WAP5805

5-GHz Wireless N600 HD Media Streaming Box

Version 1.00
Edition 1, 9/2013

User's Guide

Default Login Details	
LAN IP Address	AP: 192.168.1.2 Client: 192.168.1.10
Password	1234

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

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

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the WAP5805 and access the Web Configurator.

Contents Overview

Table of Contents

PART I

User's Guide

Getting to Know Your WAP5805

1.1 Overview

This chapter introduces the main features and applications of the WAP5805.

The WAP5805 enables home users to easily stream HD video content, enjoy IPTV services, and play online games in different rooms via a wireless network connection with set-top boxes, game consoles, and other heavy bandwidth devices.

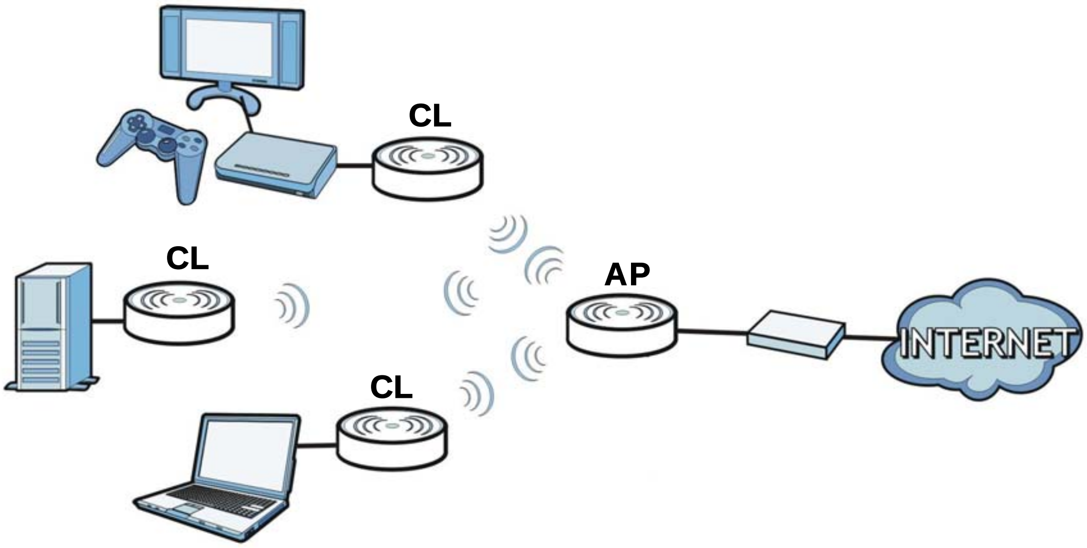
With data rates of up to 600 Mbps, you can enjoy a breathtaking high-speed connection at home or in the office. It is an excellent solution for daily activities such as file transfers, music downloading, HD video streaming and online gaming.

1.2 Applications

The WAP5805 can be configured to use the following operating modes:

- **AP**. Use the switch on the side panel to set the WAP5805 to work in AP mode (**AP**). You can connect to a broadband modem/router for Internet access and/or connect network devices via the Ethernet ports of the WAP5805 in AP mode so that they can communicate with each other and access the Internet. Wireless clients can connect to the WAP5805 in AP mode to access network resources.
- **Client**. Use the switch on the side panel to set the WAP5805 to work in client mode (**CL**). The WAP5805 in client mode can access the Internet through a WAP5805 in AP mode.

Figure 1 WAP5805 Applications



1.3 Ways to Manage the WAP5805

Use any of the following methods to manage the WAP5805.

- Web Configurator. This is recommended for everyday management of the WAP5805 using a (supported) web browser.
- WPS (Wi-Fi Protected Setup) button. You can use the WPS button or the WPS section of the Web Configurator to set up a wireless network with your WAP5805.

1.4 Good Habits for Managing the WAP5805

Do the following things regularly to make the WAP5805 more secure and to manage the WAP5805 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 WAP5805 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the WAP5805. You could simply restore your last configuration.

1.5 Resetting the WAP5805

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the **RESET** button at the back of the WAP5805 to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to "1234" and the IP address of the WAP5805 in AP mode will be reset to "192.168.1.2" and the IP address of the WAP5805 in client mode will be reset to "192.168.1.10".

1.5.1 Procedure to Use the Reset Button

1. Make sure the power LED is on.
2. Press the **RESET** button for longer than 1 second to restart/reboot the WAP5805.
3. Press the **RESET** button for longer than five seconds to set the WAP5805 back to its factory-default configurations.

1.6 The WPS Button

You can use the WPS button ( ) on the front panel of the WAP5805 to activate WPS in order to quickly set up a wireless network with strong security.

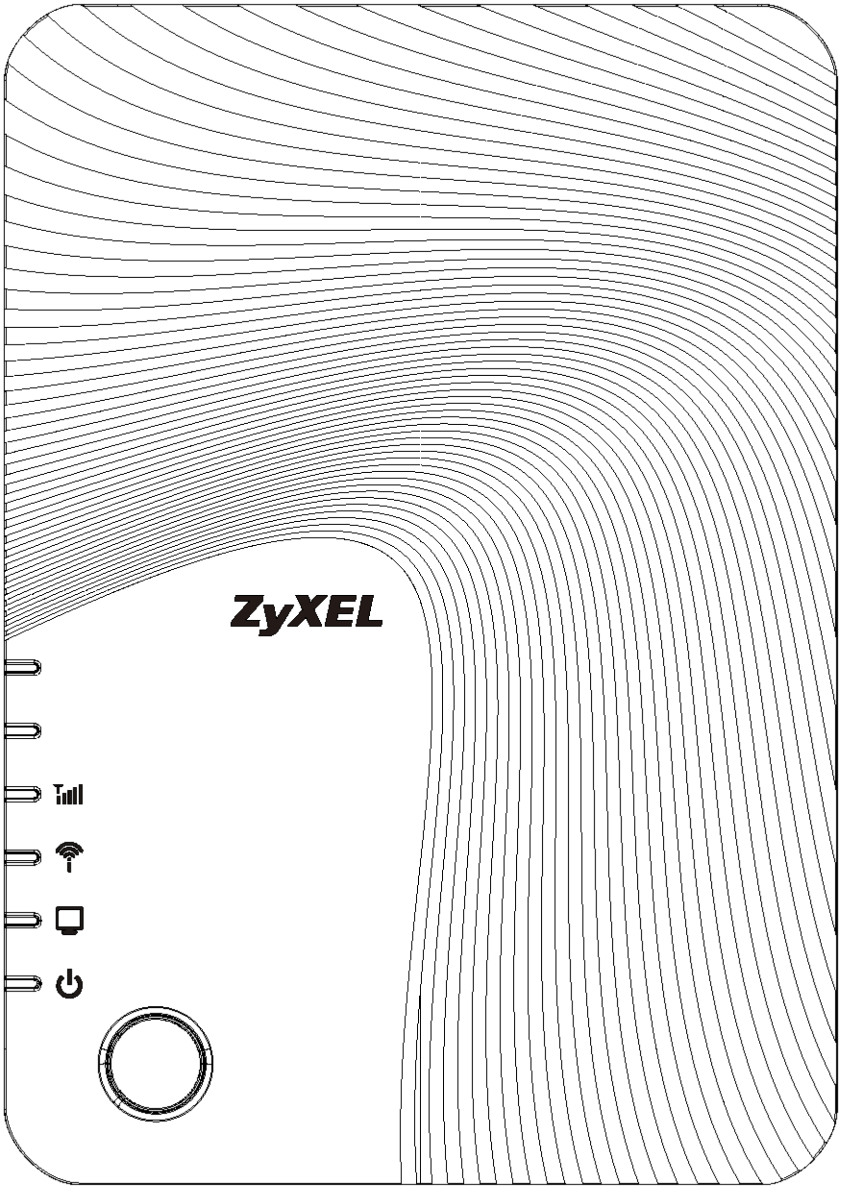
1 Make sure the **POWER** LED is on (not blinking).

2 Press the WPS button for more than three seconds and release it. Press the WPS button on another WPS-enabled device within range of the WAP5805.

Note: You must activate WPS in the WAP5805 that acts as the AP and in another WAP5805 that acts as the client within two minutes of each other.

1.7 LEDs

Figure 2 Front Panel



The following table describes the LEDs and the WPS button for AP mode.

Table 1 Front Panel LEDs and WPS Button in AP mode

LED	COLOR	STATUS	DESCRIPTION
Link Quality 📶	Green	On	This LED is always on after the system starts up.
		Off	The WAP5805 is not receiving power or WiFi is not functional.
Wireless 🛜	Green	On	The WAP5805 is ready, able to send/receive data through the wireless LAN.
		Blinking	The WAP5805 is sending/receiving data through the wireless LAN.
		Off	The wireless LAN is not ready or has failed.
LAN 🖥	Green	On	The WAP5805 has a successful 10/100 Mbps fast Ethernet connection.
		Blinking	The WAP5805 is sending/receiving data through the LAN.
		Off	The LAN is not connected.
	Blue	On	The WAP5805 has a successful 10/100/1000 Mbps GbE connection.
		Blinking	The WAP5805 is sending/receiving data through the LAN.
		Off	The LAN is not connected.
Power ⏻	Green	On	The WAP5805 is receiving power and functioning properly.
		Off	The WAP5805 is not receiving power.
WPS ⚷	Blue	On	The WPS function is enabled.
		Blinking	The WAP5805 is negotiating a WPS connection with a wireless device.
		Off	The WPS function is not ready or failed.

The following table describes the LEDs and the WPS button for CL mode.

Table 2 Front Panel LEDs and WPS Button in CL mode

LED	COLOR	STATUS	DESCRIPTION
Link Quality 📶	Blue	On	The WAP5805 is connecting to an AP and the transmission rate is greater than 150 Mbps.
		Off	The WAP5805 is not receiving power or not associating with an AP.
	Green	On	The WAP5805 is connecting to an AP and the transmission rate is 50 to 150 Mbps.
		Off	The WAP5805 is not receiving power or not associating with an AP.
	Amber	On	The WAP5805 is connecting to an AP and the transmission rate is less than 50 Mbps.
		Off	The WAP5805 is not receiving power or not associating with an AP.

Table 2 Front Panel LEDs and WPS Button in CL mode (continued)

LED	COLOR	STATUS	DESCRIPTION
Wireless 📶	Blue	On	The WAP5805 is ready, able to send/receive data through the wireless LAN.
		Blinking	The WAP5805 is sending/receiving data through the wireless LAN.
		Off	The wireless LAN is not ready or has failed.
LAN 🖥	Green	On	The WAP5805 has a successful 10/100 Mbps fast Ethernet connection.
		Blinking	The WAP5805 is sending/receiving data through the LAN.
		Off	The LAN is not connected.
	Blue	On	The WAP5805 has a successful 10/100/1000 Mbps GbE connection.
		Blinking	The WAP5805 is sending/receiving data through the LAN.
		Off	The LAN is not connected.
Power ⏻	Green	On	The WAP5805 is receiving power and functioning properly.
		Off	The WAP5805 is not receiving power.
WPS ⚿	Blue	On	The WPS function is enabled.
		Blinking	The WAP5805 is negotiating a WPS connection with a wireless device.
		Off	The WPS function is not ready or failed.

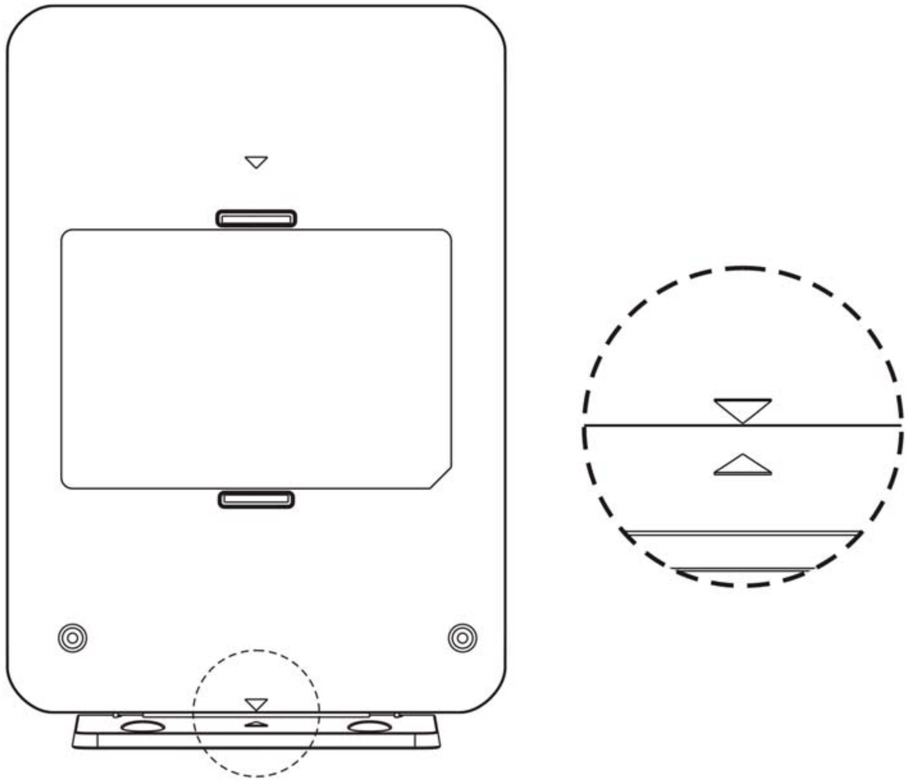
1.8 Wall-mounting Instructions

1.8.1 Desktop Installation

When opening the product, there will be no need to assemble the device, as the WAP5805 will be fully assembled for you.

For desktop installation, place the WAP5805 in an area that is convenient for you to access and preferably in a location that is away from other electric devices.

Figure 3 Arrows on the Stand and WAP5805



1.8.2 Wall-mounting Installation

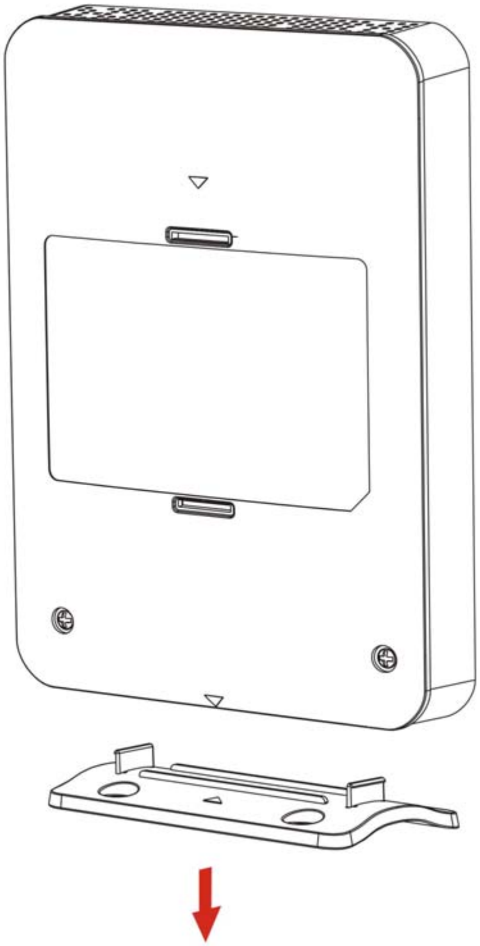
Complete the following steps to hang your WAP5805 on a wall.

Table 3 Wall Mounting Information

Distance between holes	5 cm
M4 Screws	Two

1 Disassemble the stand, see Section Figure 4 on page 16.

Figure 4 Stand Installation Example

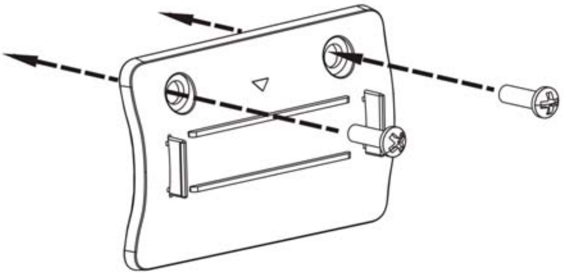


2 Select a position free of obstructions on a sturdy wall.

3 Install the stand on the wall. Make sure the screw holes of the stand are on the top and screws are snugly fastened to the wall. The stand needs to hold the weight of the WAP5805 with the connection cables.

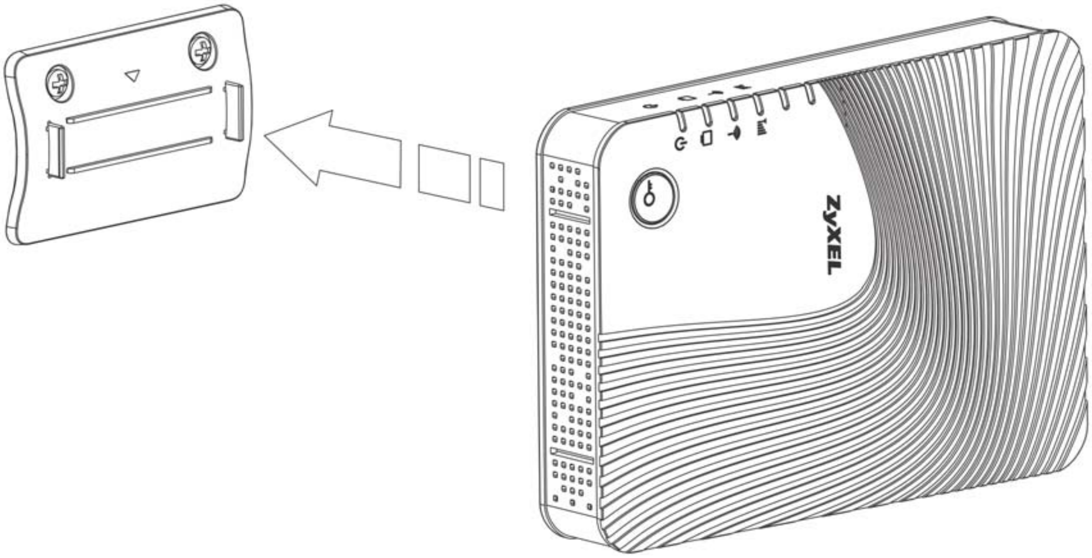
Be careful to avoid damaging pipes or cables located inside the wall when installing the stand.

