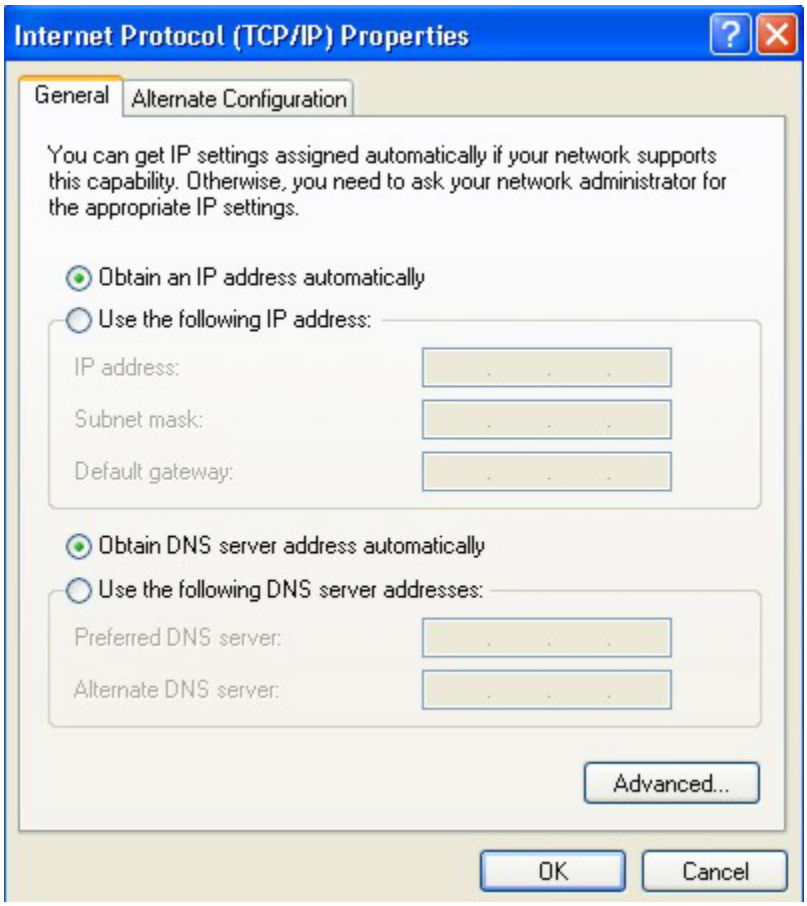
3 Right-click **Local Area Connection** and then select **Properties**.



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



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



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**.

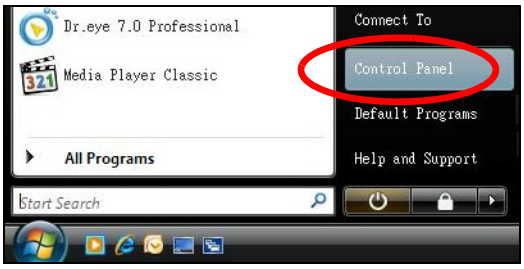
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

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.

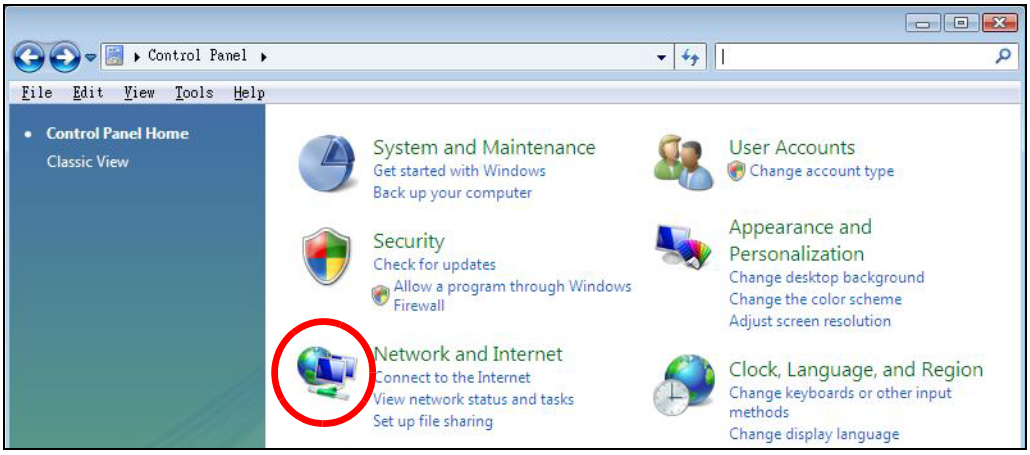
Windows Vista

This section shows screens from Windows Vista Professional.

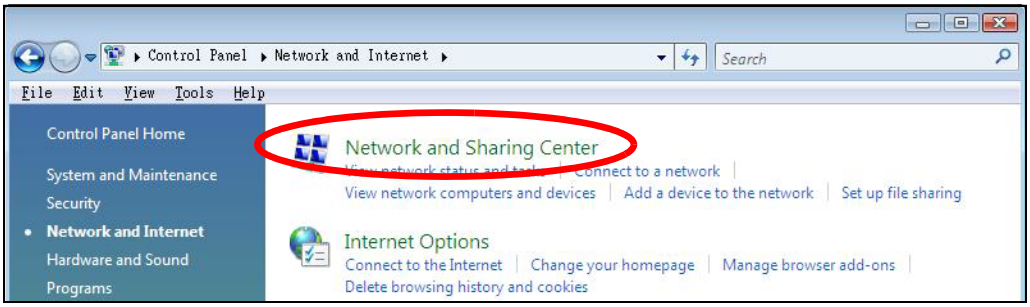
1 Click **Start** > **Control Panel**.



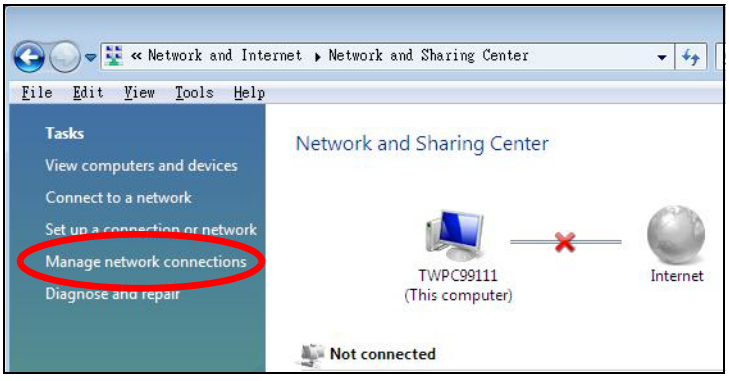
2 In the **Control Panel**, click the **Network and Internet** icon.



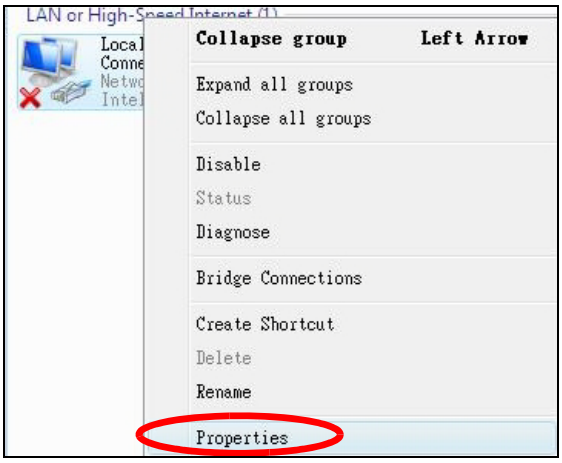
3 Click the **Network and Sharing Center** icon.