Figure 5 Installing the Stand



4 Hold the WAP5805 with the LEDs facing upward. Align the holes on the back of the WAP5805 with the tabs on the stand. Attach the WAP5805 to the stand. Press gently but firmly until the WAP5805 clicks into place.

Figure 6 Attaching the WAP5805 to the Stand



2

WAP5805 Modes

2.1 Overview

This chapter introduces the different modes available on your WAP5805. First, the term “mode” refers to two things in this User’s Guide.

- **Web Configurator mode**. This refers to the Web Configurator screen you want to use for editing WAP5805 features.
- **Device mode**. This is the operating mode of your WAP5805, or simply how the WAP5805 is being used in the network.

2.1.1 Web Configurator Modes

This refers to the configuration interface of the Web Configurator, which has two modes:

- **Expert**. Advanced users can change to this mode to customize all the functions of the WAP5805. Click **Expert Mode** after logging into the Web Configurator. The User’s Guide Chapter 3 on page 20 through Chapter 10 on page 65 discusses the screens in this mode.

2.1.2 Device Operating Modes

This refers to the operating mode of the WAP5805, which can act as a:

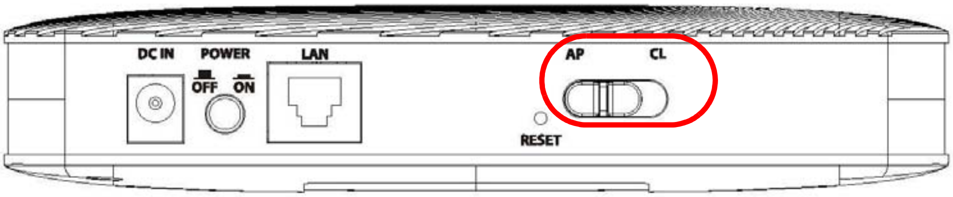
- **Access Point** (**AP**). Use this mode if you want to extend your network by allowing network devices to connect to the WAP5805 wirelessly. Go to Section 5.5 on page 34 to view the **Status** screen in this mode.
- **Client** (**CL**). Use this mode if there is an existing WAP5805 that acts as an AP in your network. Go to Section 6.5 on page 39 to view the **Status** screen in this mode. In Client mode, you should know the SSID and wireless security details of the WAP5805 to which you want to connect.

Note: Choose your device mode carefully to avoid having to change it later.

2.1.3 Changing Operating Mode

Push the **AP / CL** switch on the WAP5805's side panel to the **AP** position to have the WAP5805 act as an access point. Otherwise, push the switch to the **CL** position to have the WAP5805 work as a wireless client. The WAP5805 restarts automatically after you change operating modes.

Figure 7 Side Panel



3

The Web Configurator

3.1 Overview

This chapter describes how to access the WAP5805 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 WAP5805 via Internet browser. Use Internet Explorer 6.0 and later or Firefox 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

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

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

Refer to the Troubleshooting chapter (Chapter 11 on page 72) to see how to make sure these functions are allowed in Internet Explorer.

3.2 Accessing the Web Configurator

1 Connect your computer to the LAN port of the WAP5805.

2 The default IP address of the WAP5805 in access point mode is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254". The default IP address of the WAP5805 in client mode is "192.168.1.10". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254" except for "192.168.1.10".

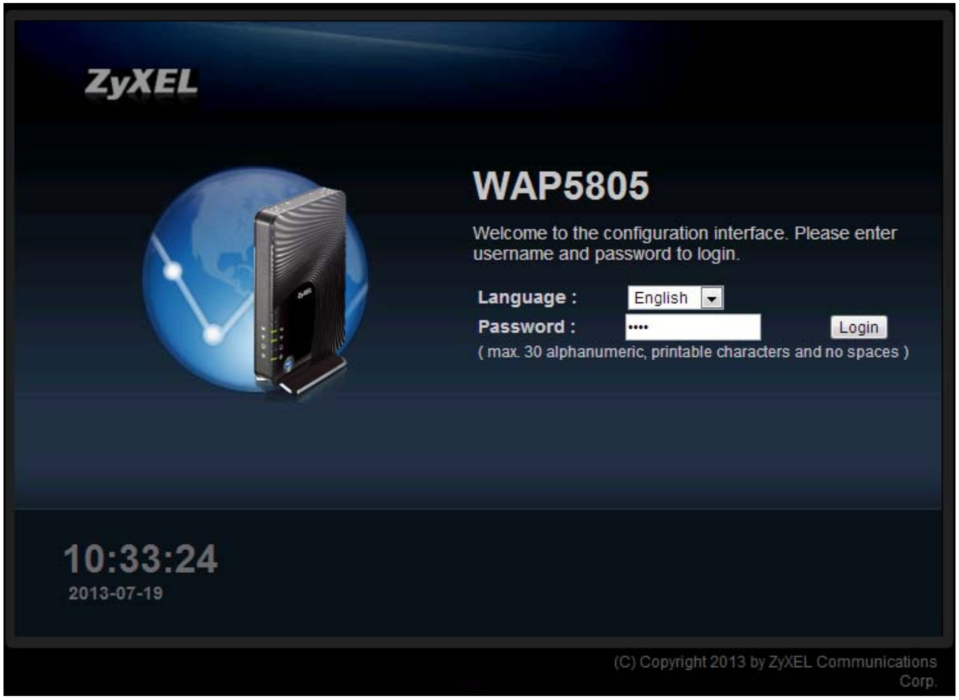
3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see Appendix A on page 77 for information on changing your computer's IP address.

4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "http://192.168.1.2" for AP and "http://192.168.1.10" for CL as the web address in your web browser.

3.2.1 Login Screen

The Web Configurator initially displays the following login screen.

Figure 8 Login screen



WAP5805

Welcome to the configuration interface. Please enter username and password to login.

Language : English

Password : ••••

Login

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

10:33:24

2013-07-19

(C) Copyright 2013 by ZyXEL Communications Corp.

The following table describes the labels in this screen.

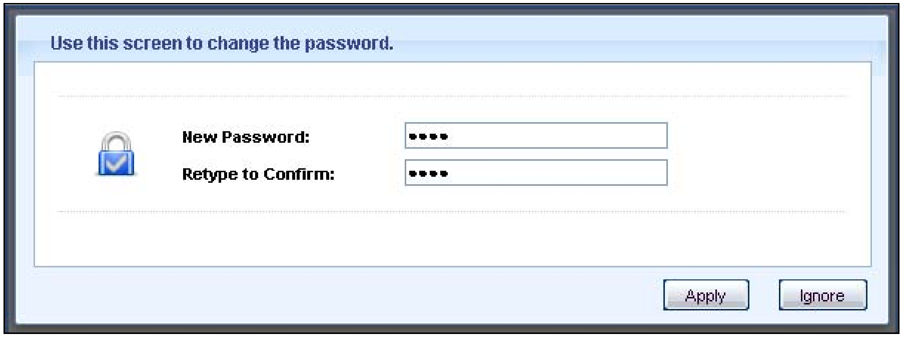
Table 4 Login screen

LABEL	DESCRIPTION
Language	Select the language you want to use to configure the Web Configurator.
Password	Type "1234" (default) as the password. Click **Login**.
00:07:37 2013-06-19	This shows the time (hh:mm:ss) and date (yyyy:mm:dd) of the timezone in your regional location. This is set by factory default. The time is in 24-hour format, for example 15:00 is 3:00 PM.

3.2.2 Password Screen

You should see a screen asking you to change your password (highly recommended) as shown next.

Figure 9 Change Password Screen



Use this screen to change the password.

New Password: ••••

Retype to Confirm: ••••

The following table describes the labels in this screen.

Table 5 Change Password Screen

LABEL	DESCRIPTION
New Password	Type a new password.
Retype to Confirm	Retype the password for confirmation.
Apply	Click **Apply** to save your changes back to the WAP5805.
Ignore	Click **Ignore** if you do not want to change the password this time.

Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes; go to Chapter 10 on page 65 to change this). Simply log back into the WAP5805 if this happens.

4

Tutorials

4.1 Overview

You can configure a WAP5805 AP - WAP5805 Client wireless connection using:

- Push Button Configuration (PBC)
- PIN Configuration
- Configuring AP - Client Wireless Connection Using the Expert Mode Screens

4.2 Configuring AP - Client Wireless Connection Using WPS

This section gives you an example of how to set up wireless network using WPS. This example uses the WAP5805 in AP mode as the AP and WAP5805 in client mode as the wireless client which connects to a notebook.

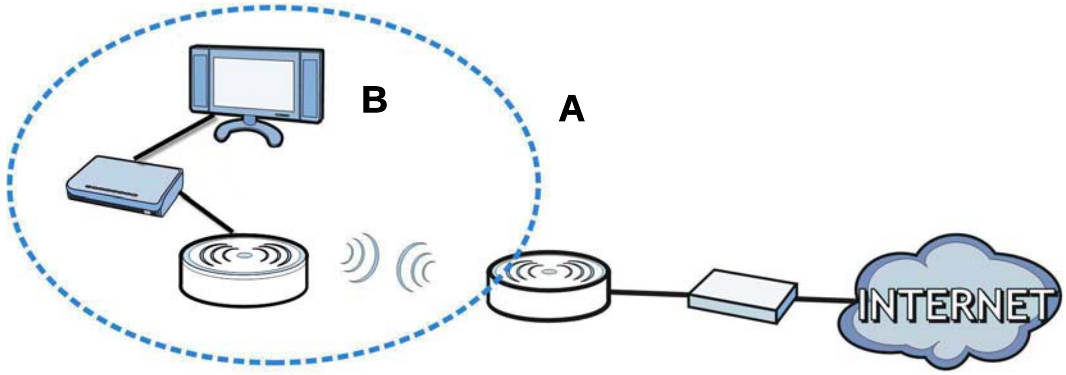
There are two WPS methods for creating a secure connection. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See Section 4.2.2 on page 24.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 WAP5805's interface. See Section 4.2.3 on page 25. This is the more secure method, since one device can authenticate the other.

4.2.1 Connecting to the Internet from an Access Point

This section gives you an example of how to set up an access point (**A**) and wireless client (**B** in this example) for wireless communication. Computers that connect to **B** can access the Internet through the access point wirelessly.

Figure 10 Wireless Access Point Connection to the Internet



4.2.2 Push Button Configuration (PBC)

1 Make sure that your WAP5805s are turned on and that they are within range of each other.

2 Make sure the WPS ( ) buttons of both WAP5805s are on.

3 Press the WPS buttons for more than three seconds. The WPS LEDs blink.

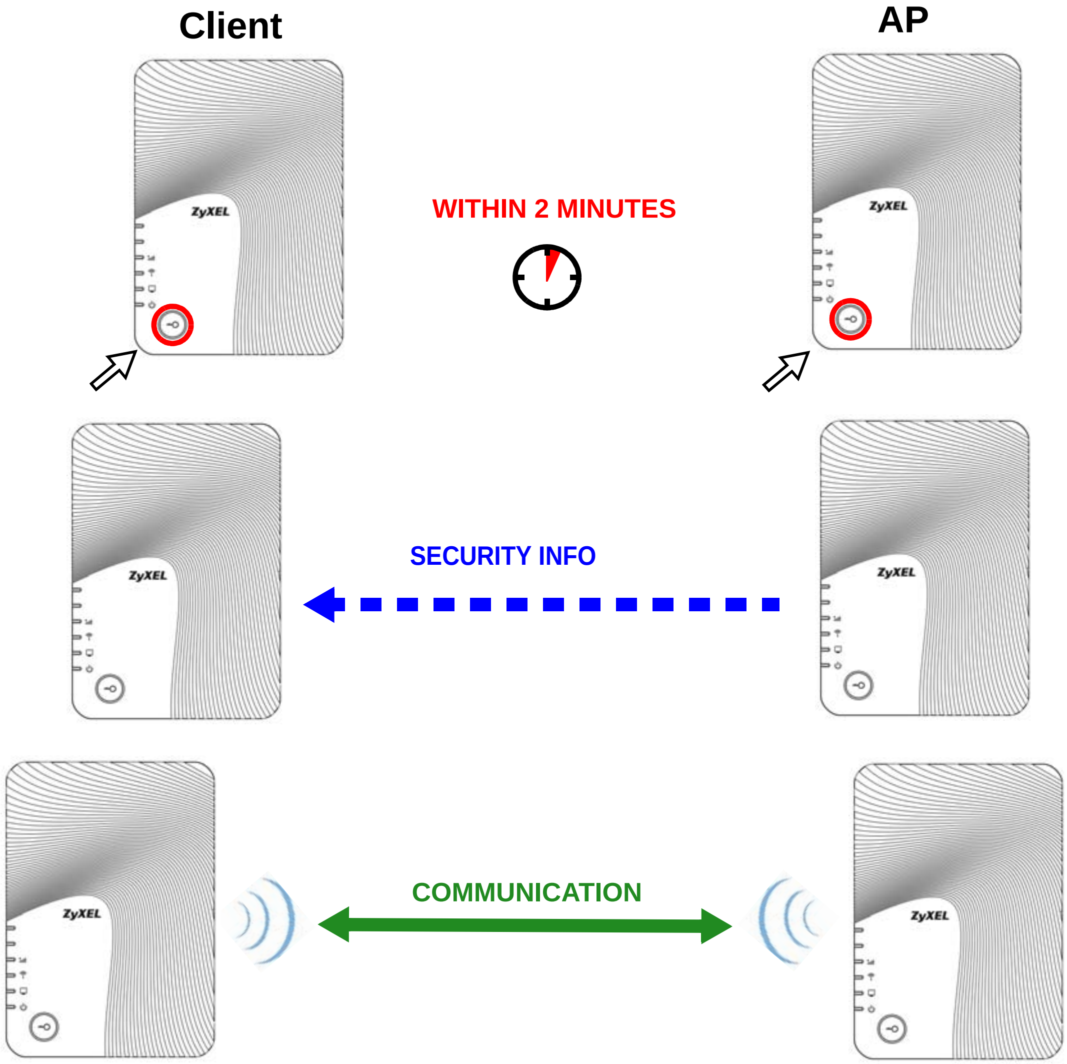
Note: It doesn’t matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

Note: Your WAP5805 has a WPS button located on its panel, as well as a WPS button in its Web Configurator. Both buttons have exactly the same function; you can also log into the Web Configurator and press the **Push Button** in the AP’s **Configuration > Network > Wireless LAN > WPS Station** screen and the **PBC Start** button in the client’s **Configuration > Network > Wireless LAN > WPS** screen.

The AP 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 AP securely.

The following figure shows you how to set up wireless network and security by pressing a button on both AP and wireless client.

Figure 11 Example WPS Process: PBC Method



4.2.3 PIN Configuration

When you use the PIN configuration method, you need to use configuration interfaces of both AP and client.

1 Log into the client's Web Configurator. Go to the **Configuration > Network > Wireless LAN > WPS** screen to get a PIN number.

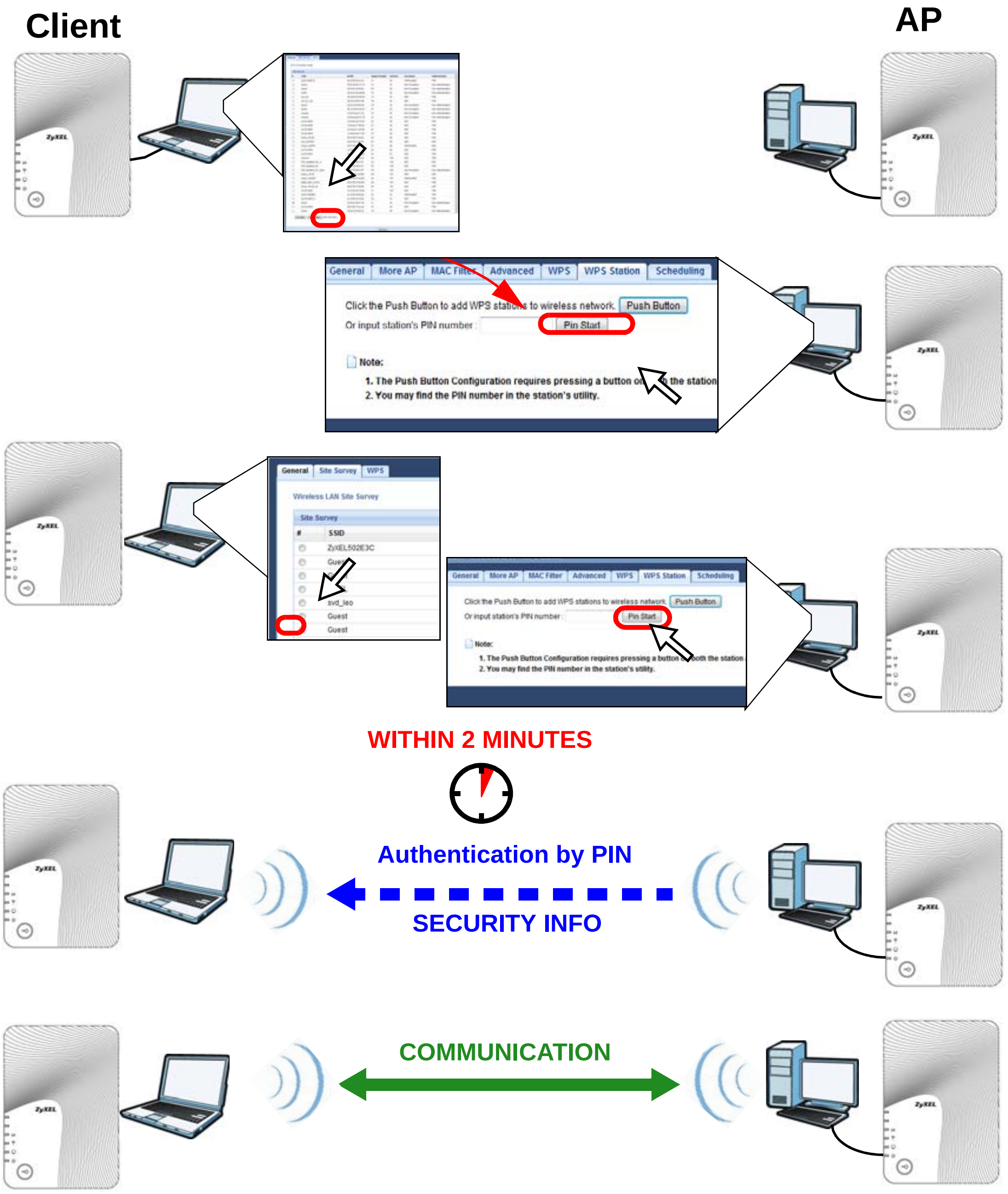
2 Log into the AP's Web Configurator. Enter the client's PIN number to the **PIN** field in the **Configuration > Network** > **Wireless LAN** > **WPS Station** screen.

3 Click the **PIN Start** button in the client's **WPS** screen and the **start** button in the AP's **WPS Station** screen within two minutes.

The AP 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 AP securely.

The following figure shows you how to set up wireless network and security on AP and wireless client by using PIN method.

Figure 12 Example WPS Process: PIN Method



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

Or input station's PIN number :

Note:

1. The Push Button Configuration requires pressing a button on both the station

2. You may find the PIN number in the station's utility.

4.3 Configuring AP - Client Wireless Connection Using the Expert Mode Screens

This example shows you how to configure wireless security settings with the following parameters on your WAP5805.

SSID	SSID_Example3
Channel	Auto
Security	WPA2-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

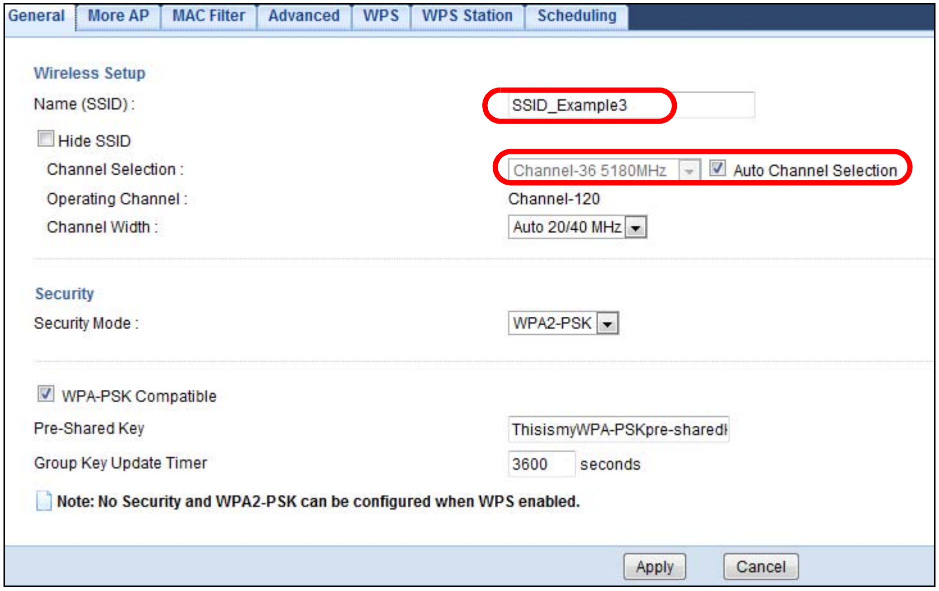
Follow the steps below to configure the wireless settings on your WAP5805.

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 3.2 on page 20).

1 Open the **Wireless LAN > General** screen in the AP's Web Configurator.

2 Enter **SSID_Example3** as the Name (SSID) and select a channel or select **Auto Channel Selection** to have the WAP5805 scans for and select an available channel automatically. Set security mode to **WPA2-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.

Figure 13 Tutorial: Network > Wireless LAN > General (AP)



Wireless Setup

Name (SSID) : SSID_Example3

□ Hide SSID

Channel Selection : Channel-36 5180MHz ☑ Auto Channel Selection

Operating Channel : Channel-120

Channel Width : Auto 20/40 MHz

Security

Security Mode : WPA2-PSK

☑ WPA-PSK Compatible

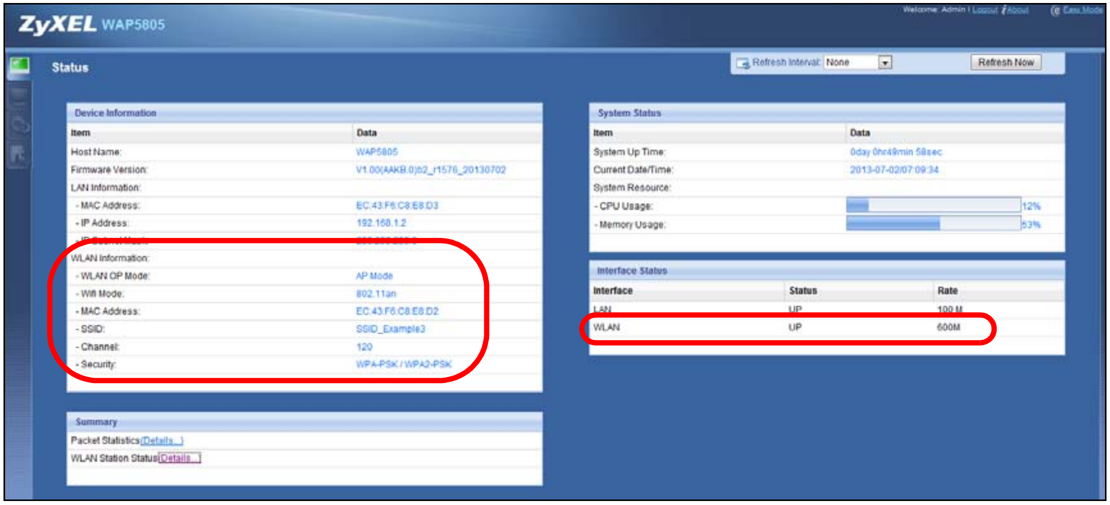
Pre-Shared Key ThisismyWPA-PSKpre-sharedk

Group Key Update Timer 3600 seconds

Note: No Security and WPA2-PSK can be configured when WPS enabled.

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

Figure 14 Tutorial: Checking Wireless Settings



Device Information

Item	Data
Host Name:	WAP5805
Firmware Version:	V1.00(AAKB.0)b2_r1576_20130702
LAN Information:	
- MAC Address:	EC:43:F6:C8:E8:D3
- IP Address:	192.168.1.2
- IP Subnet Mask:	255.255.255.0
WLAN Information:	
- WLAN OP Mode:	AP Mode
- Wifi Mode:	802.11an
- MAC Address:	EC:43:F6:C8:E8:D2
- SSID:	SSID_Example3
- Channel:	120
- Security:	WPA-PSK / WPA2-PSK

System Status

Item	Data
System Up Time:	0day 0hr49min 58sec
Current Date/Time:	2013-07-02/07:09:34
System Resource:	
- CPU Usage:	12%
- Memory Usage:	53%

Interface Status

Interface	Status	Rate
LAN	UP	100 M
WLAN	UP	600M

Summary

Packet Statistics(Details...)

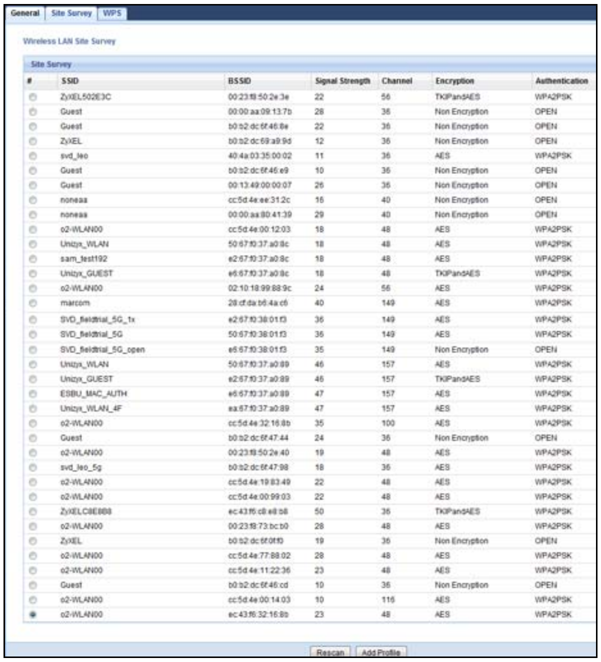
WLAN Station Status(Details...)

4.4 Connecting the WAP5805 Client to a WAP5805 AP

If you have an access point with Internet access deployed in your network already, and you want to use the WAP5805 as a wireless client to connect to the existing AP, set the WAP5805 to client mode. The WAP5805 then acts as a wireless client. Your device, such as a computer, can connect to the WAP5805 through a wired connection to access the Internet.

4.4.1 Connecting to a Wireless Network Using Site Survey

1 Go to **Configuration > Network > Wireless LAN > Site Survey**. The WAP5805 automatically scans for and connects to an available wireless network. Select a SSID's radio button and click **Add Profile** to add this wireless device to a profile.



Wireless LAN Site Survey

Site Survey

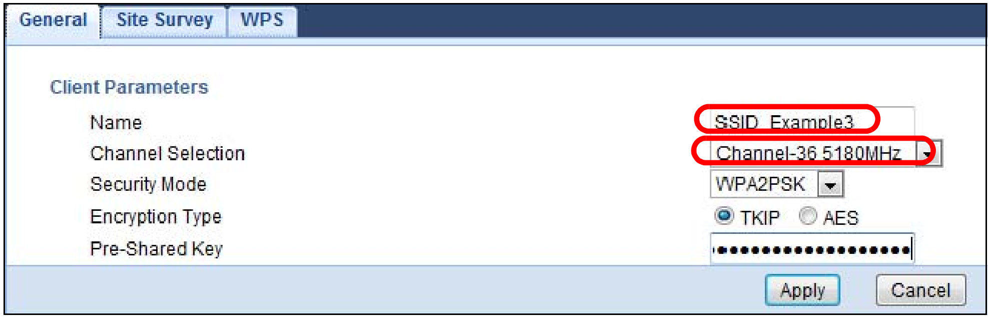
#	SSID	BSSID	Signal Strength	Channel	Encryption	Authentication
○	ZyXEL502E3C	00:23:f8:50:2e:3e	22	56	TKIPandAES	WPA2PSK
○	Guest	00:00:aa:09:13:7b	28	36	Non Encryption	OPEN
○	Guest	b0:b2:dc:6f:46:8e	22	36	Non Encryption	OPEN
○	ZyXEL	b0:b2:dc:69:a9:9d	12	36	Non Encryption	OPEN
○	svd_leo	40:4a:03:35:00:02	11	36	AES	WPA2PSK
○	Guest	b0:b2:dc:6f:46:e9	10	36	Non Encryption	OPEN
○	Guest	00:13:49:00:00:07	26	36	Non Encryption	OPEN
○	noneaa	cc:5d:4e:ee:31:2c	16	40	Non Encryption	OPEN
○	noneaa	00:00:aa:80:41:39	29	40	Non Encryption	OPEN
○	o2-WLAN00	cc:5d:4e:00:12:03	18	48	AES	WPA2PSK
○	Unizyx_WLAN	50:67:f0:37:a0:8c	18	48	AES	WPA2PSK
○	sam_test192	e2:67:f0:37:a0:8c	18	48	AES	WPA2PSK
○	Unizyx_GUEST	e6:67:f0:37:a0:8c	18	48	TKIPandAES	WPA2PSK
○	o2-WLAN00	02:10:18:99:88:9c	24	56	AES	WPA2PSK
○	marcom	28:cf:da:b6:4a:c6	40	149	AES	WPA2PSK
○	SVD_fieldtrial_5G_1x	e2:67:f0:38:01:f3	36	149	AES	WPA2PSK
○	SVD_fieldtrial_5G	50:67:f0:38:01:f3	36	149	AES	WPA2PSK
○	SVD_fieldtrial_5G_open	e6:67:f0:38:01:f3	35	149	Non Encryption	OPEN
○	Unizyx_WLAN	50:67:f0:37:a0:89	46	157	AES	WPA2PSK
○	Unizyx_GUEST	e2:67:f0:37:a0:89	46	157	TKIPandAES	WPA2PSK
○	ESBU_MAC_AUTH	e6:67:f0:37:a0:89	47	157	AES	WPA2PSK
○	Unizyx_WLAN_4F	ea:67:f0:37:a0:89	47	157	AES	WPA2PSK
○	o2-WLAN00	cc:5d:4e:32:16:8b	35	100	AES	WPA2PSK
○	Guest	b0:b2:dc:6f:47:44	24	36	Non Encryption	OPEN
○	o2-WLAN00	00:23:f8:50:2e:40	19	48	AES	WPA2PSK
○	svd_leo_5g	b0:b2:dc:6f:47:98	18	36	AES	WPA2PSK
○	o2-WLAN00	cc:5d:4e:19:83:49	22	48	AES	WPA2PSK
○	o2-WLAN00	cc:5d:4e:00:99:03	22	48	AES	WPA2PSK
○	ZyXELC8E8B8	ec:43:f6:c8:e8:b8	50	36	TKIPandAES	WPA2PSK
○	o2-WLAN00	00:23:f8:73:bc:b0	28	48	AES	WPA2PSK
○	ZyXEL	b0:b2:dc:6f:0f:f0	19	36	Non Encryption	OPEN
○	o2-WLAN00	cc:5d:4e:77:88:02	28	48	AES	WPA2PSK
○	o2-WLAN00	cc:5d:4e:11:22:36	23	48	AES	WPA2PSK
○	Guest	b0:b2:dc:6f:46:cd	10	36	Non Encryption	OPEN
○	o2-WLAN00	cc:5d:4e:00:14:03	10	116	AES	WPA2PSK
●	o2-WLAN00	ec:43:f6:32:16:8b	23	48	AES	WPA2PSK

4.4.2 Configuring Your Wireless Client

1 Open the **Wireless LAN > General** screen for WAP5805 in Client mode Web Configurator.

2 Enter **SSID_Example3** as the **Name** and select a channel in **Channel Selection** to have the WAP5805 scans for that available channel. Set security mode to **WPA2PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.

Figure 15 Tutorial: Network > Wireless LAN > General (Client)



Client Parameters

Name	SSID_Example3
Channel Selection	Channel-36 5180MHz
Security Mode	WPA2PSK
Encryption Type	● TKIP ○ AES
Pre-Shared Key	•••••••••••••••••••

PART II

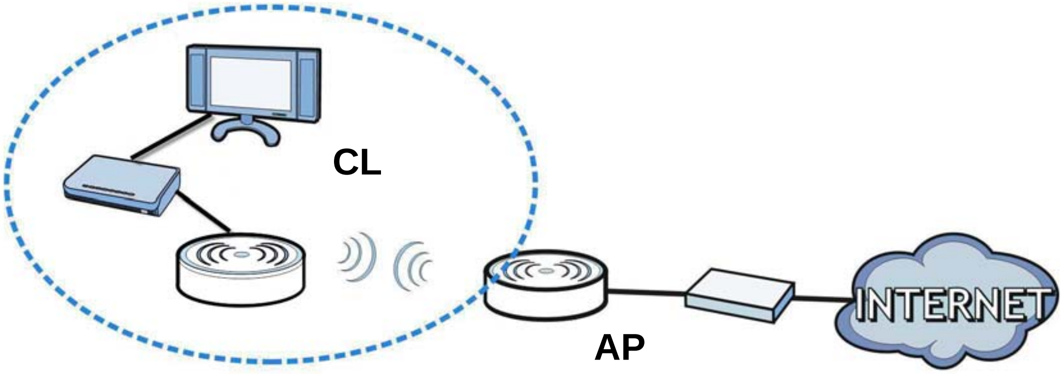
Technical Reference: Expert Mode

Access Point Expert Mode

5.1 Overview

The WAP5805 is set to one single package. In Access Point mode your WAP5805 bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet. See the figure below for an example.

Figure 16 Wireless Internet Access in Access Point Mode



Note: See Chapter 4 on page 23 for an example of setting up a wireless network in Access Point mode.

5.2 What You Can Do

- Use the **Status** screen (Section 5.5 on page 34) to view read-only information about your WAP5805.
- Use the **LAN** screen (Chapter 10 on page 79) to set the IP address for your WAP5805 acting as an access point.
- Use the **Wireless LAN** screens (Chapter 8 on page 46) to configure the wireless settings and wireless security between the wireless clients and the WAP5805.

5.3 What You Need to Know

See Chapter 4 on page 23 for a tutorial on setting up a network with the WAP5805 as an access point.

5.3.1 Configuring your WLAN, LAN and Maintenance Settings

- See Chapter 8 on page 46 and Chapter 10 on page 79 for information on the configuring your wireless network and LAN settings.
- See Chapter 10 on page 65 for information on configuring your Maintenance settings.

5.4 Setting your WAP5805 to AP Mode

1 To set your WAP5805 to AP mode, see Section 2.1.3 on page 19.

2 Connect your computer to the LAN port of the WAP5805.

3 The default IP address of the WAP5805 in AP mode is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254", except for "192.168.1.10" since it is reserved for CL.

4 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see Appendix A on page 77 for information on changing your computer's IP address.

5 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "http://192.168.1.2" as the web address in your web browser.