4 Click **Manage network connections**.

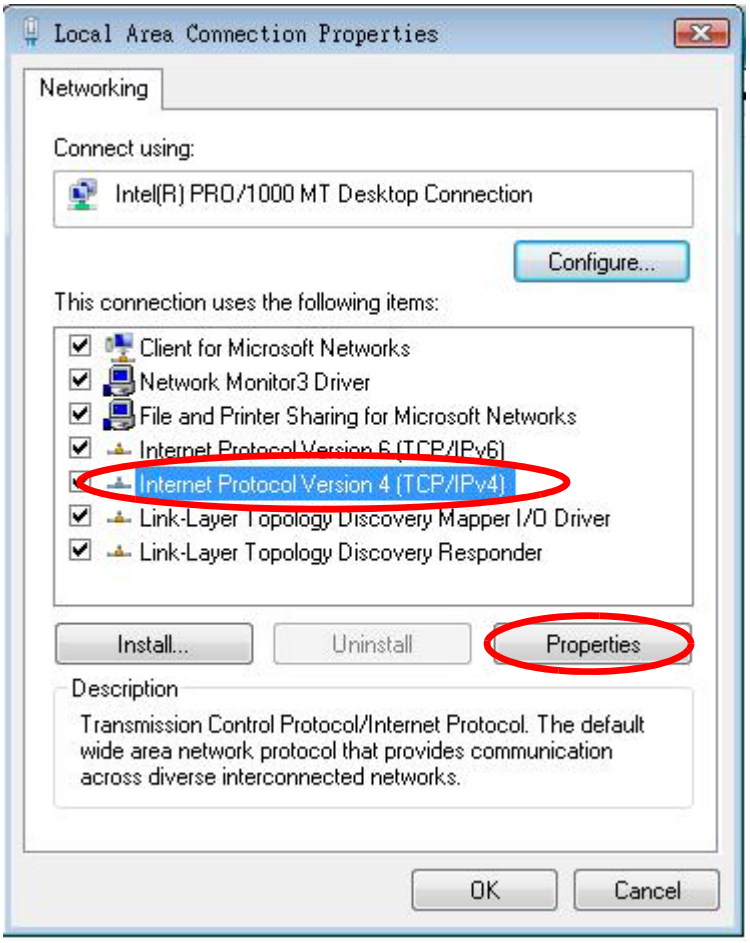


5 Right-click **Local Area Connection** and then select **Properties**.

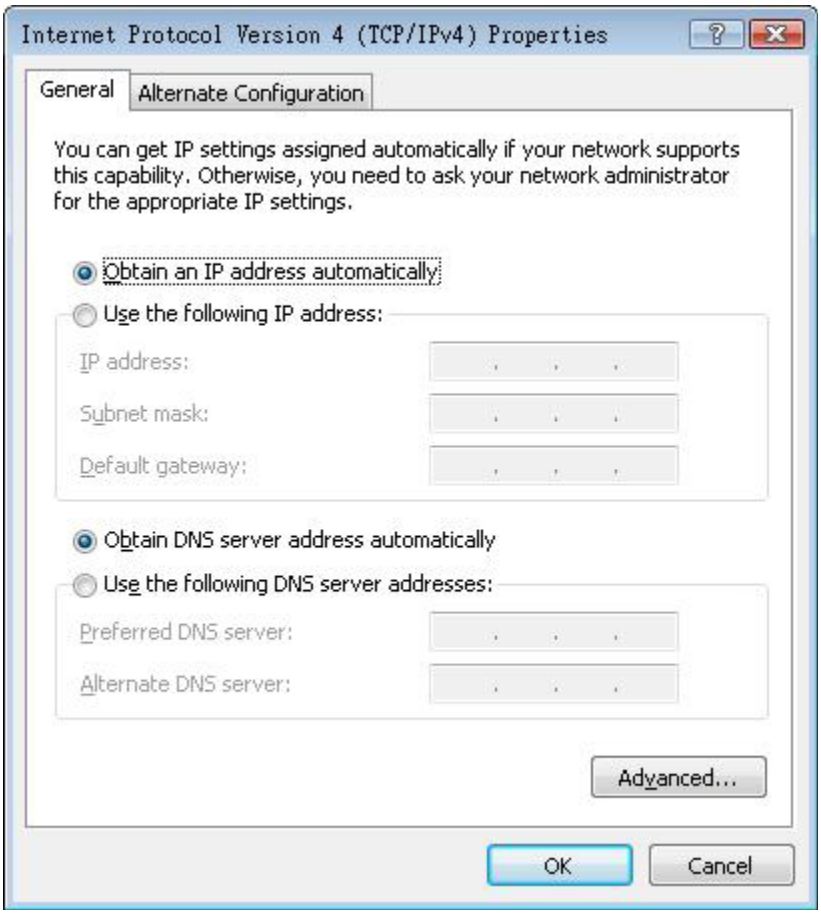


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

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



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



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**.

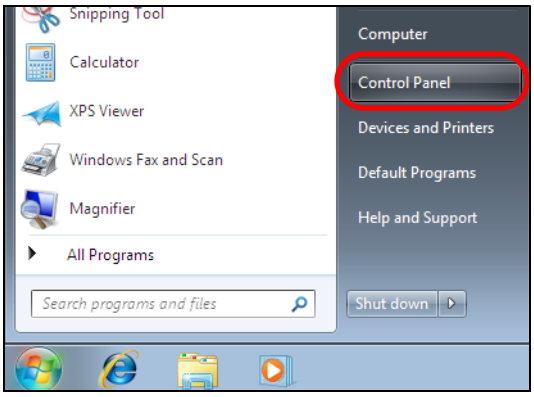
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

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.

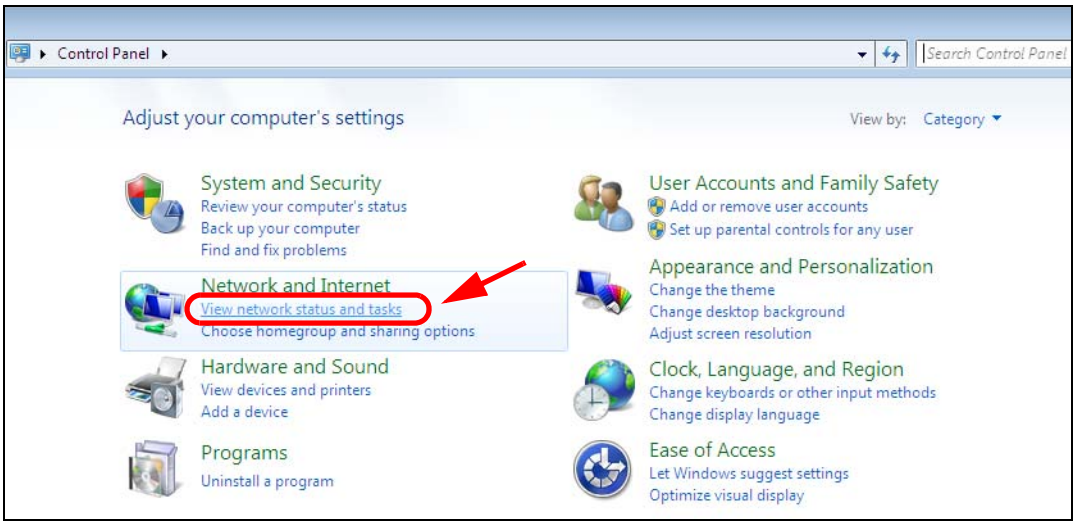
Windows 7

This section shows screens from Windows 7 Enterprise.

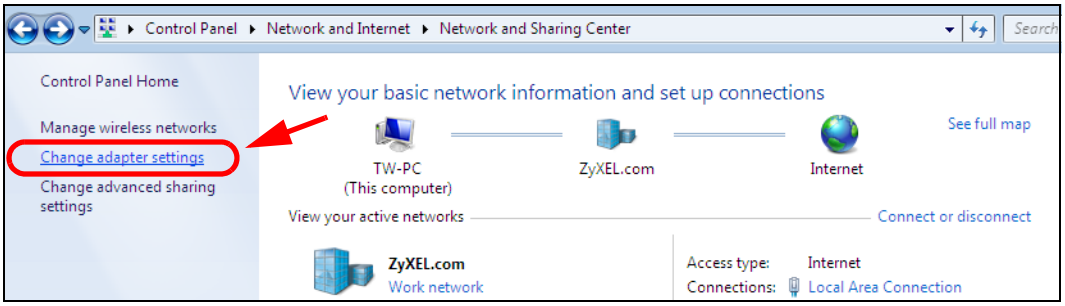
1 Click **Start** > **Control Panel**.



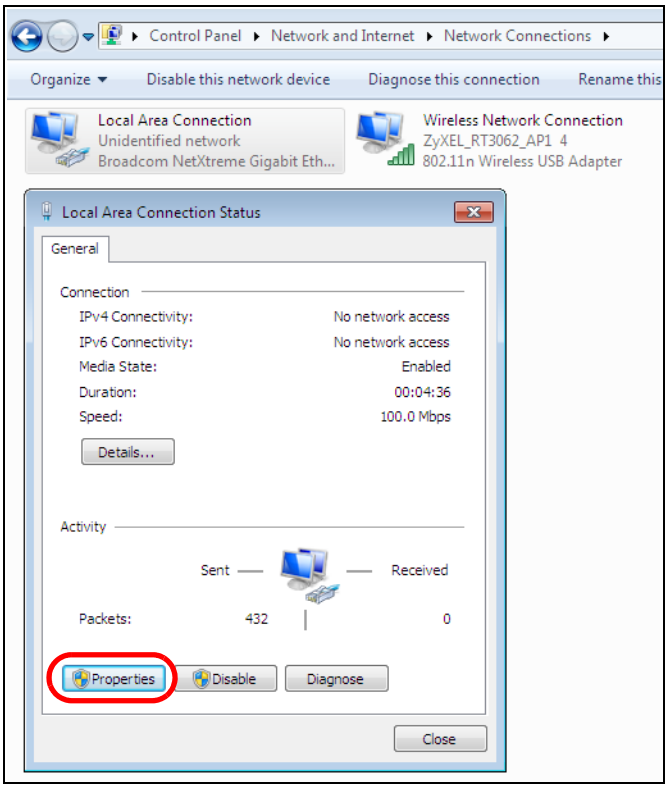
2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.