6 Enter "1234" (default) as the password and click **Login**.

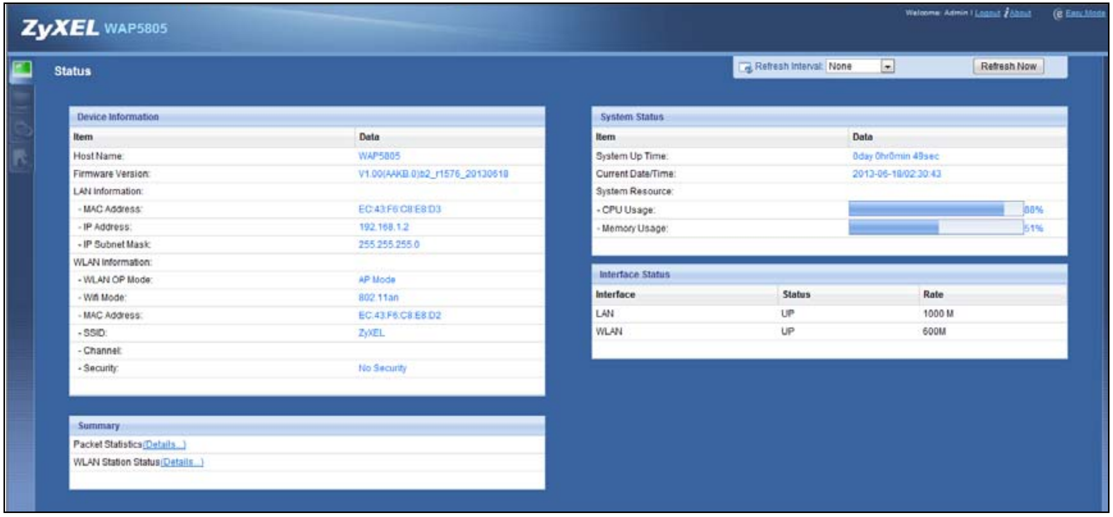
7 Type a new password and retype it to confirm, then click **Apply**. Otherwise, click **Ignore**.

8 The Easy mode appears. Click **Expert Mode** in the navigation panel.

5.5 AP Mode Status Screen

Click 🖥 to open the **Status** screen.

Figure 17 Status Screen: Access Point Mode



Device Information

Item	Data
Host Name:	WAP5805
Firmware Version:	V1.00(AAKB.0)b2_r1576_20130618
LAN Information:	
- MAC Address:	EC:43:F6:C8:E8:D3
- IP Address:	192.168.1.2
- IP Subnet Mask:	255.255.255.0
WLAN Information:	
- WLAN OP Mode:	AP Mode
- Wifi Mode:	802.11an
- MAC Address:	EC:43:F6:C8:E8:D2
- SSID:	ZyXEL
- Channel:	
- Security:	No Security

System Status

Item	Data
System Up Time:	0day 0hr0min 49sec
Current Date/Time:	2013-06-18/02:30:43
System Resource:	
- CPU Usage:	88%
- Memory Usage:	51%

Interface Status

Interface	Status	Rate
LAN	UP	1000 M
WLAN	UP	600M

Summary

Packet Statistics(Details...)
WLAN Station Status(Details...)

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

Table 6 Status Screen Icon Key: Access Point Mode

ICON	DESCRIPTION
About	Click this icon to view copyright and a link for related product information.
Refresh Interval: None	Select a number of seconds or **None** from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
Refresh Now	Click this button to refresh the status screen statistics.
🖥	Click this icon to see the **Status** page. The information in this screen depends on the device mode you select.
🖥	Click this icon to see the **Monitor** navigation menu.
⚙	Click this icon to see the **Configuration** navigation menu.
🔧	Click this icon to see the **Maintenance** navigation menu.

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

Table 7 Status Screen: Access Point Mode

LABEL	DESCRIPTION
Logout	Click this at any time to exit the Web Configurator.
Device Information	
Host Name	This is the WAP5805's model name.
Firmware Version	This is the firmware version.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.

Table 7 Status Screen: Access Point Mode (continued)

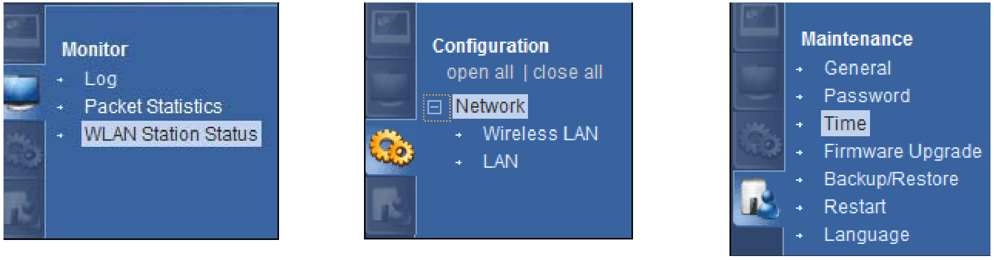
LABEL	DESCRIPTION
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
WLAN Information	
WLAN OP Mode	This is the device operating mode (Section 2.1.2 on page 18) to which the WAP5805's wireless LAN is set - **Access Point Mode**.
Wifi Mode	This is the wifi mode of your device.
MAC Address	This shows the wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the WAP5805 in the wireless LAN.
Channel	This shows the channel number which you select manually or the WAP5805 automatically scans and selects.
Security	This shows the level of wireless security the WAP5805 is using.
Summary	
Packet Statistics	Click **Details...** to go to the **Monitor > Packet Statistics** screen (Section 7.5 on page 44). Use this screen to view port status and packet specific statistics.
WLAN Station Status	Click **Details...** to go to the **Monitor > WLAN Station Status** screen (Section 7.6 on page 44). Use this screen to view the wireless stations that are currently associated to the WAP5805.
System Status	
Item	This column shows the type of data the WAP5805 is recording.
Data	This column shows the actual data recorded by the WAP5805.
System Up Time	This is the total time the WAP5805 has been on.
Current Date/Time	This field displays your WAP5805's present date and time.
System Resource	
CPU Usage	This displays what percentage of the WAP5805's processing ability is currently used. When this percentage is close to 100%, the WAP5805 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management.
Memory Usage	This shows what percentage of the heap memory the WAP5805 is using.
Interface Status	
Interface	This displays the WAP5805 port types. The port types are: **LAN** and **WLAN**.
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.

5.5.1 Navigation Panel

Use the menu in the navigation panel to configure WAP5805 features in Access Point mode.

The following screen and table show the features you can configure in Access Point mode.

Figure 18 Menu: Access Point Mode



The following table describes the sub-menus.

Table 8 Navigation Panel: Access Point Mode

LINK	TAB	FUNCTION
Status		This screen shows the WAP5805's general device, system and interface status information. Use this screen to access the summary statistics tables.
MONITOR		
Log	View Log	Use this screen to view the list of activities recorded by your WAP5805 and change your log settings.
	Log Settings	
Packet Statistics		Use this screen to view port status and packet specific statistics.
WLAN Station Status		Use this screen to view the wireless stations that are currently associated to the WAP5805.
CONFIGURATION		
Network		
Wireless LAN	General	Use this screen to configure general wireless LAN settings.
	More AP	Use this screen to configure AP settings.
	MAC Filter	Use the MAC filter screen to configure the WAP5805 to block access to devices or block the devices from accessing the WAP5805.
	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.
	IP Alias	Use this screen to have the WAP5805 apply IP alias to create LAN subnets.
MAINTENANCE		
General		Use this screen to view and change administrative settings such as system and domain names.
Password	Password Setup	Use this screen to change the password of your WAP5805.
Time	Time Setting	Use this screen to change your WAP5805's time and date.
Firmware Upgrade		Use this screen to upload firmware to your WAP5805.
Backup/ Restore		Use this screen to backup and restore the configuration or reset the factory defaults to your WAP5805.
Restart	System Restart	This screen allows you to reboot the WAP5805 without turning the power off.
Language		Select the language you want to use to configure the Web Configurator.

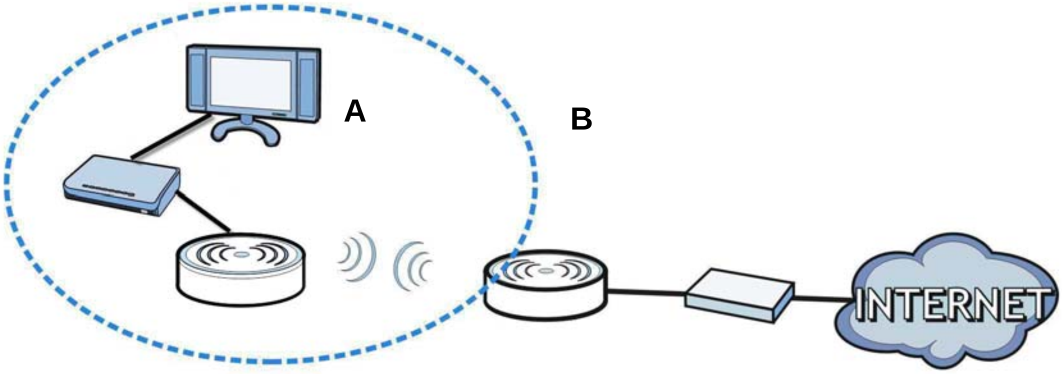
Client Expert Mode

6.1 Overview

Your WAP5805 can act as a wireless client. In wireless client mode, it can connect to an existing network via an access point. Use this mode if you already have a WAP5805 working as an access point in your network.

In the example below, one WAP5805 (**A**) is configured as a wireless client and another is used as an access point (**B**). The WAP5805 has only one client, supporting one LAN port, that needs to connect to the Internet. The WAP5805 wirelessly connects to the available access point (**B**).

Figure 19 Wireless Client Mode



After the WAP5805 and the access point connect, the WAP5805 acquires its WAN IP address from the access point. The clients of the WAP5805 can now surf the Internet.

6.2 What You Can Do

- Use the **Status** screen (Section 6.5 on page 39) to view read-only information about your WAP5805.
- Use the **LAN** screen (Chapter 10 on page 79) to set the IP address for your WAP5805.
- Use the **Wireless LAN** screen (Section 6.6 on page 40) to associate your WAP5805 (acting as a wireless client) with an existing access point.

6.3 What You Need to Know

With the exception of the **Wireless LAN** screens, the **LAN**, **Monitor**, and **Maintenance** screens in client mode are similar to the ones in access point Mode. See Chapter 8 on page 46 through Chapter 10 on page 65 of this User’s Guide.

6.4 Setting your WAP5805 to Client Mode

1 To set your WAP5805 to client mode, see Section 2.1.3 on page 19.

2 Connect your computer to the LAN port of the WAP5805.

3 The default IP address of the WAP5805 in client mode is “192.168.1.10”. In this case, your computer must have an IP address in the range between “192.168.1.3”and “192.168.1.254”, except “192.168.10”.

4 Click **Start > Run** on your computer in Windows. Type “cmd” in the dialog box. Enter “ipconfig” to show your computer’s IP address. If your computer’s IP address is not in the correct range then see Appendix A on page 77 for information on changing your computer’s IP address.

5 After you’ve set your computer’s IP address, open a web browser such as Internet Explorer and type “http://192.168.1.10” as the web address in your web browser.

6 Enter “1234” (default) as the password and click **Login**.

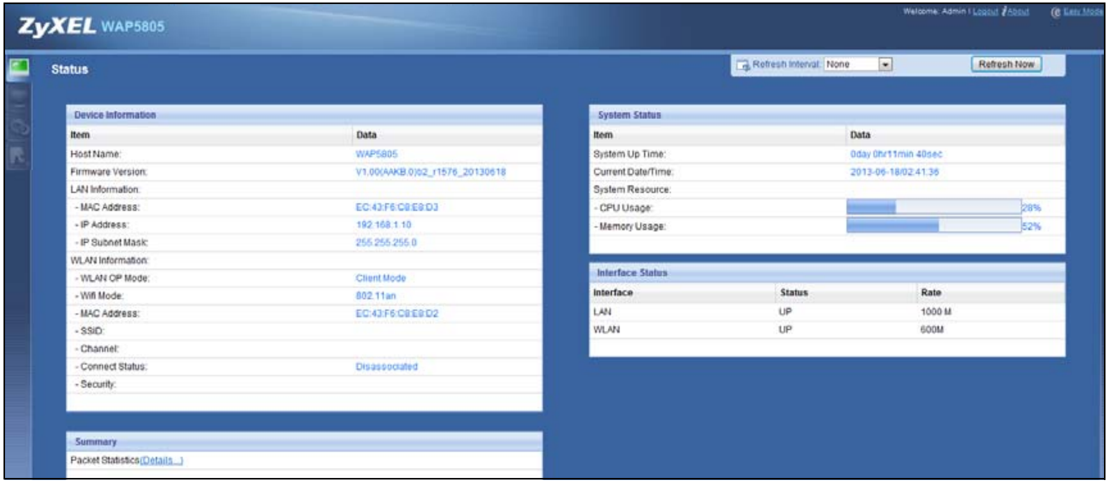
7 Type a new password and retype it to confirm, then click **Apply**. Otherwise, click **Ignore**.

8 The Easy mode appears. Click **Expert Mode** in the navigation panel.

6.5 Client Mode Status Screen

Click 🖥 to open the status screen.

Figure 20 Status: Client Mode



Device Information

Item	Data
Host Name:	WAP5805
Firmware Version:	V1.00(AAKB.0)02_r1576_20130618
LAN Information:	
- MAC Address:	EC:43:F6:C8:E8:D3
- IP Address:	192.168.1.10
- IP Subnet Mask:	255.255.255.0
WLAN Information:	
- WLAN OP Mode:	Client Mode
- Wifi Mode:	802.11an
- MAC Address:	EC:43:F6:C8:E8:D2
- SSID:	
- Channel:	
- Connect Status:	Disassociated
- Security:	

Summary

Packet Statistics(Details...)

System Status

Item	Data
System Up Time:	0day 0hr11min 40sec
Current Date/Time:	2013-06-18/02:41:36
System Resource:	
- CPU Usage:	28%
- Memory Usage:	52%

Interface Status

Interface	Status	Rate
LAN	UP	1000 M
WLAN	UP	600M

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

Table 9 Status Screen: Client Mode

LABEL	DESCRIPTION
Logout	Click this at any time to exit the Web Configurator.
Device Information	
Host Name	This is the WAP5805’s model name.
Firmware Version	This is the firmware version.
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.
WLAN Information	
WLAN OP Mode	This is the device operating mode (Section 2.1.2 on page 18) to which the WAP5805’s wireless LAN is set - **Client Mode**.
Wifi Mode	This is the wifi mode of your device.
MAC Address	This shows the wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the WAP5805 in the wireless LAN.
Channel	This shows the channel number used by the WAP5805 now.
Connect Status	This shows whether or not the WAP5805 has successfully associated with an access point - **Associated** or **Disassociated**.
Security	This shows the level of wireless security the WAP5805 is using.
Summary	
Packet Statistics	Click **Details...** to go to the **Monitor > Packet Statistics** screen (Section 7.5 on page 44). Use this screen to view port status and packet specific statistics.
System Status	
Item	This column shows the type of data the WAP5805 is recording.

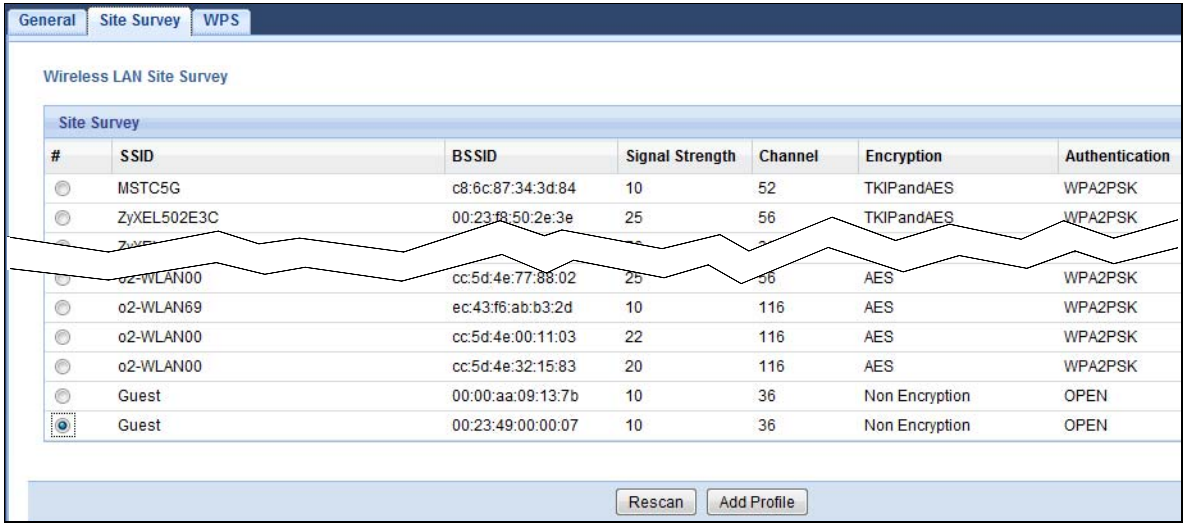
Table 9 Status Screen: Client Mode (continued)

LABEL	DESCRIPTION
Data	This column shows the actual data recorded by the WAP5805.
System Up Time	This is the total time the WAP5805 has been on.
Current Date/Time	This field displays your WAP5805's present date and time.
System Resource	
CPU Usage	This displays what percentage of the WAP5805's processing ability is currently used. When this percentage is close to 100%, the WAP5805 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management.
Memory Usage	This shows what percentage of the heap memory the WAP5805 is using.
Interface Status	
Interface	This displays the WAP5805 port types. The port types are: **LAN** and **WLAN**.
Status	For the LAN and WAN 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.

6.6 Wireless LAN Site Survey Screen

Use this screen to scan for and connect to a wireless network automatically. Go to **Configuration > Network > Wireless LAN > Site Survey** to open the following screen.

Figure 21 Client Mode: Configuration > Network > Wireless LAN > Site Survey



Wireless LAN Site Survey

Site Survey

#	SSID	BSSID	Signal Strength	Channel	Encryption	Authentication
○	MSTC5G	c8:6c:87:34:3d:84	10	52	TKIPandAES	WPA2PSK
○	ZyXEL502E3C	00:23:f8:50:2e:3e	25	56	TKIPandAES	WPA2PSK
○	o2-WLAN00	cc:5d:4e:77:88:02	25	56	AES	WPA2PSK
○	o2-WLAN69	ec:43:f6:ab:b3:2d	10	116	AES	WPA2PSK
○	o2-WLAN00	cc:5d:4e:00:11:03	22	116	AES	WPA2PSK
○	o2-WLAN00	cc:5d:4e:32:15:83	20	116	AES	WPA2PSK
○	Guest	00:00:aa:09:13:7b	10	36	Non Encryption	OPEN
●	Guest	00:23:49:00:00:07	10	36	Non Encryption	OPEN

The following table describes the labels in this screen.

Table 10 Client Mode: Configuration > Network > Wireless LAN > Site Survey

LABEL	DESCRIPTION
Site Survey	
#	Select a wireless device and click **Add Profile** to open a configuration screen where you can add the selected wireless device to a profile and then enable it.
SSID	This displays the SSID of the wireless device. ✓ indicates the wireless device is added to an activated profile and the WAP5805 is connecting to it.
BSSID	This displays the MAC address of the wireless device.
Signal Strength	This displays the strength of the wireless signal. The signal strength mainly depends on the antenna output power and the distance between your WAP5805 and this device.
Channel	This displays the channel number used by this wireless device.
Encryption	This displays the data encryption method used by this wireless device.
Authentication	This displays the authentication method used by this wireless device.
Rescan	Click this button to search for available wireless devices within transmission range and update this table.
Add Profile	Select a wireless device and click this button to add it to a profile.

6.7 Expert Mode

The following **Monitor**, **Configuration**, and **Maintenance** screens are in **AP Expert Mode** since all **CL Expert Mode** screens appear in **AP Expert Mode** (see Section Table 9 on page 39 and Section Table 8 on page 36 for comparison).

7

Monitor

7.1 Overview

This chapter discusses read-only information related to the device state of the WAP5805.

Note: To access the Monitor screens, you can also click the links in the Summary table of the Status screen to view the packets sent/received as well as the status of clients connected to the WAP5805.

7.2 What You Can Do

- Use the **View Log** screen (Section 7.3 on page 42) to see the logs for the categories that you selected in the **Log Setting** screen.
- Use the **Log Setting** screen (Section 7.4 on page 43) to configure which logs and/or immediate alerts the WAP5805 is to record.
- use the **Packet Statistics** screen (Section 7.5 on page 44) to view port status, packet specific statistics, the "system up time" and so on.
- Use the **WLAN Station Status** screen (Section 7.6 on page 44) to view the wireless stations that are currently associated to the WAP5805.

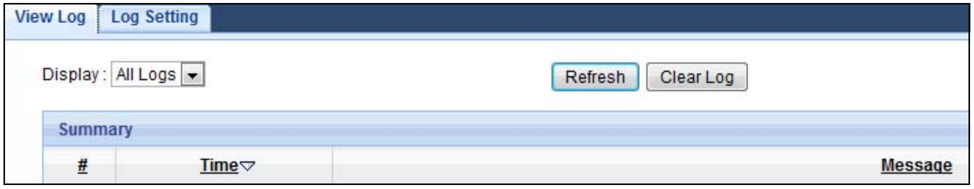
7.3 View Log

Use the **View Log** screen to see the logged messages for the WAP5805.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills.

Click **Monitor** > **Log**.

Figure 22 Monitor > Log



The following table describes the labels in this screen.

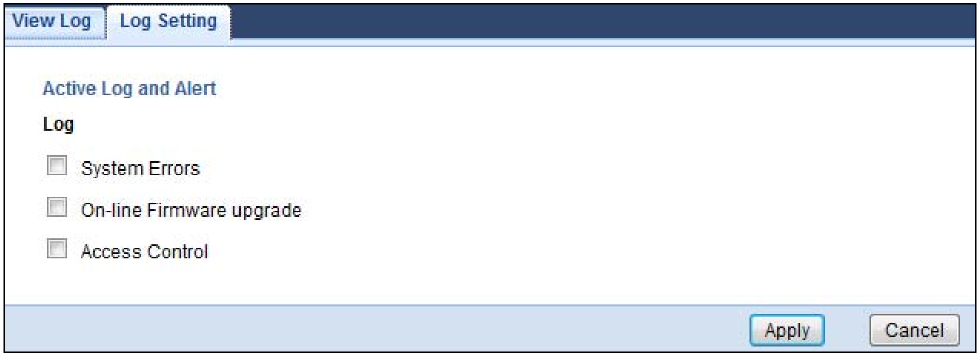
Table 11 Monitor > Log

LABEL	DESCRIPTION
Display	Select a category of logs to view. Select **All logs** to view logs from all of the log categories that you selected in the **Log Settings** screen.
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.

7.4 Log Setting

Use the **Log Setting** screen to choose which categories of events and/or alerts the WAP5805 is to log and then display the logs. To change your WAP5805's log settings, click **Monitor > Log** > **Log Setting**. The screen appears as shown.

Figure 23 Monitor > Log > Log Setting



□ System Errors

□ On-line Firmware upgrade

□ Access Control

The following table describes the labels in this screen.

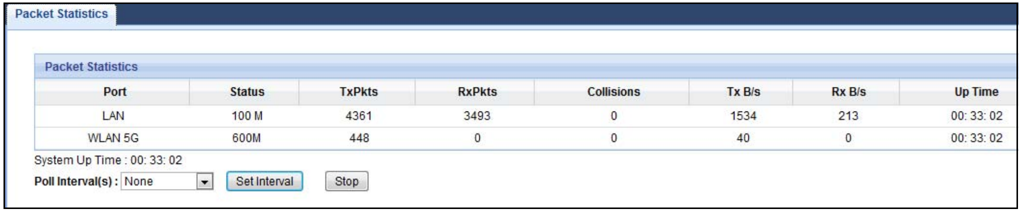
Table 12 Monitor > Log > Log Setting

LABEL	DESCRIPTION
System Errors	Select this category of logs to view system errors.
On-line Firmware upgrade	Select this category of logs to view firmware upgrade on-line.
Access Control	Select this category of logs to access control.
Apply	Click **Apply** to view results.
Cancel	Click **Cancel** to discard the changes.

7.5 Packet Statistics

Click the **Packet Statistics (Details...)** hyperlink in the **Status** screen or **Monitor** > **Packet Statistics**. Read-only information here includes port status, packet specific statistics and the "system up time". The **Poll Interval(s)** field is configurable and is used for refreshing the screen.

Figure 24 Monitor > Packet Statistics



Packet Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
LAN	100 M	4361	3493	0	1534	213	00: 33: 02
WLAN 5G	600M	448	0	0	40	0	00: 33: 02

System Up Time : 00: 33: 02

Poll Interval(s) : None

The following table describes the labels in this screen.

Table 13 Monitor > Packet Statistics

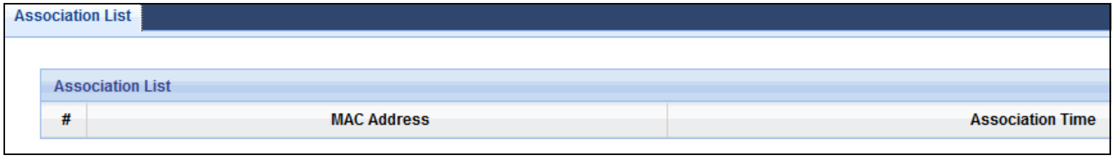
LABEL	DESCRIPTION
Port	This is the WAP5805’s port type.
Status	For the LAN ports, this displays the port speed or **Down** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **Down** when the WLAN is disabled.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total time the WAP5805 has been for each session.
System Up Time	This is the total time the WAP5805 has been on.
Poll Interval(s)	Enter the time interval in seconds for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics.

7.6 WLAN Station Status

Click the **WLAN Station Status (Details...)** hyperlink in the **Status** screen or **Monitor** > **WLAN Station Status**. View the wireless stations that are currently associated to the WAP5805 in the **Association List**. Association means that a wireless client (for example, your network or computer with a wireless network card) has connected successfully to the AP (or wireless router) using the same SSID, channel and security settings.

Note: This screen is not available when the WAP5805 is in Client mode.

Figure 25 Monitor > WLAN Station Status > Association List



The following table describes the labels in this screen.

Table 14 Monitor > WLAN Station Status > Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the WAP5805's WLAN network.

8

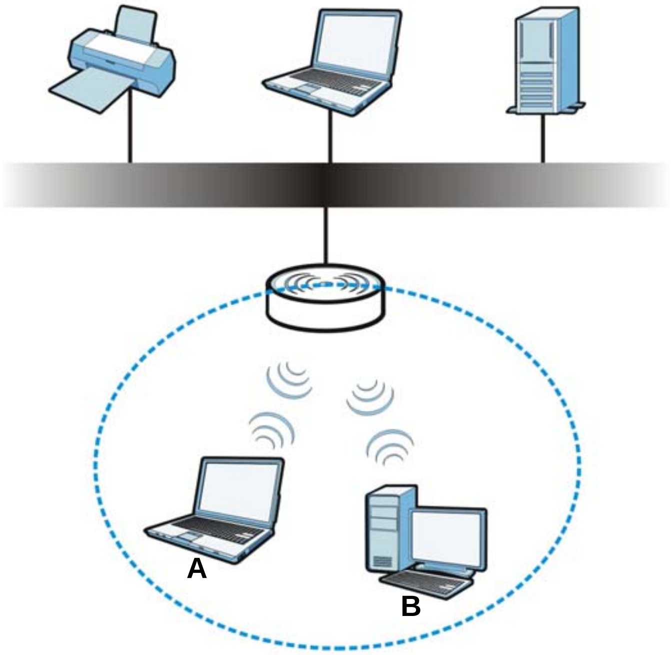
Wireless LAN

8.1 Overview

This chapter discusses how to configure the wireless network settings in your WAP5805. See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 26 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 WAP5805 is the AP.

8.2 What You Can Do

- Use the **General** screen (Section 8.4 on page 48) to enter the SSID, enable intra-BSS traffic and select the channel.
- Use the **More AP** screen (Section 8.4.1 on page 50) to configure AP settings through wireless setup and security.
- Use the **MAC Filter** screen (Section 8.6 on page 55) to allow or deny wireless stations based on their MAC addresses from connecting to the WAP5805.

- Use the **Advanced** screen (Section 8.7 on page 56) to configure wireless advanced features, such as set the RTS/CTS Threshold and HT physical mode.
- Use the **WPS** screen (Section 8.8 on page 57) to quickly set up a wireless network with strong security, without having to configure security settings manually.
- Use the **WPS Station** screen (Section 8.9 on page 58) to add a wireless station using WPS.
- Use the **Scheduling** screen (Section 8.10 on page 59) to set the times your wireless LAN is turned on and off.

8.3 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.

8.3.1 Wireless Security Overview

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

8.3.1.1 SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

8.3.1.2 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

[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.

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.

8.3.1.3 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.

The types of encryption you can choose depend on the type of user authentication.

Table 15 Types of Encryption for Each Type of Authentication

Weakest	**NO AUTHENTICATION**
↕	No Security
	WPA-PSK
Strongest	WPA2-PSK

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

When you select **WPA2-PSK** in your WAP5805, you can also select an option (**WPA Compatible**) to support WPA as well. In this case, if some wireless clients support WPA and some support WPA2, you should set up **WPA2-PSK** (depending on the type of wireless network login) and select the **WPA Compatible** option in the WAP5805.

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.

8.3.1.4 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 4.2 on page 23.

8.4 General Wireless LAN Screen

Use this screen to enter the SSID, select the channel and enable intra-BSS traffic.

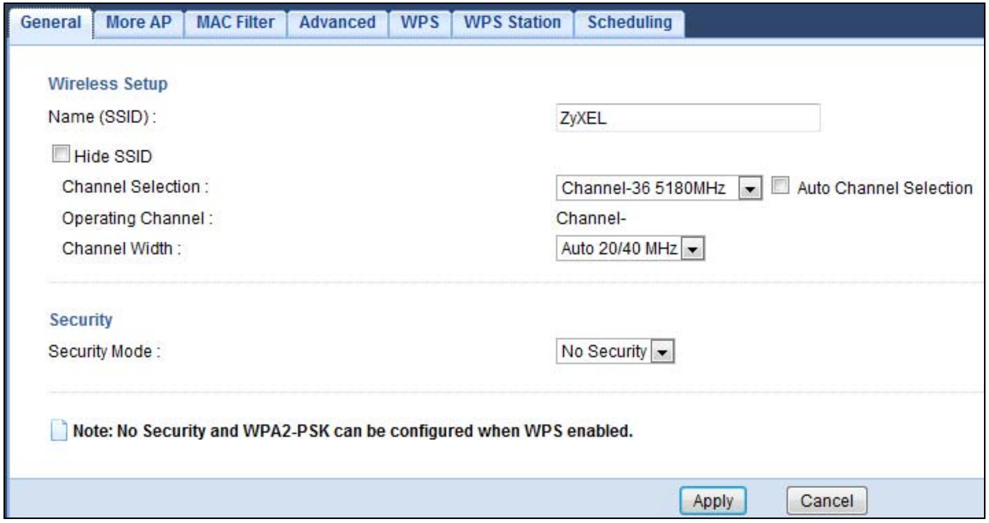
Note: If you are configuring the WAP5805 from a computer connected to the wireless LAN and you change the WAP5805's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the WAP5805's new settings.

Use this screen to select the wireless security mode for each SSID.

Click **Configuration > Network > Wireless LAN** to open the **General** screen. The screen varies depending on what you select in the **Security Mode** field. Select **No Security** to allow wireless clients to communicate with the access points without any data encryption.

Note: If you do not enable any wireless security on your WAP5805, your network is accessible to any wireless networking device that is within range.

Figure 27 Configuration > Network > Wireless LAN > General



Wireless Setup

Name (SSID) : ZyXEL

□ Hide SSID

Channel Selection : Channel-36 5180MHz □ Auto Channel Selection

Operating Channel : Channel-

Channel Width : Auto 20/40 MHz

Security

Security Mode : No Security

Note: No Security and WPA2-PSK can be configured when WPS enabled.

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

Table 16 Configuration > Network > Wireless LAN > General

LABEL	DESCRIPTION
Wireless Setup	
Wireless LAN	This is turned on by default. The current wireless state is reflected in this field.
Name (SSID)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a wireless client 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. This option is only available if **Auto Channel Selection** is disabled.
Auto Channel Selection	Select the check box to have the WAP5805 automatically scan for and select a channel which is not used by another device.

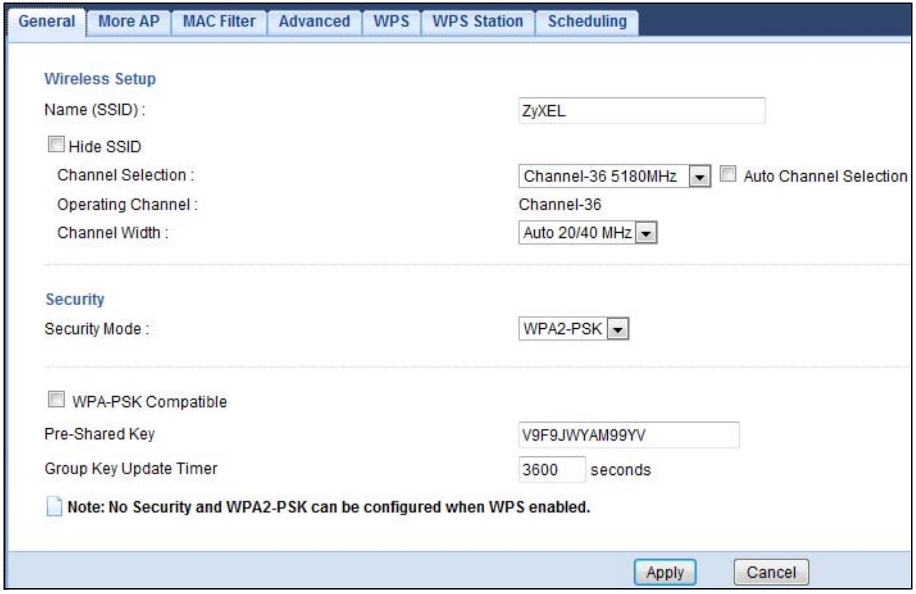
Table 16 Configuration > Network > Wireless LAN > General (continued)

LABEL	DESCRIPTION
Operating Channel	This displays the channel the WAP5805 is currently using.
Channel Width	Set the operating width of the channel depending on your particular region. The default is **Auto 20/40 MHz**.
Security	
Security Mode	Choose **No Security** from the drop-down list box.
Apply	Click **Apply** to save your changes back to the WAP5805.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

8.4.1 WPA2-PSK

Select **WPA2-PSK** from the **Security Mode** list.

Figure 28 Configuration > Network > Wireless LAN > General: Security



Wireless Setup

Name (SSID) : ZyXEL

□ Hide SSID

Channel Selection : Channel-36 5180MHz □ Auto Channel Selection

Operating Channel : Channel-36

Channel Width : Auto 20/40 MHz

Security

Security Mode : WPA2-PSK

□ WPA-PSK Compatible

Pre-Shared Key V9F9JWYAM99YV

Group Key Update Timer 3600 seconds

Note: No Security and WPA2-PSK can be configured when WPS enabled.

The following table describes the labels in this screen.

Table 17 Configuration > Network > Wireless LAN > General: Security

LABEL	DESCRIPTION
Wireless Setup	
Wireless LAN	This is turned on by default. The current wireless state is reflected in this field.
Name (SSID)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a wireless client cannot obtain the SSID through scanning using a site survey tool.