3 Click **Change adapter settings**.

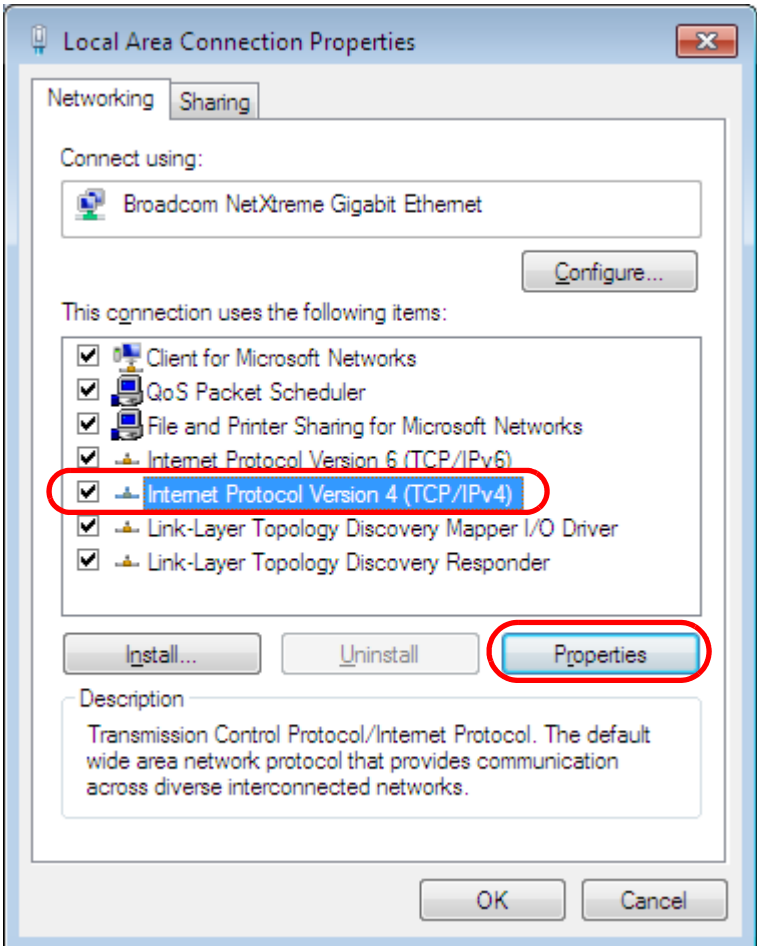


4 Double click **Local Area Connection** and then select **Properties**.

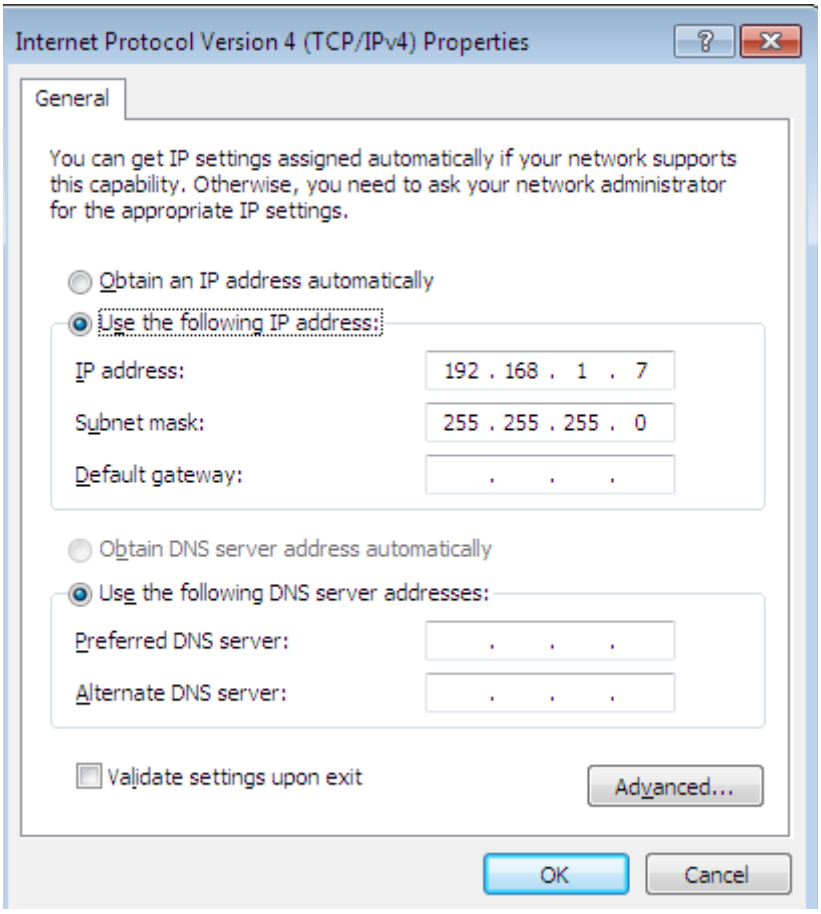


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

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



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



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.

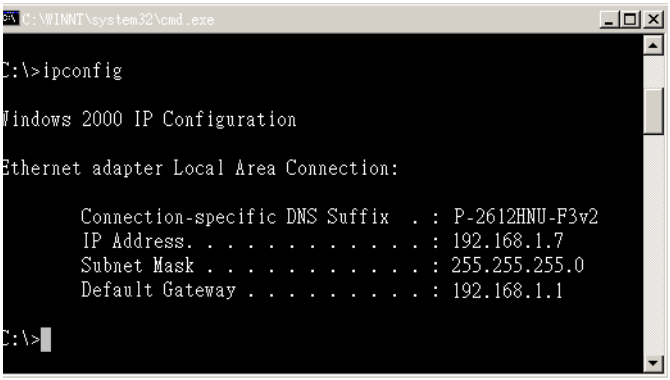
9 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

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

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

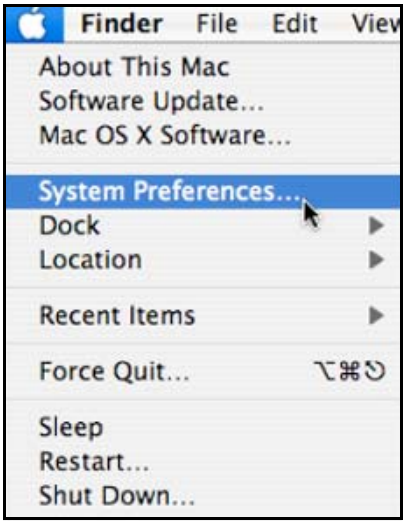
3 The IP settings are displayed as follows.



Mac OS X: 10.3 and 10.4

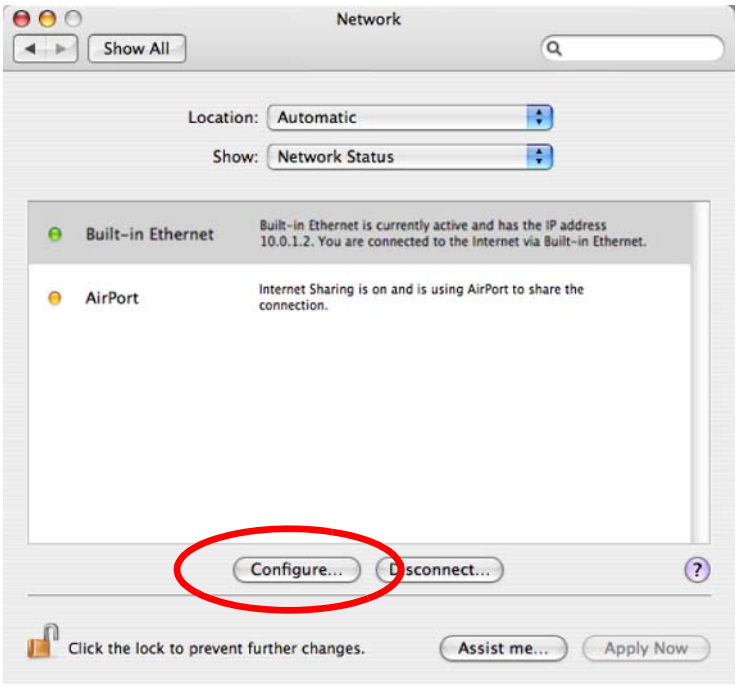
The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

1 Click **Apple** > **System Preferences**.

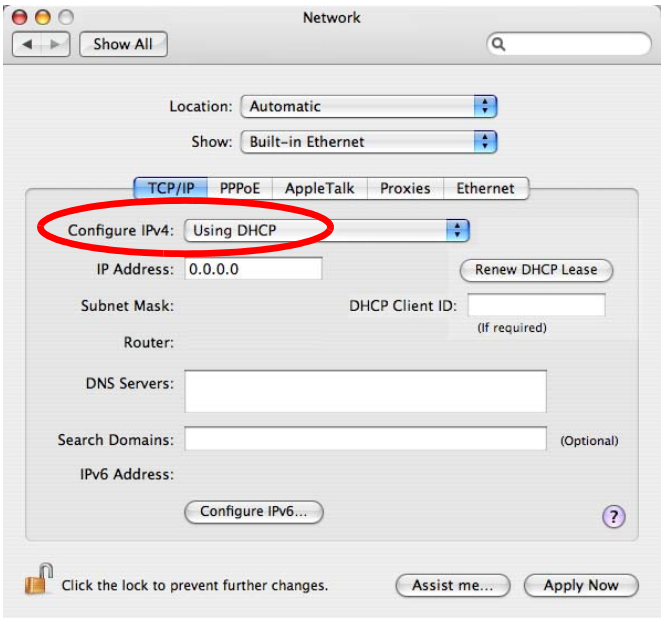


2 In the **System Preferences** window, click the **Network** icon.

3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure.**

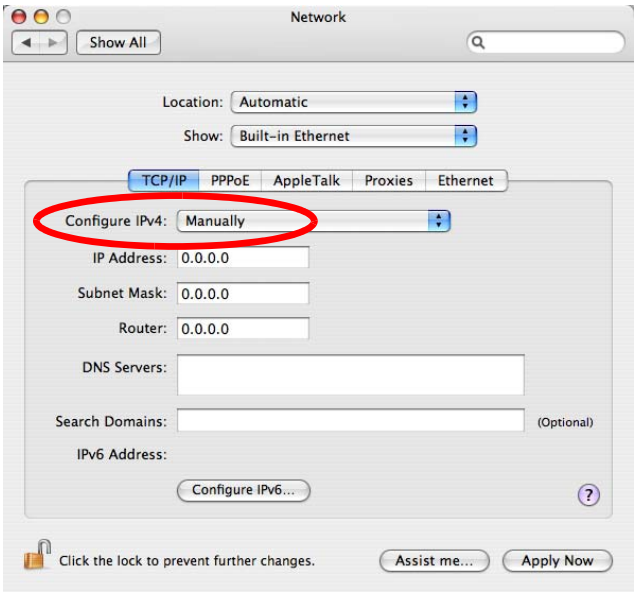


4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.



5 For statically assigned settings, do the following:

- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.
- In the **Router** field, type the IP address of your device.

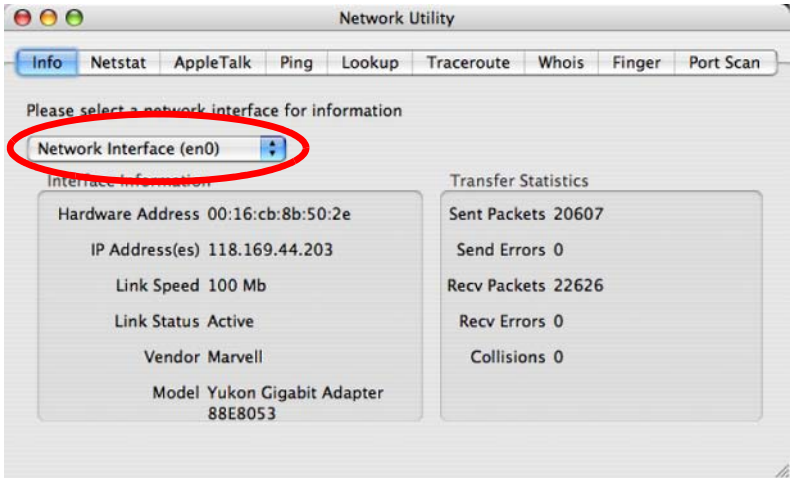


6 Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

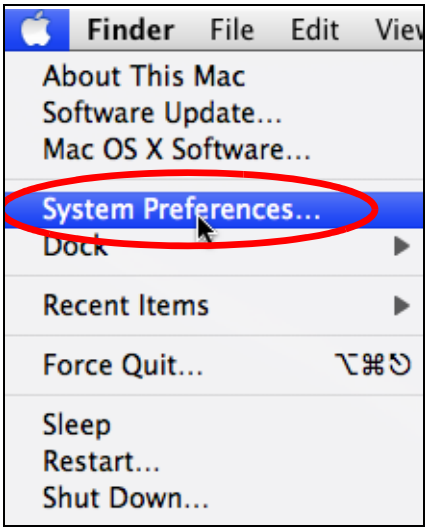
Figure 83 Mac OS X 10.4: Network Utility



Mac OS X: 10.5 and 10.6

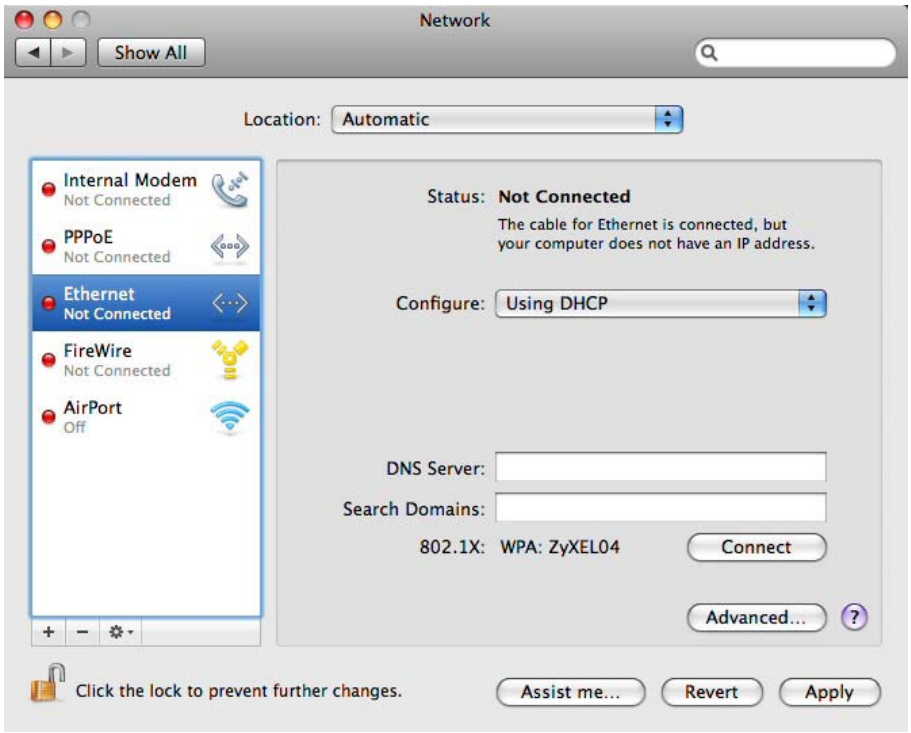
The screens in this section are from Mac OS X 10.5 but can also apply to 10.6.

1 Click **Apple** > **System Preferences**.



2 In **System Preferences**, click the **Network** icon.

3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.

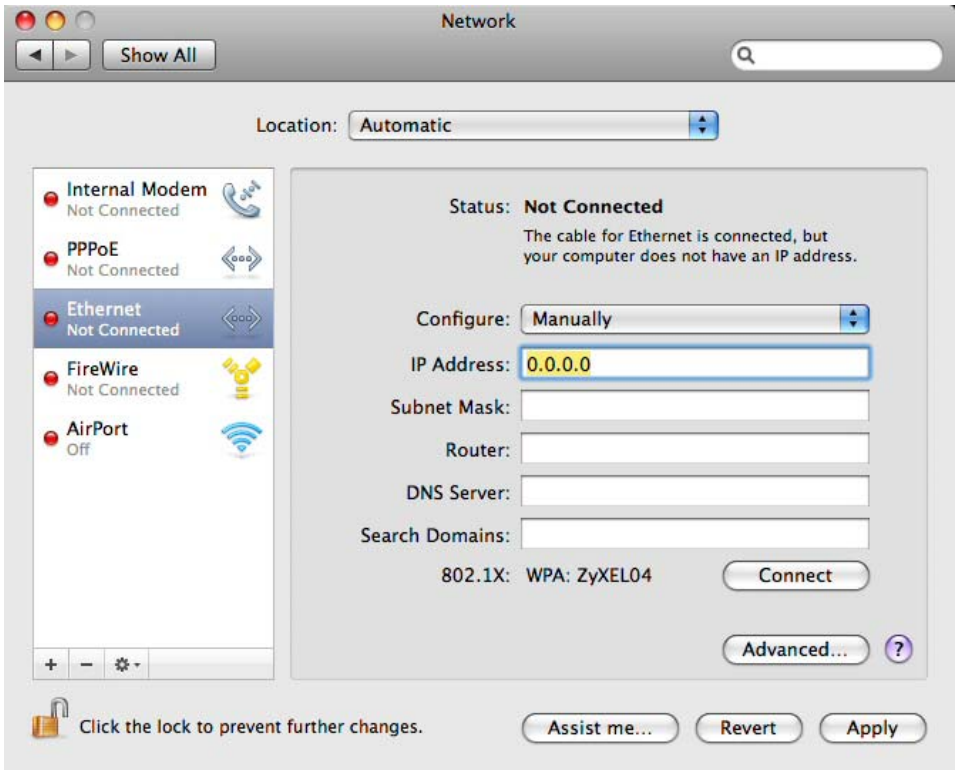


4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.

- In the **Subnet Mask** field, enter your subnet mask.
- In the **Router** field, enter the IP address of your WAP3205 v3.

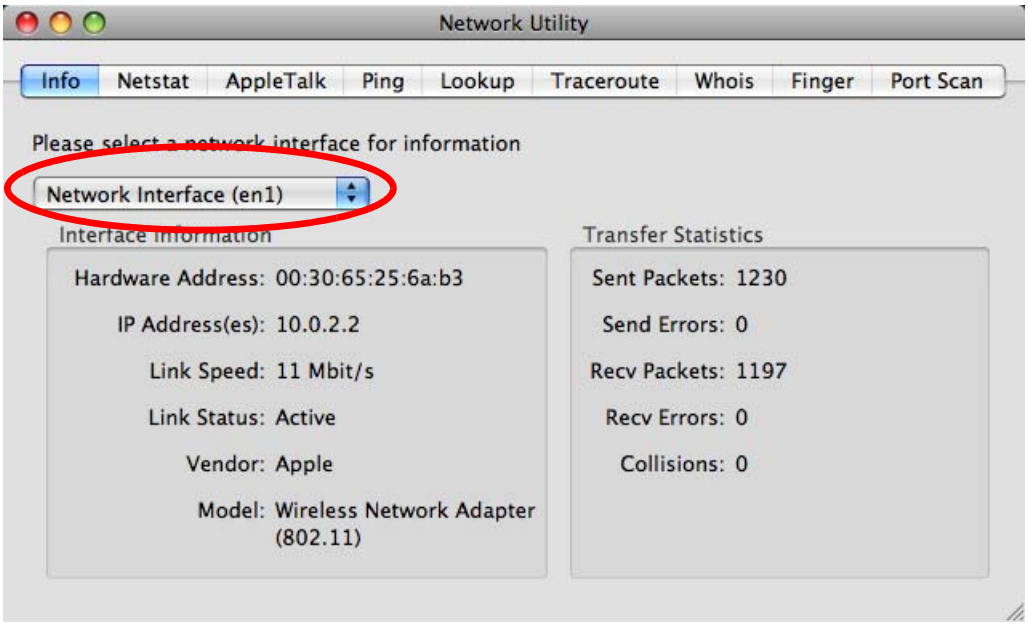


6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 84 Mac OS X 10.5: Network Utility



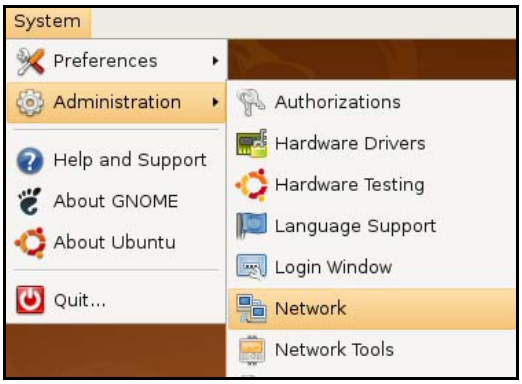
Linux: Ubuntu 8 (GNOME)

This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

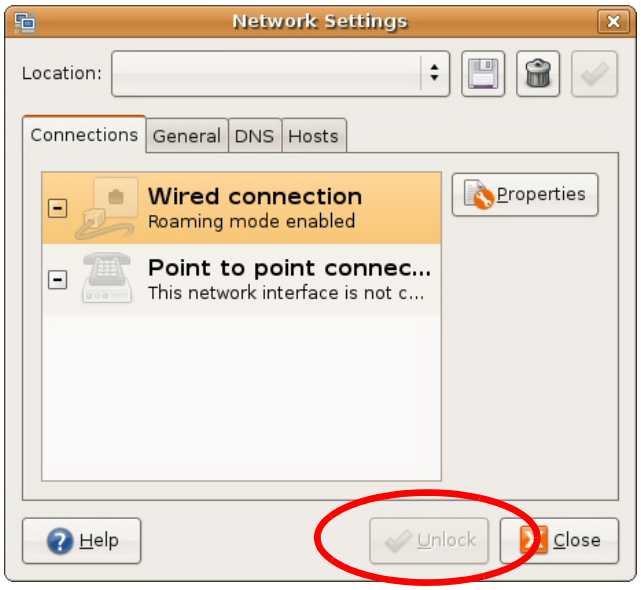
Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

1 Click **System > Administration > Network**.



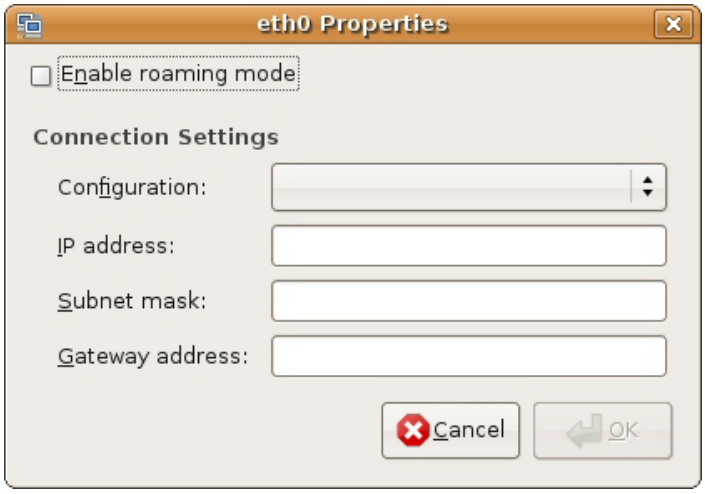
2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.