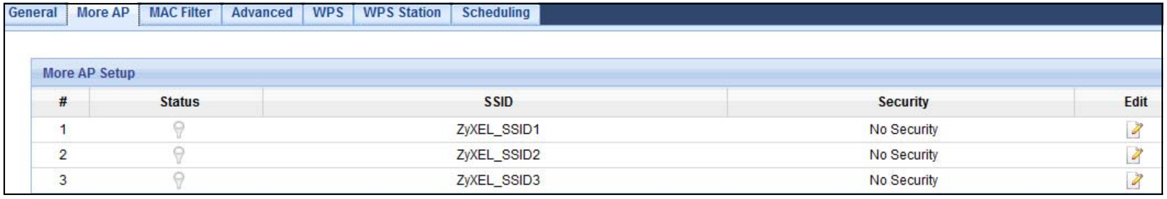
Table 17 Configuration > Network > Wireless LAN > General: Security

LABEL	DESCRIPTION
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. This option is only available if **Auto Channel Selection** is disabled.
Auto Channel Selection	Select the check box to have the WAP5805 automatically scan for and select a channel which is not used by another device.
Operating Channel	This displays the channel the WAP5805 is currently using.
Channel Width	Set the operating width of the channel depending on your particular region. The default is **Auto 20/40 MHz**.
Security	
Security Mode	Select **WPA2-PSK** to enable data encryption.
WPA-PSK Compatible	This field appears when you choose **WPA2-PSK** as the **Security Mode**. Check this field to allow wireless devices using **WPA2-PSK** security mode to connect to your WAP5805.
Pre-Shared Key	**WPA2-PSK** uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The default is **3600** seconds (60 minutes).
Apply	Click **Apply** to save your changes back to the WAP5805.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

8.5 AP Setup Screen

Use this screen to configure AP settings. Click **Configuration** > **Network** > **Wireless LAN** > **More AP** to open the **More AP Setup** screen.

Figure 29 Configuration > Network > Wireless LAN > More AP



More AP Setup

#	Status	SSID	Security	Edit
1		ZyXEL_SSID1	No Security	
2		ZyXEL_SSID2	No Security	
3		ZyXEL_SSID3	No Security	

The following table describes the labels in this screen.

Table 18 Configuration > Network > Wireless LAN > More AP

LABEL	DESCRIPTION
#	This field is a sequential value and is not associated with a specific entry.
Status	This field displays the status of the device: operating or not operating.
SSID	This displays the SSID of the wireless device.

Table 18 Configuration > Network > Wireless LAN > More AP

LABEL	DESCRIPTION
Security	This displays the security type of the wireless device.
Edit	Click this icon to modify settings.

8.5.1 Edit

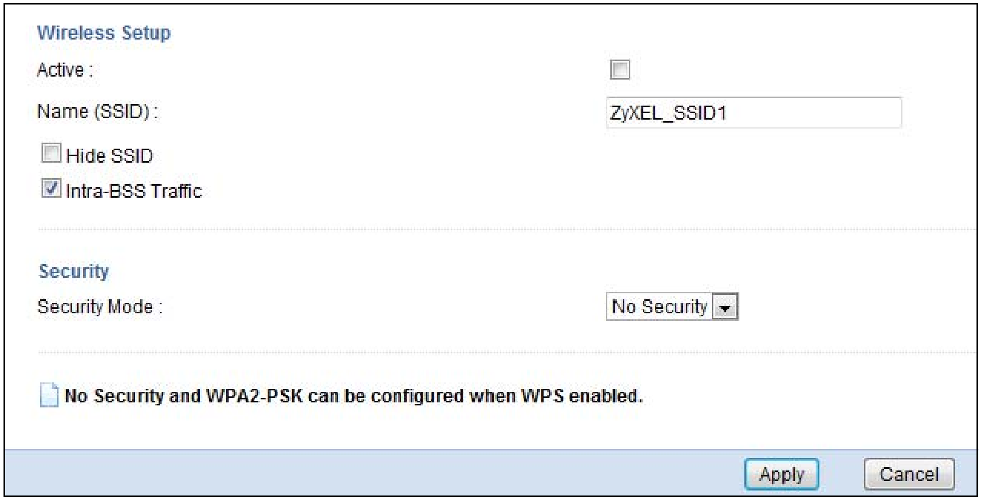
Click **Configuration > Network > Wireless LAN > More AP > Edit** to modify AP settings.

No Security

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

Note: If you do not enable any wireless security on your WAP5605, your network is accessible to any wireless networking device that is within range.

Figure 30 Configuration > Network > Wireless LAN > More AP > Edit: No Security



Wireless Setup

Active : □

Name (SSID) : ZyXEL_SSID1

□ Hide SSID

☑ Intra-BSS Traffic

Security

Security Mode : No Security

No Security and WPA2-PSK can be configured when WPS enabled.

The following table describes the labels in this screen.

Table 19 Configuration > Network > Wireless LAN > More AP > Edit: No Security

LABEL	DESCRIPTION
Wireless Setup	
Active	Select this check box to activate and start the process.
Name (SSID)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a wireless client cannot obtain the SSID through scanning using a site survey tool.
Intra-BSS Traffic	Select this check box to enable the traffic for Intra-BSS. Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless clients can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless clients can still access the wired network but cannot communicate with each other.

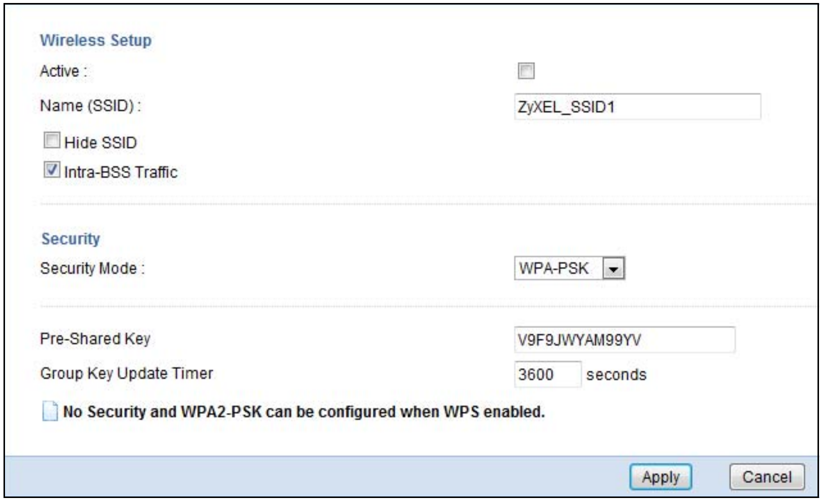
Table 19 Configuration > Network > Wireless LAN > More AP > Edit: No Security

LABEL	DESCRIPTION
Security	
Security Mode	Choose **No Security** from the drop-down list box.
Apply	Click **Apply** to save your changes back to the WAP5805.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

WPA-PSK

Select **WPA-PSK** from the **Security Mode** list.

Figure 31 Configuration > Network > Wireless LAN > More AP > Edit: WPA-PSK



Wireless Setup

Active : □

Name (SSID) : ZyXEL_SSID1

□ Hide SSID

☑ Intra-BSS Traffic

Security

Security Mode : WPA-PSK

Pre-Shared Key V9F9JWYAM99YV

Group Key Update Timer 3600 seconds

No Security and WPA2-PSK can be configured when WPS enabled.

The following table describes the labels in this screen.

Table 20 Configuration > Network > Wireless LAN > More AP > Edit: WPA-PSK

LABEL	DESCRIPTION
Wireless Setup	
Active	Select this check box to activate and start the process.
Name (SSID)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a wireless client cannot obtain the SSID through scanning using a site survey tool.
Intra-BSS Traffic	Select this check box to enable the traffic for Intra-BSS. Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless clients can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless clients can still access the wired network but cannot communicate with each other.
Security	
Security Mode	Select **WPA-PSK** to enable data encryption.
Pre-Shared Key	**WPA-PSK** uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.

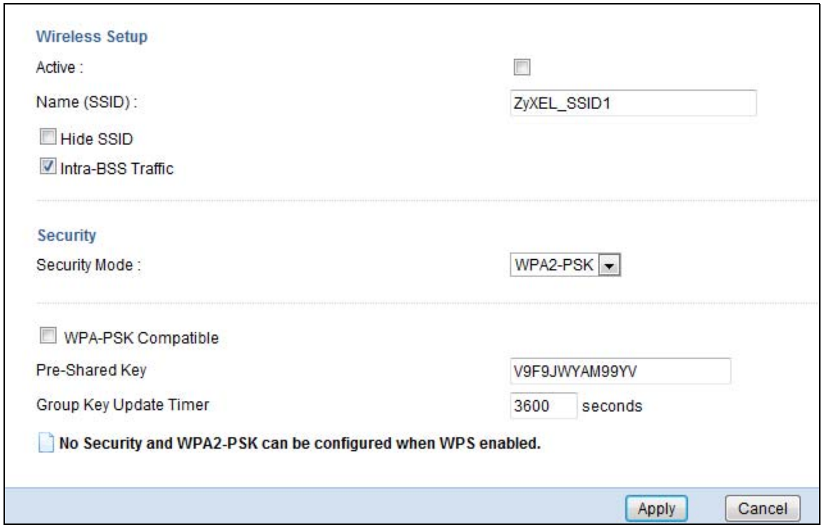
Table 20 Configuration > Network > Wireless LAN > More AP > Edit: WPA-PSK (continued)

LABEL	DESCRIPTION
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The default is **3600** seconds (60 minutes).
Apply	Click **Apply** to save your changes back to the WAP5805.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

WPA2-PSK

Select **WPA2-PSK** from the **Security Mode** list.

Figure 32 Configuration > Network > Wireless LAN > More AP > Edit: WPA2-PSK



Wireless Setup

Active : □

Name (SSID) : ZyXEL_SSID1

□ Hide SSID

☑ Intra-BSS Traffic

Security

Security Mode : WPA2-PSK

□ WPA-PSK Compatible

Pre-Shared Key V9F9JWYAM99YV

Group Key Update Timer 3600 seconds

No Security and WPA2-PSK can be configured when WPS enabled.

The following table describes the labels in this screen.

Table 21 Configuration > Network > Wireless LAN > More AP > Edit: WPA2-PSK

LABEL	DESCRIPTION
Wireless Setup	
Active	Select this check box to activate and start the process.
Name (SSID)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a wireless client cannot obtain the SSID through scanning using a site survey tool.
Intra-BSS Traffic	Select this check box to enable the traffic for Intra-BSS. Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless clients can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless clients can still access the wired network but cannot communicate with each other.
Security	
Security Mode	Select **WPA2-PSK** to enable data encryption.

Table 21 Configuration > Network > Wireless LAN > More AP > Edit: WPA2-PSK (continued)

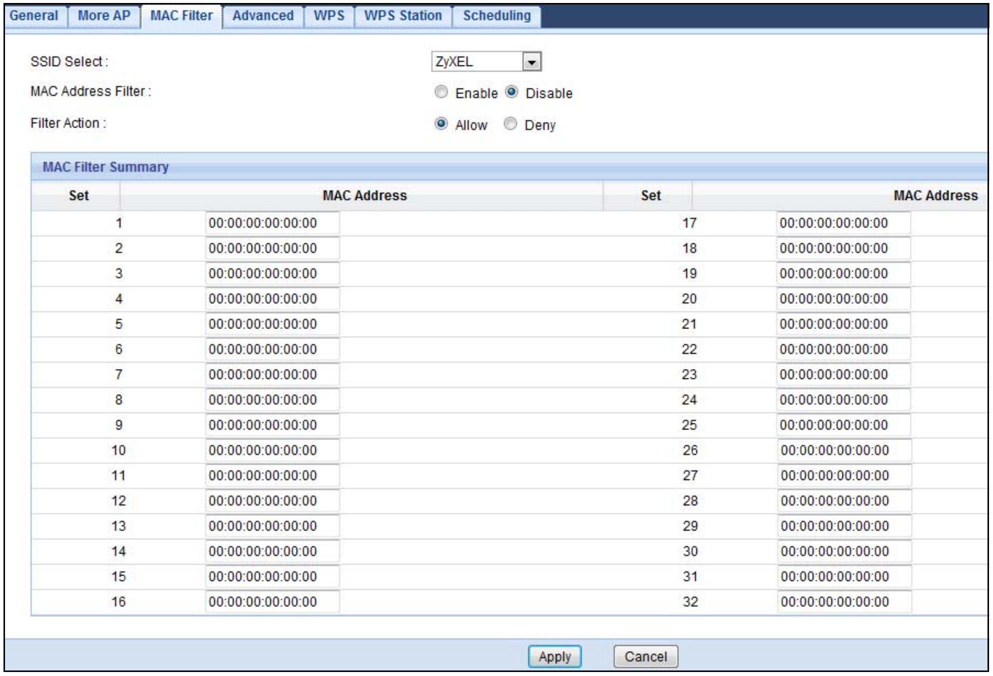
LABEL	DESCRIPTION
WPA-PSK Compatible	This field appears when you choose **WPA2-PSK** as the **Security Mode**. Check this field to allow wireless devices using **WPA2-PSK** security mode to connect to your WAP5805.
Pre-Shared Key	**WPA2-PSK** uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The default is **3600** seconds (60 minutes).
Apply	Click **Apply** to save your changes back to the WAP5805.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

8.6 MAC Filter

The MAC filter screen allows you to configure the WAP5805 to give exclusive access to devices (Allow) or exclude devices from accessing the WAP5805 (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 WAP5805’s MAC filter settings, click **Configuration > Network** > **Wireless LAN** > **MAC Filter**. The screen appears as shown.

Figure 33 Configuration > Network > Wireless LAN > MAC Filter



SSID Select : ZyXEL

MAC Address Filter : ○ Enable ● Disable

Filter Action : ● Allow ○ Deny

MAC Filter Summary

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

The following table describes the labels in this menu.

Table 22 Configuration > Network > Wireless LAN > MAC Filter

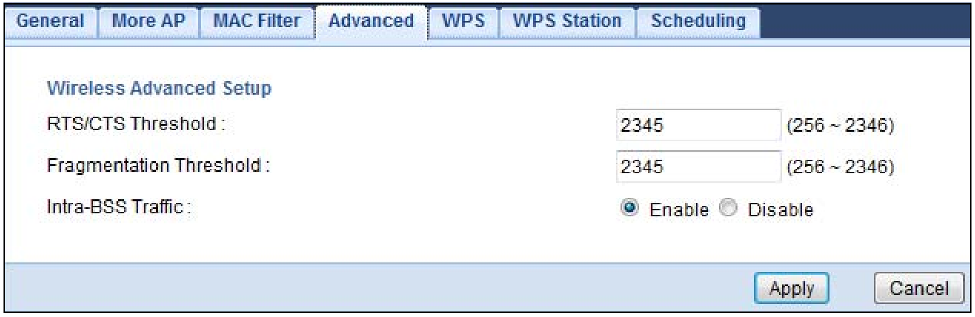
LABEL	DESCRIPTION
SSID	Select the SSID for which you want to configure MAC filtering.
MAC Address Filter	You can use the MAC address filter to tell the AP which wireless clients are allowed or not allowed to use the wireless network. If a wireless client is allowed to use the wireless network, it still 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.
Filter Action	Choose from **Allow** or **Deny** for the filter action setting.
MAC Filter Summary	
Set	This field displays the set by number.
MAC Address	This is the MAC address of the wireless station that are allowed or denied access to the WAP5805.
Apply	Click **Apply** to save your changes back to the WAP5805.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

8.7 Wireless LAN Advanced Screen

Use this screen to allow wireless advanced features, such as the output power, RTS/CTS Threshold and high-throughput physical mode settings.

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

Figure 34 Configuration > Network > Wireless LAN > Advanced



Wireless Advanced Setup

RTS/CTS Threshold : 2345 (256 ~ 2346)

Fragmentation Threshold : 2345 (256 ~ 2346)

Intra-BSS Traffic : ● Enable ○ Disable

The following table describes the labels in this screen.

Table 23 Configuration > Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between **256** and **2346**.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between **256** and **2346**.

Table 23 Configuration > Network > Wireless LAN > Advanced

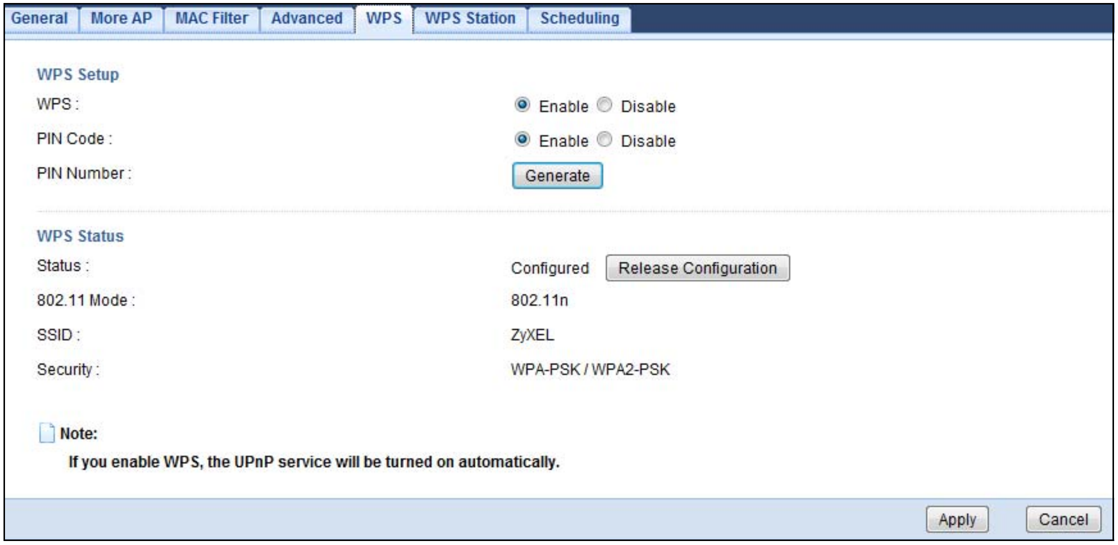
LABEL	DESCRIPTION
Intra-BSS Traffic	Select to enable or disable the traffic for Intra-BSS. Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless clients can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless clients can still access the wired network but cannot communicate with each other.
Apply	Click **Apply** to save your changes back to the WAP5805.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

8.8 TWPS 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 **Configuration > Network** > **Wireless LAN** > **WPS** tab.

Note: With WPS, wireless clients can only connect to the wireless network using the first SSID on the WAP5805.

Figure 35 Configuration > Network > Wireless LAN > WPS



WPS Setup

WPS : ● Enable ○ Disable

PIN Code : ● Enable ○ Disable

PIN Number :

WPS Status

Status : Configured

802.11 Mode : 802.11n

SSID : ZyXEL

Security : WPA-PSK / WPA2-PSK

Note:

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

The following table describes the labels in this screen.