3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

5 The **Properties** dialog box opens.



- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

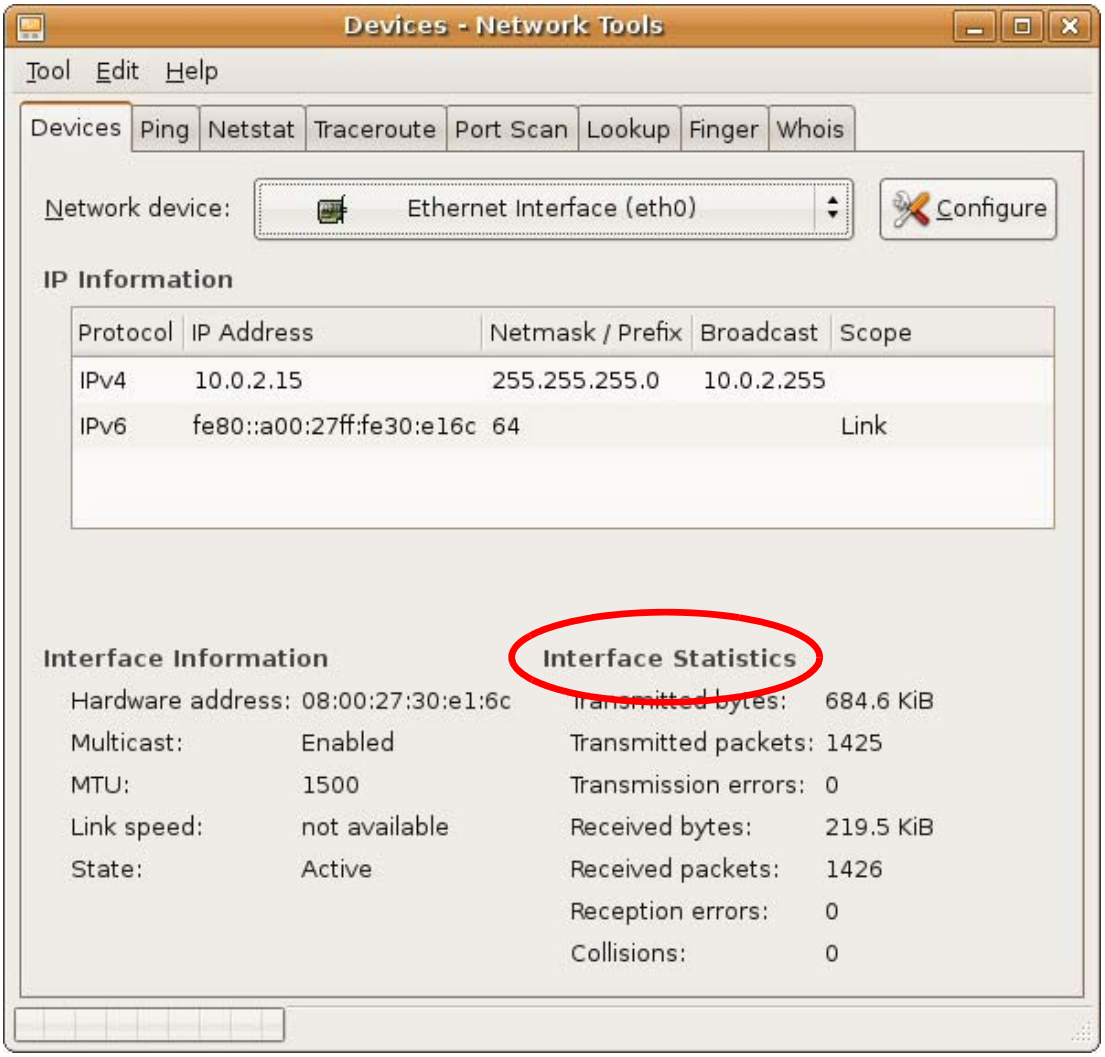
7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices** tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 85 Ubuntu 8: Network Tools



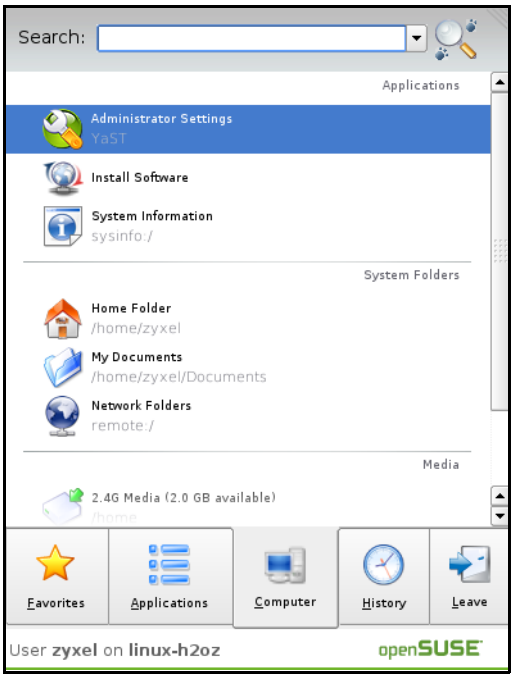
Linux: openSUSE 10.3 (KDE)

This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

Note: Make sure you are logged in as the root administrator.

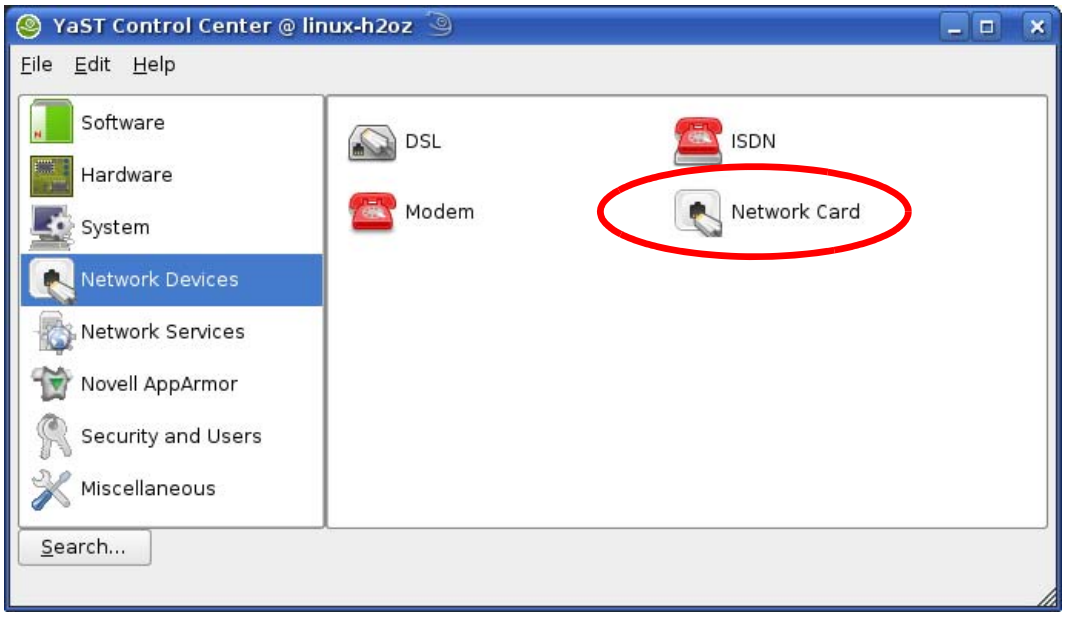
Follow the steps below to configure your computer IP address in the KDE:

1 Click **K Menu > Computer > Administrator Settings (YaST)**.

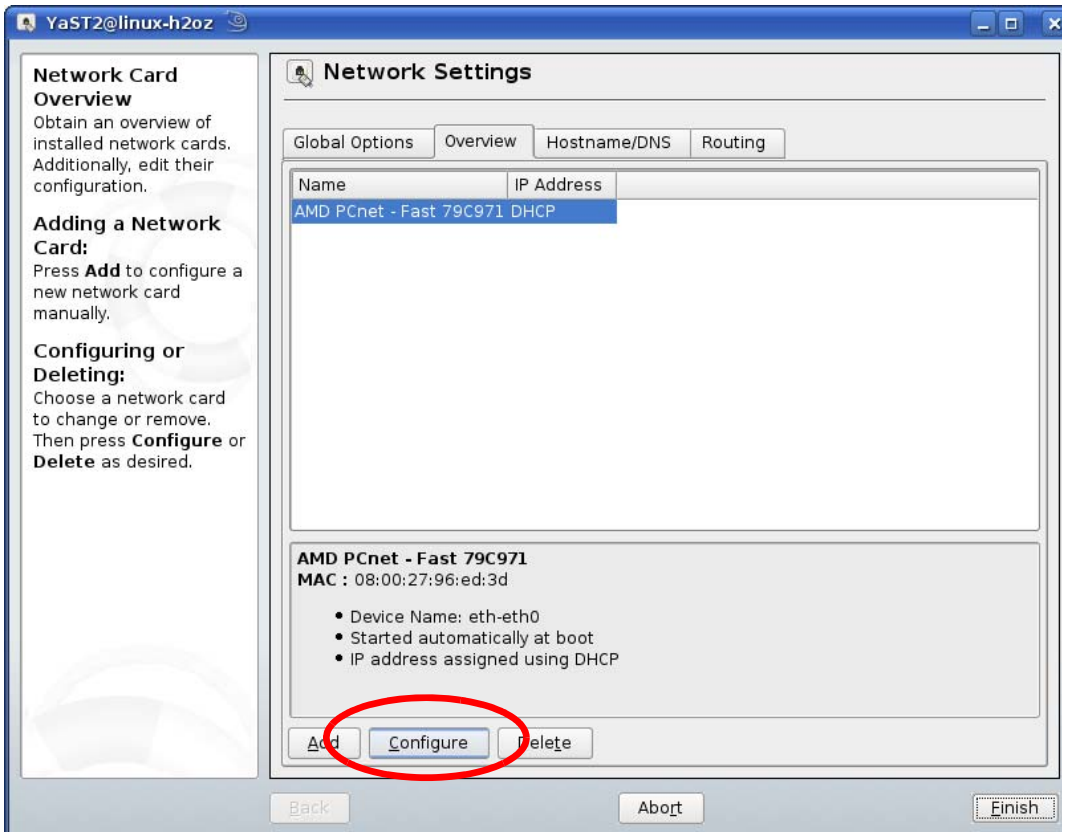


2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

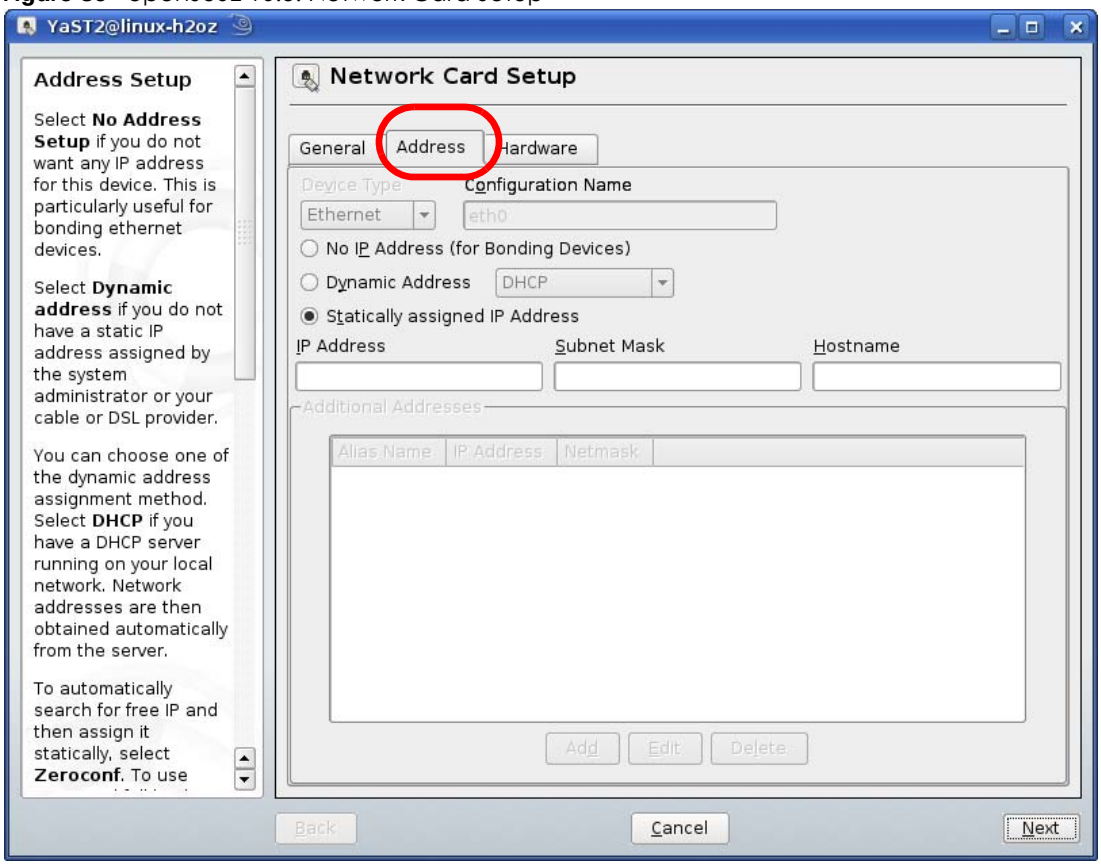


4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.



5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 86 openSUSE 10.3: Network Card Setup

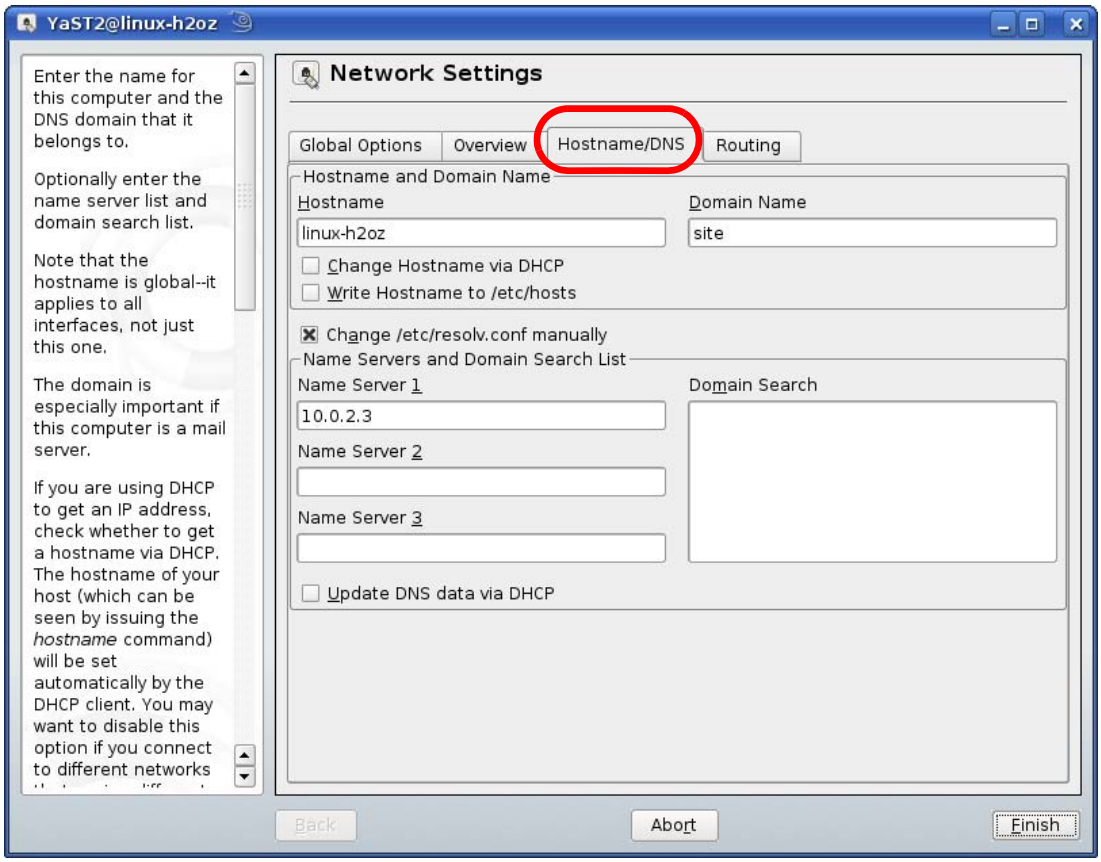


6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7 Click **Next** to save the changes and close the **Network Card Setup** window.

8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

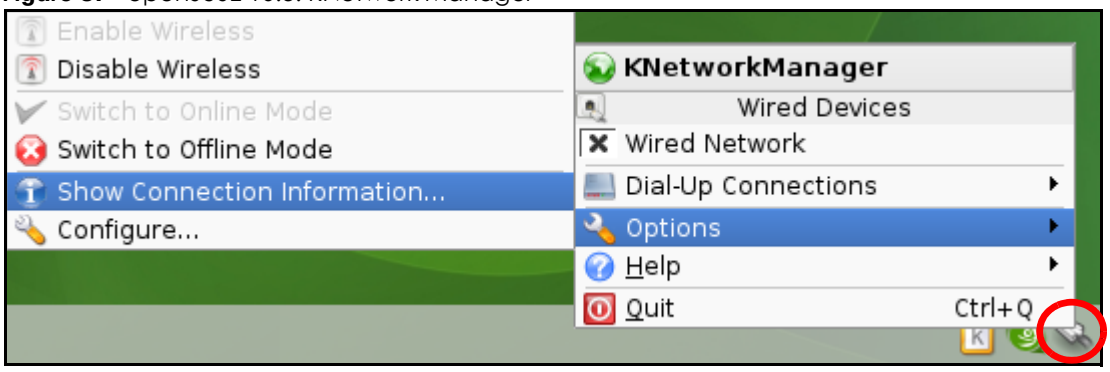


9 Click **Finish** to save your settings and close the window.

Verifying Settings

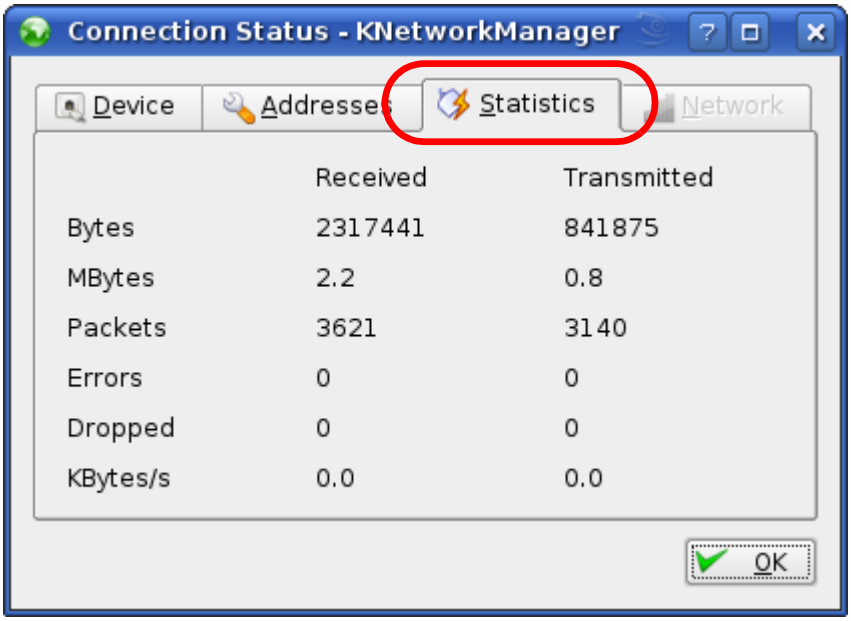
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 87 openSUSE 10.3: KNetwork Manager