Table 24 Configuration > Network > Wireless LAN > WPS

LABEL	DESCRIPTION
WPS Setup	
WPS	Select to enable or disable the WPS feature.
PIN Code	Select to enable or disable the PIN code.
PIN Number	This displays a PIN number last time system generated. Click **Generate** to generate a new PIN number.
WPS Status	

Table 24 Configuration > Network > Wireless LAN > WPS

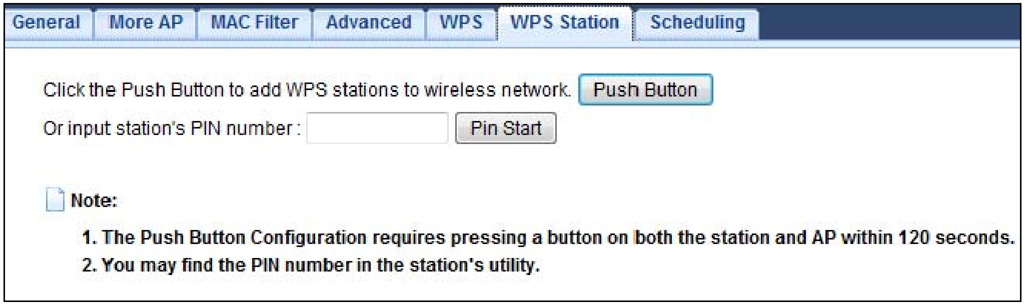
LABEL	DESCRIPTION
Status	This displays **Configured** when the WAP5805 has connected to a wireless network using WPS or when **Enable WPS** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Unconfigured** if WPS is disabled and there are no wireless or wireless security changes on the WAP5805 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 WAP5805.
802.11 Mode	This is the 802.11 mode used. Only compliant WLAN devices can associate with the WAP5805.
SSID	This is the name of the wireless network (the WAP5805's first SSID).
Security	This is the type of wireless security employed by the network.
Apply	Click **Apply** to save your changes back to the WAP5805.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

8.9 WPS Station Screen

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

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 36 Configuration > Network > Wireless LAN > WPS Station



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

Or input station's PIN number :

Note:

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

The following table describes the labels in this screen.

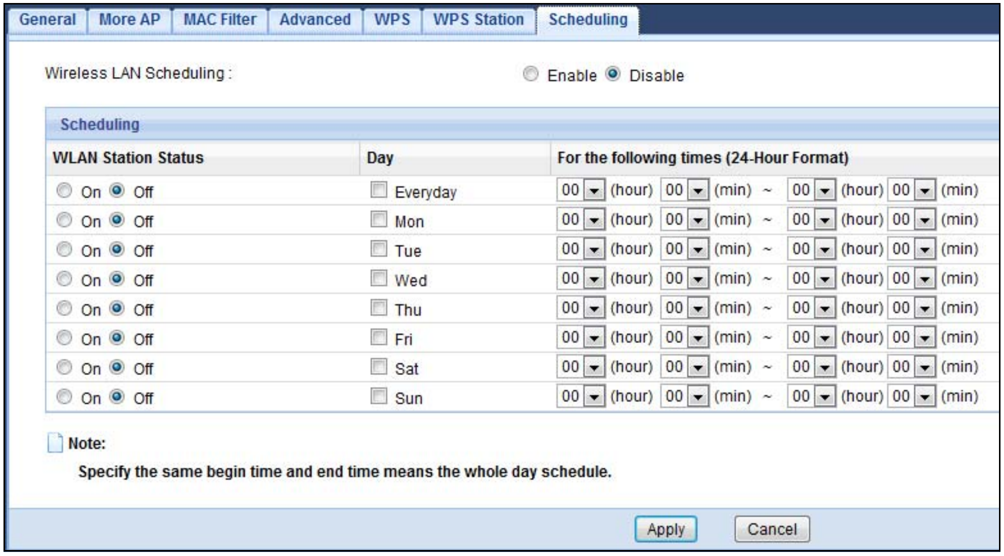
Table 25 Configuration > Network > Wireless LAN > WPS Station

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 4.2.2 on page 24. 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 4.2.3 on page 25. Type the same PIN number generated in the wireless station's utility. Then click **Pin Start** to associate to each other and perform the wireless security information synchronization.

8.10 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 **Configuration >Network** > **Wireless LAN** > **Scheduling** tab.

Figure 37 Configuration > Network > Wireless LAN > Scheduling



Wireless LAN Scheduling : ○ Enable ● Disable

Scheduling

WLAN Station Status	Day	For the following times (24-Hour Format)
○ On ● Off	□ Everyday	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Mon	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Tue	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Wed	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Thu	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Fri	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Sat	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Sun	00 (hour) 00 (min) ~ 00 (hour) 00 (min)

Note:

Specify the same begin time and end time means the whole day schedule.

The following table describes the labels in this screen.

Table 26 Configuration > Network > Wireless LAN > Scheduling

LABEL	DESCRIPTION
Wireless LAN Scheduling	Select this to enable or disable wireless LAN scheduling.
Scheduling	
WLAN Station Status	Select **On** or **Off** to specify whether the Wireless LAN is turned on or off. This field works in conjunction with the **Day** and **For the following times** fields.

Table 26 Configuration > Network > Wireless LAN > Scheduling (continued)

LABEL	DESCRIPTION
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 **For the following times** field.
For the following times (24-Hour Format)	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 on between the two times you enter in these fields. If you have chosen **Off** earlier for the WLAN Status the Wireless LAN will turn off between the two times you enter in these fields.
Apply	Click **Apply** to save your changes back to the WAP5805.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

9

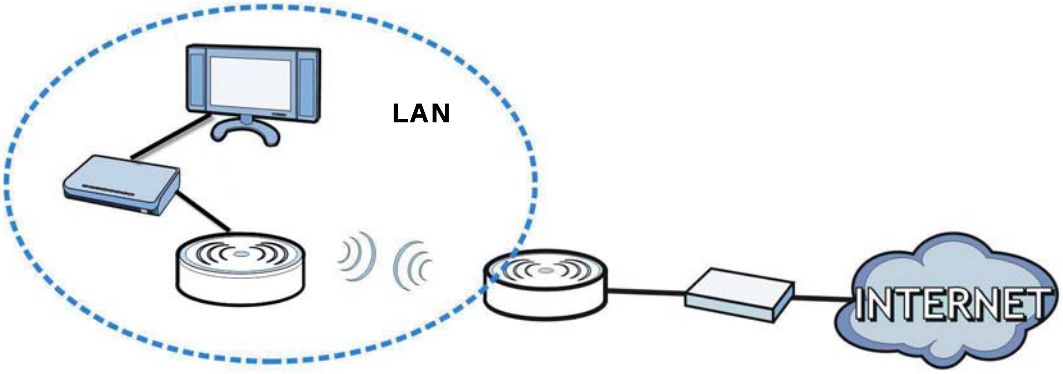
LAN

9.1 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 38 LAN Example



The LAN screens can help you manage IP addresses.

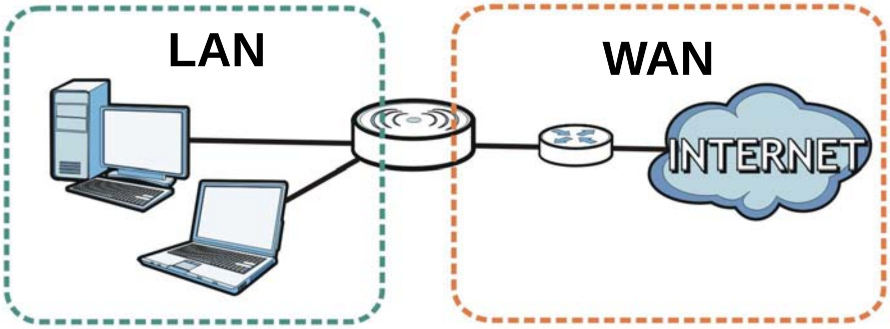
9.2 What You Can Do

- Use the **IP** screen (Section 9.4 on page 62) to change the IP address for your WAP5805 and DNS server information.
- Use the **IP Alias** screen (Section 9.5 on page 63) to have the WAP5805 apply IP alias to create LAN subnets.

9.3 What You Need To Know

There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 39 LAN and WAN IP Addresses



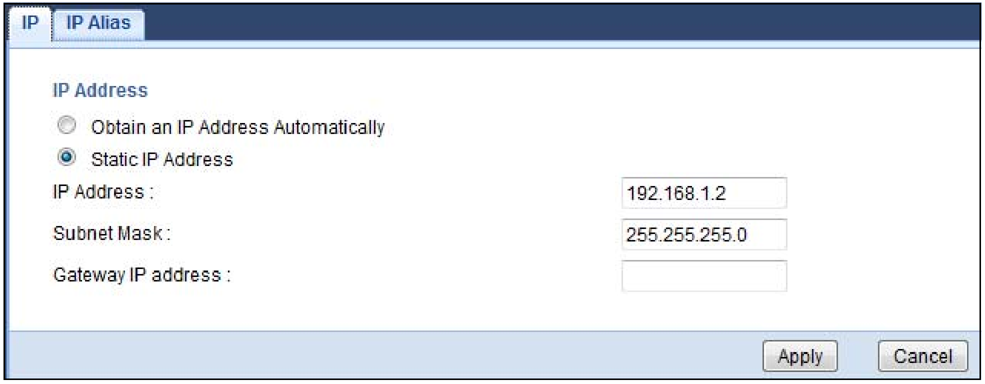
The LAN parameters of the WAP5805 are preset in the factory with the following values:

- AP mode: IP address of 192.168.1.2 with subnet mask of 255.255.255.0 (24 bits)
- Client mode: IP address of 192.168.1.10 with subnet mask of 255.255.255.0 (24 bits)

9.4 LAN IP Screen

Use this screen to change the IP address for your WAP5805. Click **Configuration > Network > LAN > IP**.

Figure 40 Configuration > Network > LAN > IP



IP Address

○ Obtain an IP Address Automatically

● Static IP Address

IP Address : 192.168.1.2

Subnet Mask : 255.255.255.0

Gateway IP address :

The following table describes the labels in this screen.

Table 27 Configuration > Network > LAN > IP

LABEL	DESCRIPTION
IP Address	
Obtain an IP Address Automatically	Click this to obtain an IP address automatically.
Static IP Address	Click this if you want a static IP address.

Table 27 Configuration > Network > LAN > IP

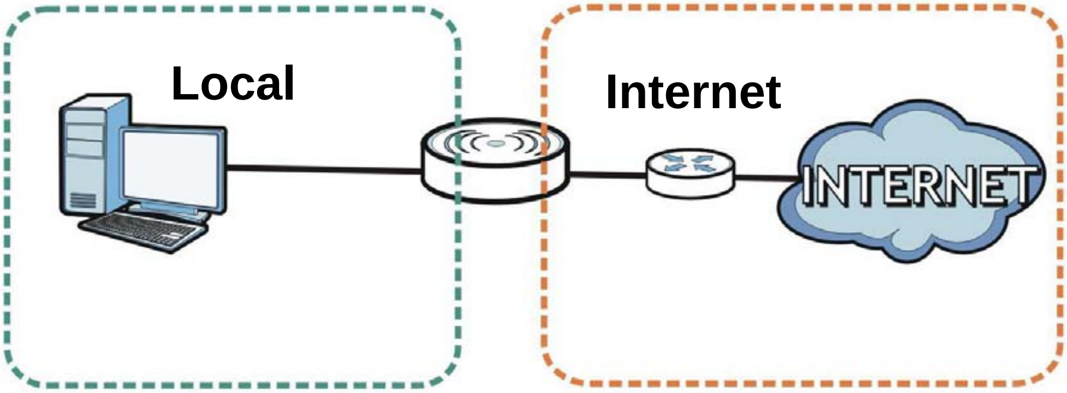
LABEL	DESCRIPTION
IP Address	Type the IP address in dotted decimal notation. If you change the IP address you will have to log in again with the new IP address.
Subnet Mask	The subnet mask specifies the network number portion of an IP address.
Gateway IP Address	Enter a gateway IP address (if your ISP or network administrator gave you one) in this field.
Apply	Click **Apply** to save your changes back to the WAP5805.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

9.5 IP Alias Screen

9.5.1 IP Alias

If you select **Obtain an IP Address Automatically** in **Configuration > Network > LAN > IP**, the WAP5805 is assigned a dynamic unknown IP address. The default IP address of 192.168.1.2 for AP mode and 192.168.1.10 for CL mode will no longer work.

Figure 41 Local and dynamic IP Addresses



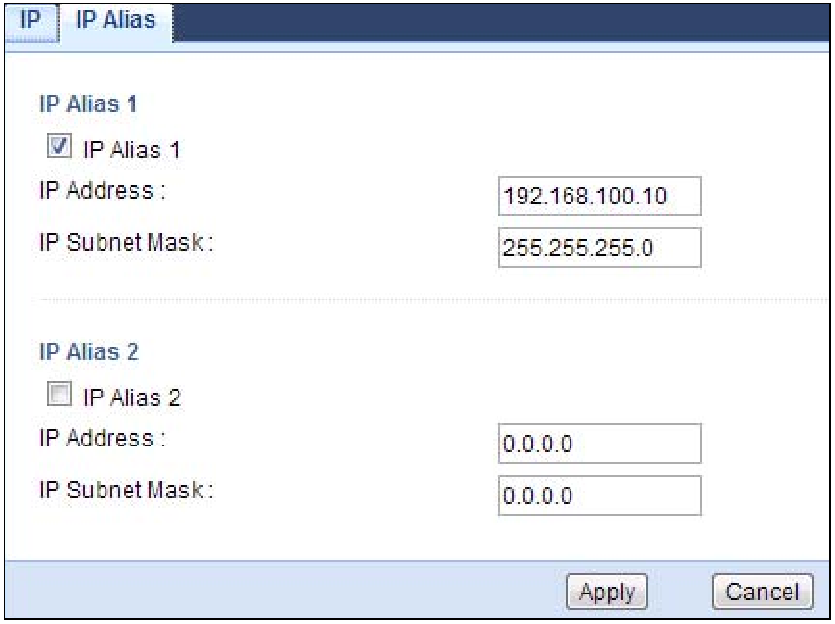
Alias IP allows you the access the WAP5805 from the local side from the following addresses:

- AP mode: alias IP address of 192.168.100.2 with subnet mask of 255.255.255.0 (24 bits)
- Client mode: alias IP address of 192.168.100.10 with subnet mask of 255.255.255.0 (24 bits)

To access the WAP5805 from the Internet side, you have to use the dynamically assigned IP address.

Click **Configuration > LAN** > **IP Alias**.

Figure 42 Configuration > Network > LAN > IP Alias



IP Alias 1

☑ IP Alias 1

IP Address : 192.168.100.10

IP Subnet Mask : 255.255.255.0

IP Alias 2

□ IP Alias 2

IP Address : 0.0.0.0

IP Subnet Mask : 0.0.0.0

The following table describes the labels in this screen.

Table 28 Configuration > Network > LAN > IP Alias

LABEL	DESCRIPTION
IP Alias 1	
IP Alias 1	Check this to enable IP alias. For the IP Alias, the default can be changed.
IP Address	Type the IP alias address of your WAP5805 in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address.
IP Alias 2	
IP Alias 2	Check this to enable IP alias. For the IP Alias, the default can be changed.
IP Address	Type the IP alias address of your WAP5805 in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address.
Apply	Click **Apply** to save your changes back to the WAP5805.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

Maintenance

10.1 Overview

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

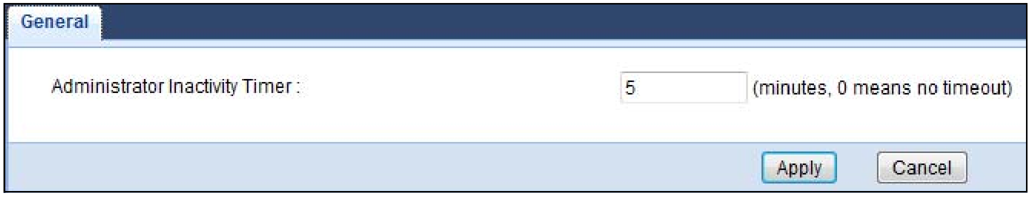
10.2 What You Can Do

- Use the **General** screen (Section 10.3 on page 65) to set the timeout period of the management session.
- Use the **Password** screen (Section 10.4 on page 66) to change your WAP5805's system password.
- Use the **Time** screen (Section 10.5 on page 67) to change your WAP5805's time and date.
- Use the **Firmware Upgrade** screen (Section 10.6 on page 68) to upload firmware to your WAP5805.
- Use the **Backup/Restore** screen (Section 10.8 on page 71) to view information related to factory defaults, backup configuration, and restoring configuration.
- Use the **Restart** screen (Section 10.8 on page 71) to reboot the WAP5805 without turning the power off.
- Use the **Language** screen (Section 10.9 on page 71) to reboot the WAP5805 without turning the power off.

10.3 General Screen

Use this screen to set the management session timeout period. Click **Maintenance** > **General**. The following screen displays.

Figure 43 Maintenance > General



General

Administrator Inactivity Timer : 5 (minutes, 0 means no timeout)

The following table describes the labels in this screen.

Table 29 Maintenance > General

LABEL	DESCRIPTION
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).
Apply	Click **Apply** to save your changes back to the WAP5805.
Cancel	Click **Cancel** to discard the changes.

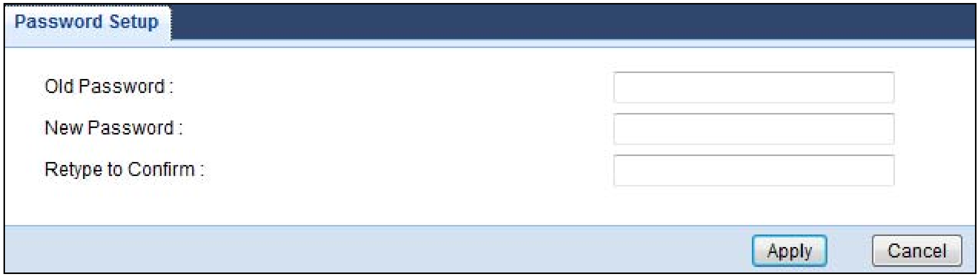
10.4 Password Screen

It is strongly recommended that you change your WAP5805's password.