When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

Figure 88 openSUSE: Connection Status - KNetwork Manager



APPENDIX D
Wireless LANs

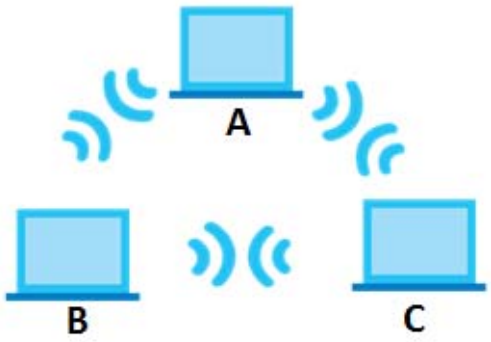
Wireless LAN Topologies

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 89 Peer-to-Peer Communication in an Ad-hoc Network

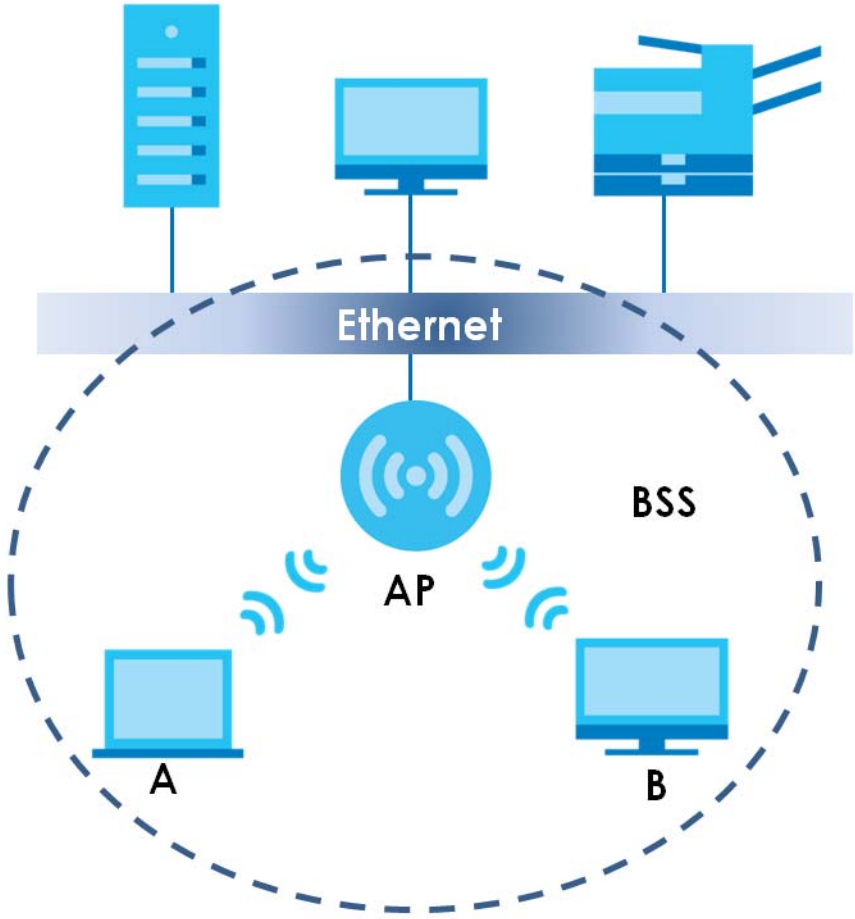


BSS

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 90 Basic Service Set



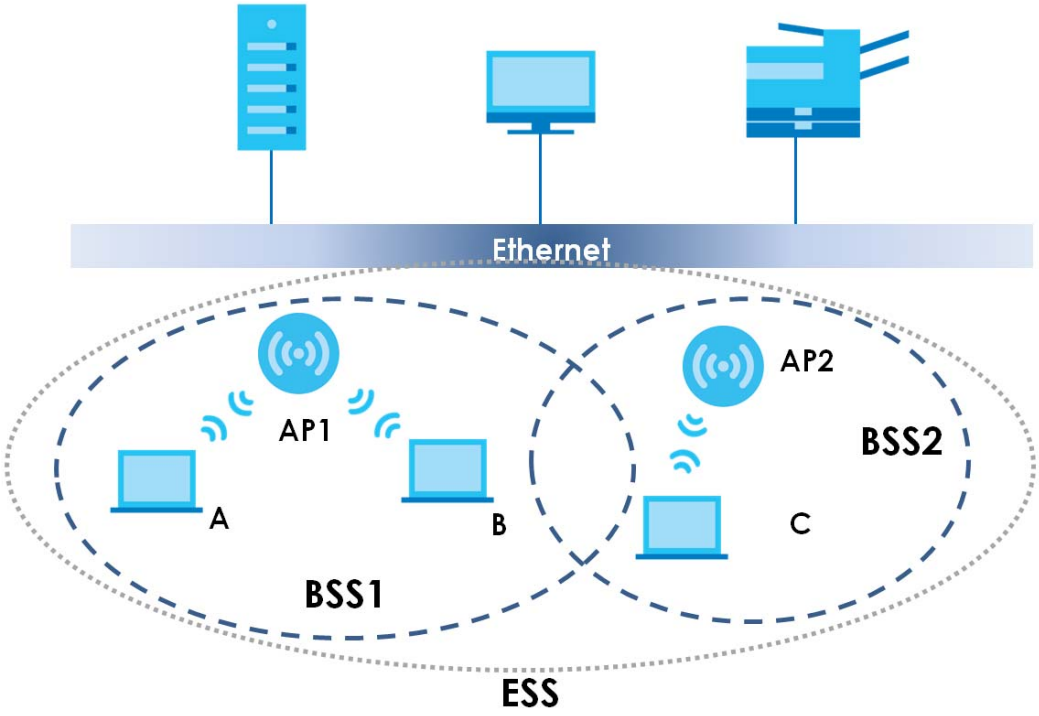
ESS

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 91 Infrastructure WLAN



Channel

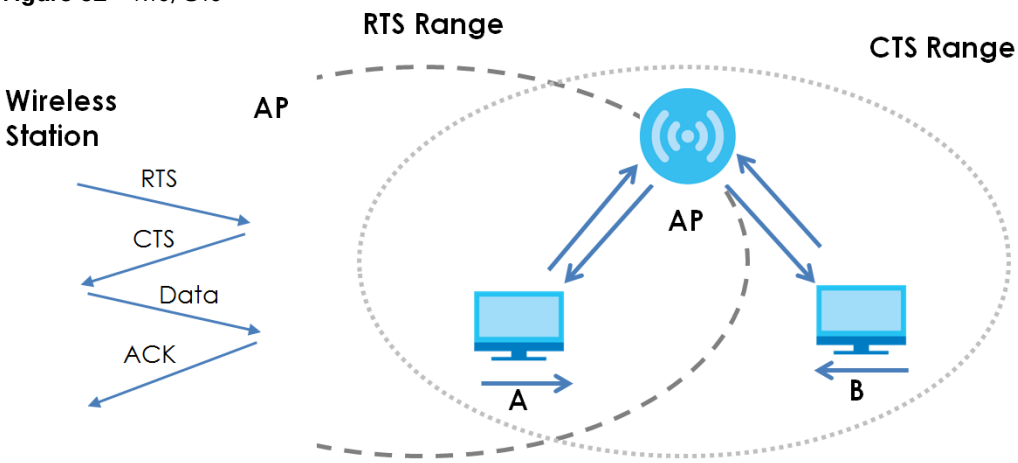
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference 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 92 RTS/CTS



Note: Stations cannot hear each other. They can hear the AP.

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 49 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 50 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)
	WPA2
Most Secure	

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 51 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

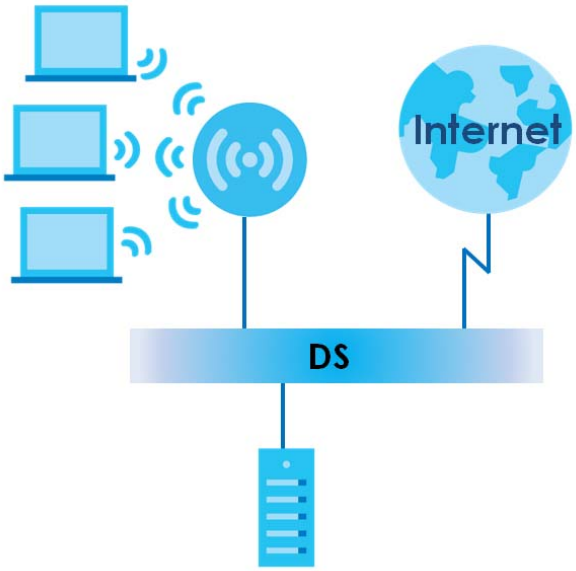
To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

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 93 WPA(2) with RADIUS Application Example



WPA(2)-PSK Application Example

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

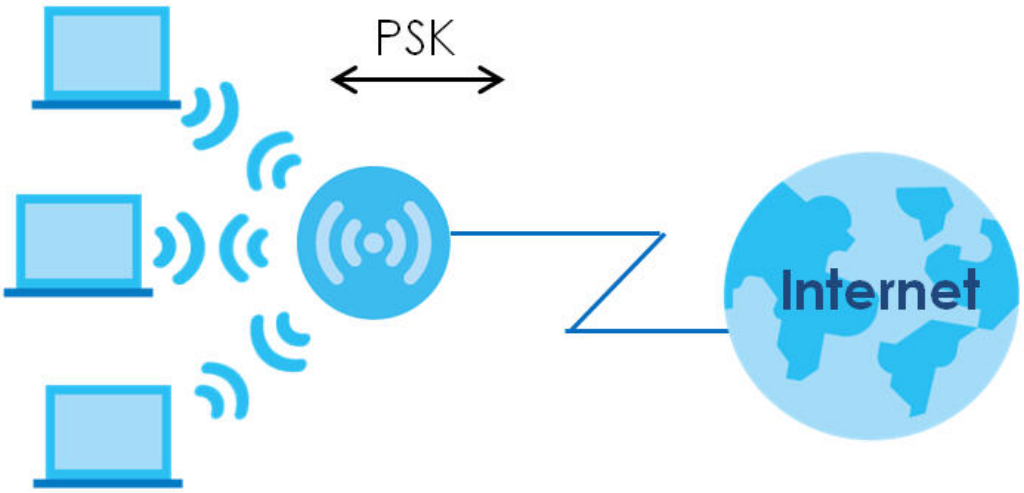
1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).

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 94 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 52 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION 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.

APPENDIX E
Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 53 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular video conferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.

Table 53 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.

Table 53 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another video conferencing solution.

APPENDIX F
Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

See *http://www.zyxel.com/homepage.shtml* and also *http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml* for the latest information.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications Corporation
- http://www.zyxel.com

Asia

China

- Zyxel Communications (Shanghai) Corp.
  Zyxel Communications (Beijing) Corp.
  Zyxel Communications (Tianjin) Corp.
- http://www.zyxel.cn

India

- Zyxel Technology India Pvt Ltd
- http://www.zyxel.in

Kazakhstan

- Zyxel Kazakhstan
- http://www.zyxel.kz

Korea

- Zyxel Korea Corp.
- http://www.zyxel.kr

Malaysia

- Zyxel Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Philippines

- Zyxel Philippines
- http://www.zyxel.com.ph

Singapore

- Zyxel Singapore Pte Ltd.
- http://www.zyxel.com.sg

Taiwan

- Zyxel Communications Corporation
- http://www.zyxel.com/tw/zh/

Thailand

- Zyxel Thailand Co., Ltd
- http://www.zyxel.co.th

Vietnam

- Zyxel Communications Corporation-Vietnam Office
- http://www.zyxel.com/vn/vi

Europe

Austria

- Zyxel Deutschland GmbH
- http://www.zyxel.de

Belarus

- Zyxel BY
- http://www.zyxel.by

Belgium

- Zyxel Communications B.V.
- http://www.zyxel.com/be/nl/
- http://www.zyxel.com/be/fr/

Bulgaria

- Zyxel България
- http://www.zyxel.com/bg/bg/

Czech Republic

- Zyxel Communications Czech s.r.o
- http://www.zyxel.cz

Denmark

- Zyxel Communications A/S
- http://www.zyxel.dk

Estonia

- Zyxel Estonia
- http://www.zyxel.com/ee/et/

Finland

- Zyxel Communications
- http://www.zyxel.fi

France

- Zyxel France
- http://www.zyxel.fr

Germany

- Zyxel Deutschland GmbH
- http://www.zyxel.de

Hungary

- Zyxel Hungary & SEE
- http://www.zyxel.hu

Italy

- Zyxel Communications Italy
- http://www.zyxel.it/

Latvia

- Zyxel Latvia
- http://www.zyxel.com/lv/lv/homepage.shtml

Lithuania

- Zyxel Lithuania
- http://www.zyxel.com/lt/lt/homepage.shtml

Netherlands

- Zyxel Benelux
- http://www.zyxel.nl

Norway

- Zyxel Communications
- http://www.zyxel.no

Poland

- Zyxel Communications Poland
- http://www.zyxel.pl

Romania

- Zyxel Romania
- http://www.zyxel.com/ro/ro

Russia

- Zyxel Russia
- http://www.zyxel.ru

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- http://www.zyxel.sk

Spain

- Zyxel Communications ES Ltd
- http://www.zyxel.es

Sweden

- Zyxel Communications
- http://www.zyxel.se

Switzerland

- Studerus AG

- http://www.zyxel.ch/

Turkey

- Zyxel Turkey A.S.
- http://www.zyxel.com.tr

UK

- Zyxel Communications UK Ltd.
- http://www.zyxel.co.uk

Ukraine

- Zyxel Ukraine
- http://www.ua.zyxel.com

Latin America

Argentina

- Zyxel Communication Corporation
- http://www.zyxel.com/ec/es/

Brazil

- Zyxel Communications Brasil Ltda.
- https://www.zyxel.com/br/pt/

Ecuador

- Zyxel Communication Corporation
- http://www.zyxel.com/ec/es/

Middle East

Israel

- Zyxel Communication Corporation
- http://il.zyxel.com/homepage.shtml

Middle East

- Zyxel Communication Corporation
- http://www.zyxel.com/me/en/

North America

USA

- Zyxel Communications, Inc. - North America Headquarters
- http://www.zyxel.com/us/en/

Oceania

Australia

- Zyxel Communications Corporation
- http://www.zyxel.com/au/en/

Africa

South Africa

- Nology (Pty) Ltd.
- http://www.zyxel.co.za

APPENDIX G
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

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

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.
- Operation of this device is restricted to indoor use only, except for relevant user's manual mention that this device can be installed into the external environment.

EUROPEAN UNION

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

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED)

- Compliance information for 2.4GHz and/or 5GHz wireless products relevant to the EU and other Countries following the EU Directive 2014/53/EU (RED). And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 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 the 5GHz wireless LANs.
- If this device for operation in the band 5150-5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20cm between the radio equipment and your body.
- The maximum RF power operating for each band as follows:
  - the band 2,400 to 2,483.5 MHz is 86.10 mW,

Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС. **National Restrictions** • 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.
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 2014/53/UE..
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU. **National Restrictions** • In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage. • I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EL 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 2014/53/ΕΕ.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/UE.
Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE. **National Restrictions** • 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.

Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. **National Restrictions** • 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.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/UE.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 2014/53/UE.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU 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 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 2014/53/EU.

Notes:

- Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.
- 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 obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- 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.
- 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 < 8W, 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.

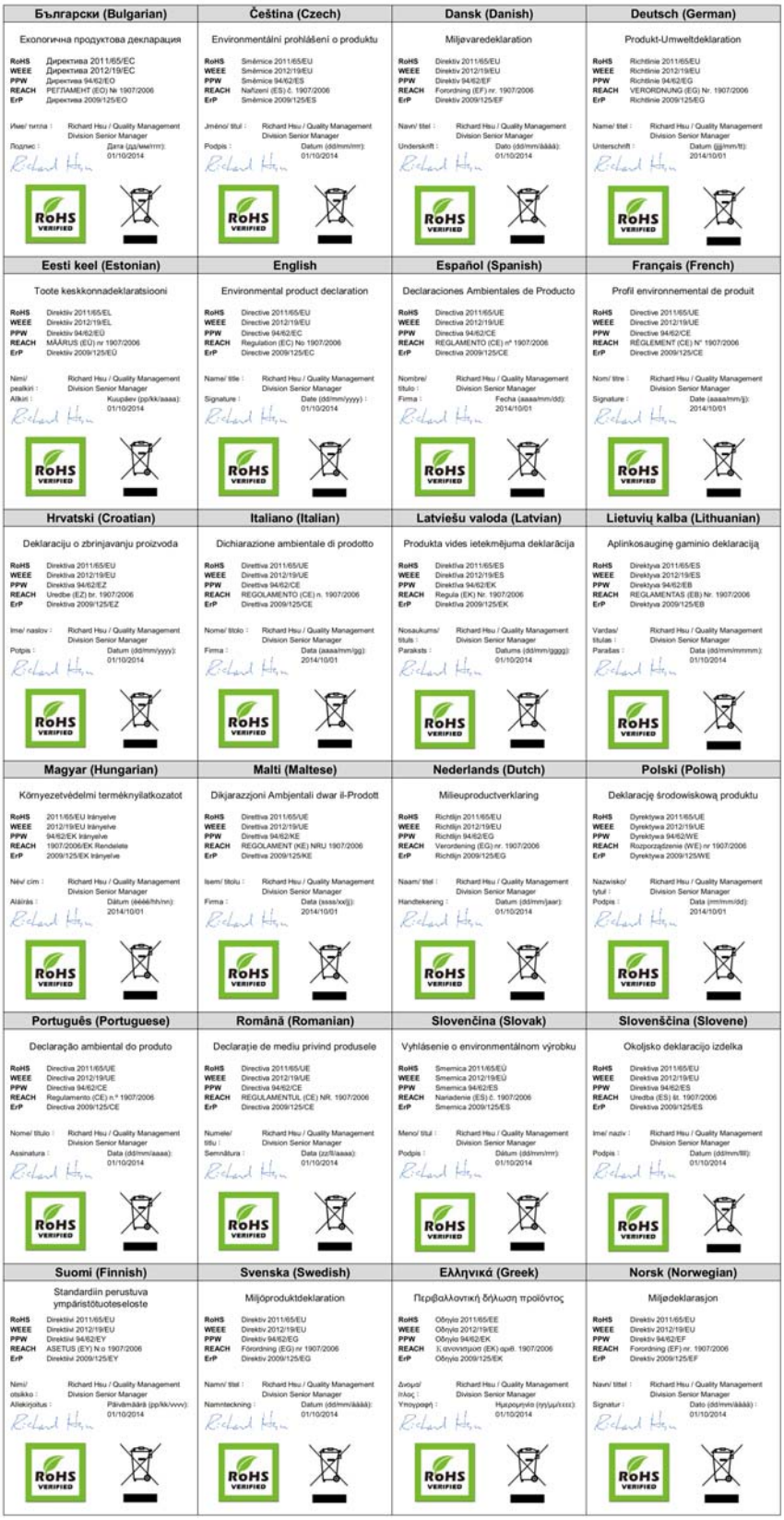
El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado 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 (ЕО) № 1907/2006
ErP Директива 2009/125/EO

Име/ титла : Richard Hsu / Quality Management Division Senior Manager
Подпис : Дата (дд/мм/гггг): 01/10/2014

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

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

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

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

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

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

Français (French)

Profil environnemental de produit

RoHS Directive 2011/65/UE
WEEE Directive 2012/19/UE
PPW Directive 94/62/CE
REACH RÈGLEMENT (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

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

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

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

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

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

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 (sssa/xx/jj): 2014/10/01

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

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 (rr/mm/dd): 2014/10/01

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

Română (Romanian)

Declarație de mediu privind produsele

RoHS Directiva 2011/65/UE
WEEE Directiva 2012/19/UE
PPW Directiva 94/62/CE
REACH REGLAMENTUL (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

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

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/ll): 01/10/2014

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

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

Ελληνικά (Greek)

Περιβαλλοντική δήλωση προϊόντος

RoHS Οδηγία 2011/65/ΕΕ
WEEE Οδηγία 2012/19/ΕΕ
PPW Οδηγία 94/62/ΕΚ
REACH Κ ανανησμοι (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

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

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC if the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

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.

Index

H

I

L

M

N

O

P

Q

R