If you forget your WAP5805's password (or IP address), you will need to reset the device. See Section 10.9 on page 71 for details

Click **Maintenance** > **Password**.

Figure 44 Maintenance > Password



The following table describes the labels in this screen.

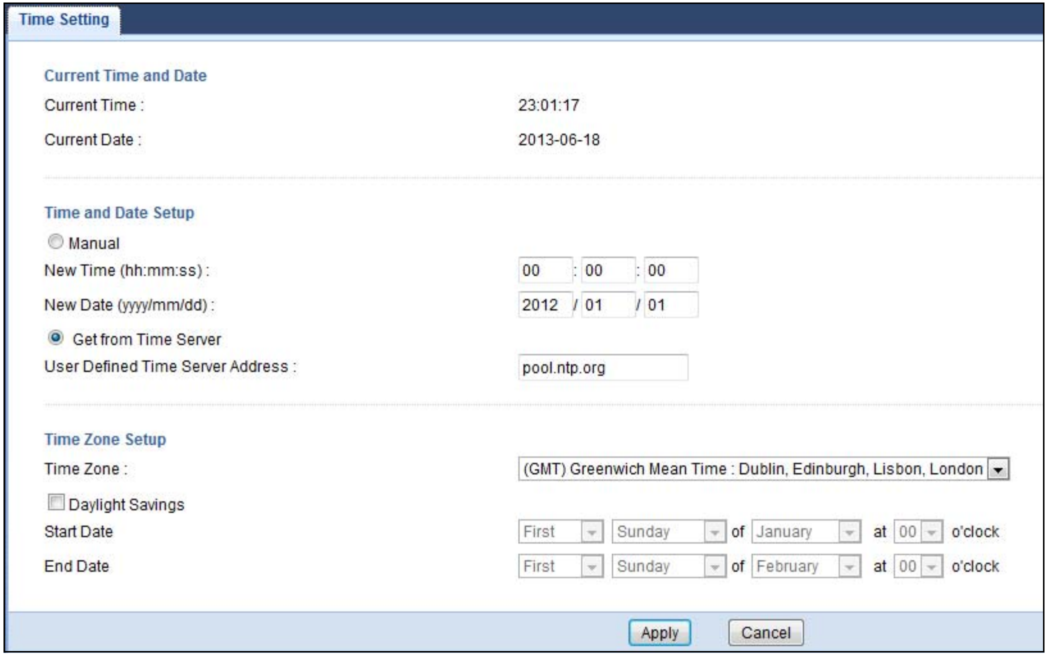
Table 30 Maintenance > Password

LABEL	DESCRIPTION
Password Setup	Change your WAP5805’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 WAP5805.
Cancel	Click **Cancel** to discard the changes.

10.5 Time Setting Screen

Use this screen to configure the WAP5805’s time based on your local time zone. To change your WAP5805’s time and date, click **Maintenance** > **Time**. The screen appears as shown.

Figure 45 Maintenance > Time



Current Time and Date

Current Time : 23:01:17

Current Date : 2013-06-18

Time and Date Setup

○ Manual

New Time (hh:mm:ss) : 00 : 00 : 00

New Date (yyyy/mm/dd) : 2012 / 01 / 01

● Get from Time Server

User Defined Time Server Address : pool.ntp.org

Time Zone Setup

Time Zone : (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

□ Daylight Savings

Start Date First Sunday of January at 00 o'clock

End Date First Sunday of February at 00 o'clock

he following table describes the labels in this screen.

Table 31 Maintenance > Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your WAP5805. Each time you reload this page, the WAP5805 synchronizes the time with the time server.
Current Date	This field displays the date of your WAP5805. Each time you reload this page, the WAP5805 synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you select **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 select **Manual**, enter the new date in this field and then click **Apply**.

Table 31 Maintenance > Time (continued)

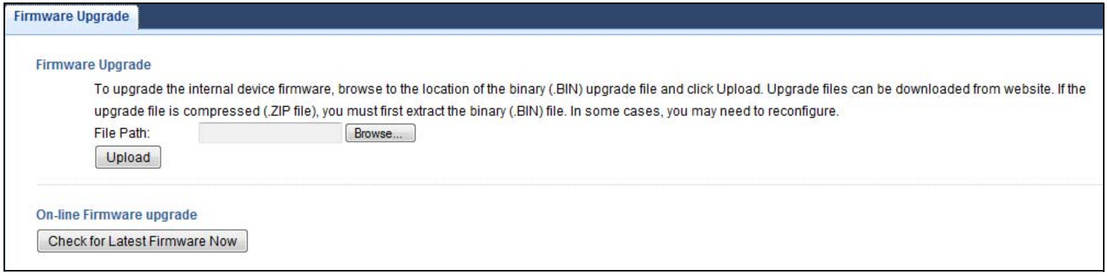
LABEL	DESCRIPTION
Get from Time Server	Select this radio button to have the WAP5805 get the time and date from the time server you specified below.
User Defined Time Server Address	Select **User Defined Time Server Address** and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes back to the WAP5805.
Cancel	Click **Cancel** to discard the changes.

10.6 Firmware Upgrade Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a “*.bin” extension, e.g., “WAP5805.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 > Firmware Upgrade**. Follow the instructions in this screen to upload firmware to your WAP5805.

Figure 46 Maintenance > Firmware Upgrade



Firmware Upgrade

Firmware Upgrade

To upgrade the internal device firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure.

File Path:

On-line Firmware upgrade

The following table describes the labels in this screen.

Table 32 Maintenance > Firmware Upgrade

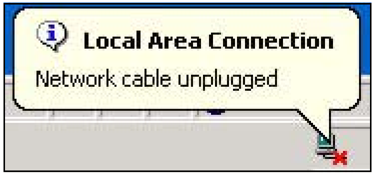
LABEL	DESCRIPTION
Firmware Upgrade	
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.
On-line Firmware upgrade	
Check for Latest Firmware Now	Click this button to get the latest firmware information, such as the version number, release date, release note and file size from the ZyXEL website. Make sure your WAP5805 has Internet access.

Note: Do not turn off the WAP5805 while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the WAP5805 again.

The WAP5805 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 47 Network Temporarily Disconnected



Local Area Connection

Network cable unplugged

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

If the upload was not successful, an error message appears. Click **Return** to go back to the **Firmware Upgrade** screen.

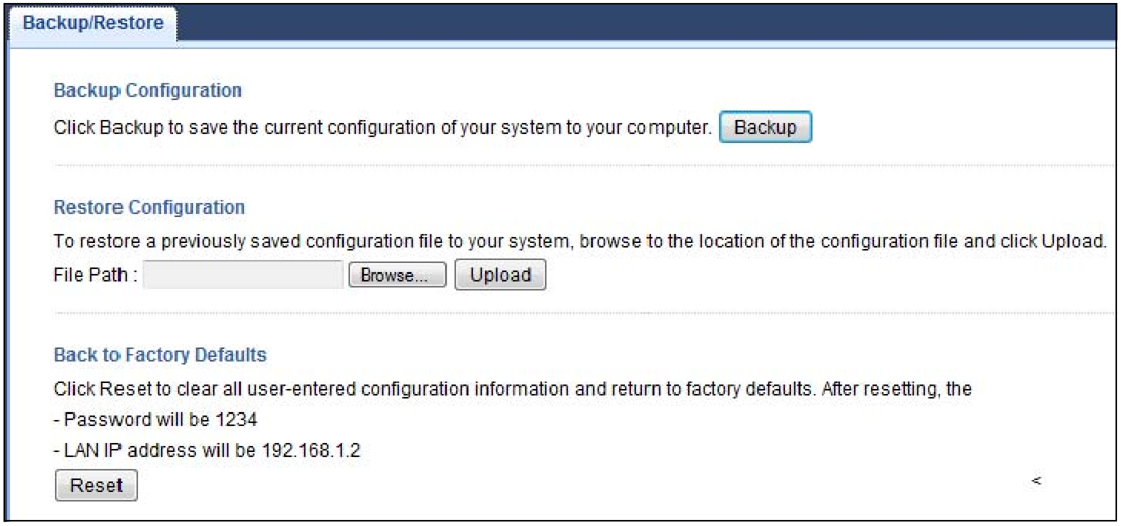
10.7 Configuration Backup/Restore Screen

Backup configuration allows you to back up (save) the WAP5805's current configuration to a file on your computer. Once your WAP5805 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.

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your WAP5805.

Click **Maintenance > Backup/Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 48 Maintenance > Backup/Restore



Backup Configuration

Click Backup to save the current configuration of your system to your computer.

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path :

Back to Factory Defaults

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the

- Password will be 1234

- LAN IP address will be 192.168.1.2

The following table describes the labels in this screen.

Table 33 Maintenance > Backup/Restore

LABEL	DESCRIPTION
Backup	Click **Backup** to save the WAP5805's current configuration to your computer.
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process. Note: Do not turn off the WAP5805 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 WAP5805 again. The WAP5805 automatically restarts in this time causing a temporary network disconnect. If you see an error screen, click Back to return to the Backup/Restore screen.
Reset	Pressing the **Reset** button in this section clears all user-entered configuration information and returns the WAP5805 to its factory defaults. You can also press the **RESET** button on the rear panel to reset the factory defaults of your WAP5805. Refer to the chapter about introducing the Web Configurator for more information on the **RESET** button.

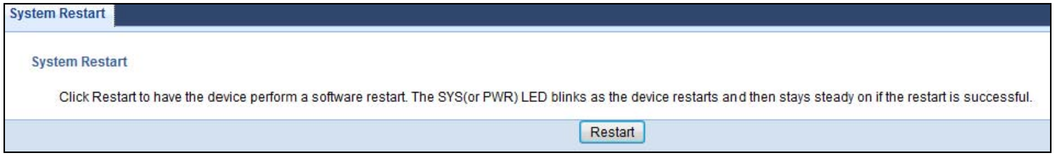
Note: If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default WAP5805 IP address. See Appendix A on page 77 for details on how to set up your computer's IP address.

10.8 Restart Screen

System restart allows you to reboot the WAP5805 without turning the power off.

Click **Maintenance > Restart** to open the following screen.

Figure 49 Maintenance > Restart



Click Restart to have the device perform a software restart. The SYS(or PWR) LED blinks as the device restarts and then stays steady on if the restart is successful.

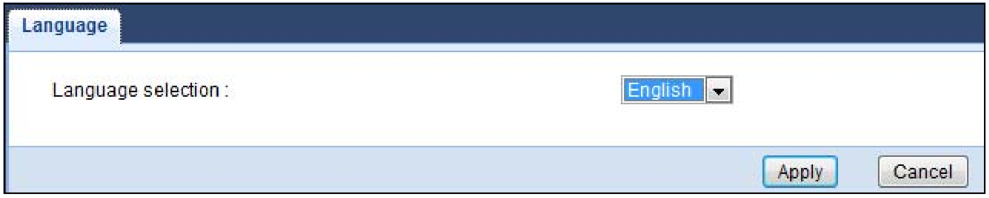
Click **Restart** to have the WAP5805 reboot. This does not affect the WAP5805's configuration.

10.9 Language

Language selection allows you to choose your preferred language.

Click **Maintenance > Language** to open the following screen.

Figure 50 Maintenance > Language



Language selection : English

The following table describes the labels in this screen.

Table 34 Maintenance > Language

LABEL	DESCRIPTION
Language selection	Choose from the drop-box your preferred language.
Apply	Click **Apply** to save your changes back to the WAP5805.
Cancel	Click **Cancel** to discard the changes.

Troubleshooting

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

- Power, Hardware Connections, and LEDs
- WAP5805 Access and Login
- Internet Access
- Resetting the WAP5805 to Its Factory Defaults

11.1 Power, Hardware Connections, and LEDs

The WAP5805 does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the WAP5805.
2. Make sure the power adaptor or cord is connected to the WAP5805 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 WAP5805.
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 1.6 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 WAP5805.
5. If the problem continues, contact the vendor.

11.2 WAP5805 Access and Login

I don’t know the IP address of my WAP5805.

1 The default IP address of the WAP5805 in access point mode is **192.168.1.2** and the default IP address of the WAP5805 in client mode is **192.168.1.10**.

2 If you changed the IP address and have forgotten it,

- and your WAP5805 is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.
- by choosing to set the IP configuration as DHCP, the default IP (for AP mode is 192.168.1.2 and CL mode is 192.168.1.10) will be replaced by the DHCP IP. The default alias IP for AP mode is 192.168.100.2 and CL mode is 192.168.100.10. You may choose to set your connected device (for example: a PC) as 192.168.100.1 or from a range of 192.168.100.3 to 192.168.100.99 to access the WAP5805 for configuration.
- reset your WAP5805 to change all settings back to their default. This means your current settings are lost. See Section 11.4 on page 75 in the **Troubleshooting** for information on resetting your WAP5805.

I forgot the password.

1 The default password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 11.4 on page 75.

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 of the WAP5805 in access point mode is **192.168.1.2** and the default IP address of the WAP5805 in client mode is **192.168.1.10**.
- If you changed the IP address (Section 10.4 on page 81), 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 WAP5805.

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 JavaScripts and Java enabled. See your Internet brower Help.

4 Make sure your computer is in the same subnet as the WAP5805. (If you know that there are routers between your computer and the WAP5805, skip this step.)

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Section 10.4 on page 81.
- If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the WAP5805. See Appendix B on page 111.

5 Reset the device to its factory defaults, and try to access the WAP5805 with the default IP address. See Section 10.7 on page 70.

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

Advanced Suggestion

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

I can see the **Login** screen, but I cannot log in to the WAP5805.

1 Make sure you have entered the password correctly. The 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 WAP5805.

4 If this does not work, you have to reset the device to its factory defaults. See Section 11.4 on page 75.

11.3 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 Make sure the WAP5805 in access point mode is connected to a broadband modem or router with Internet access. Connect to another WAP5805 in client mode to access the Internet through the WAP5805 in access point mode. Use the switch on the WAP5805's side panel to change your system operating mode setting (see Section 2.1.3 on page 19). Make sure the client is within the transmission range of the AP.

3 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.

4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

5 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the WAP5805), 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 1.6 on page 11.

2 Reboot the WAP5805.

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 1.6 on page 11. If the WAP5805 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 clients 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 WAP5805.

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

Advanced Suggestions

- Check the settings for QoS. If it is disabled, you might consider activating it.

11.4 Resetting the WAP5805 to Its Factory Defaults

If you reset the WAP5805, you lose all of the changes you have made. The WAP5805 re-loads its default settings, and the password resets to **1234**. You have to make all of your changes again.

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

To reset the WAP5805,

1 Make sure the power LED is on.

2 Press the **RESET** button for longer than 1 second to restart/reboot the WAP5805.

3 Press the **RESET** button for longer than five seconds to set the WAP5805 back to its factory-default configurations.

If the WAP5805 restarts automatically, wait for the WAP5805 to finish restarting, and log in to the Web Configurator. The password is “1234”.

If the WAP5805 does not restart automatically, disconnect and reconnect the WAP5805’s power. Then, follow the directions above again.

A

Setting Up Your Computer’s IP Address

Note: Your specific WAP5805 may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

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

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

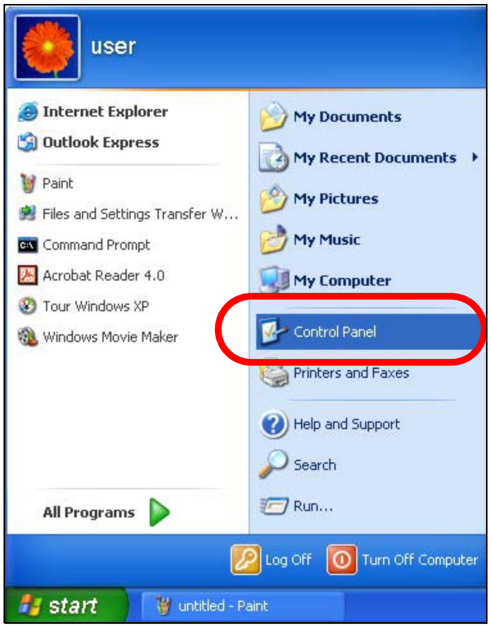
In this appendix, you can set up an IP address for:

- Windows XP/NT/2000 on page 77
- Windows Vista on page 81
- Windows 7 on page 85
- Mac OS X: 10.3 and 10.4 on page 89
- Mac OS X: 10.5 and 10.6 on page 92
- Linux: Ubuntu 8 (GNOME) on page 95
- Linux: openSUSE 10.3 (KDE) on page 99

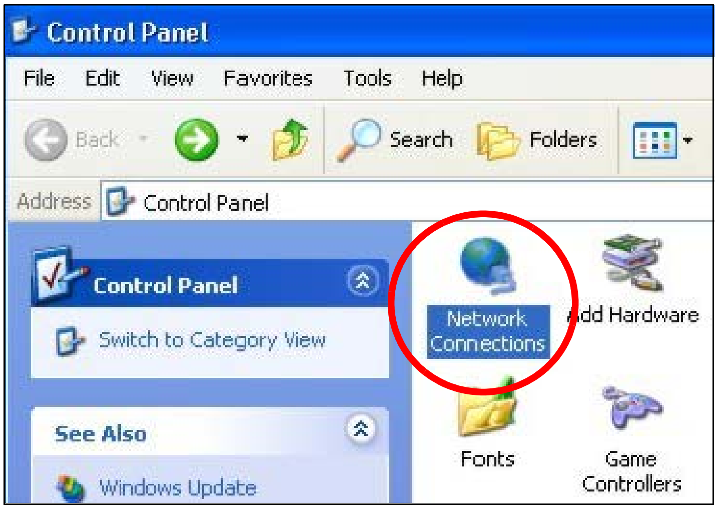
Windows XP/NT/2000

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

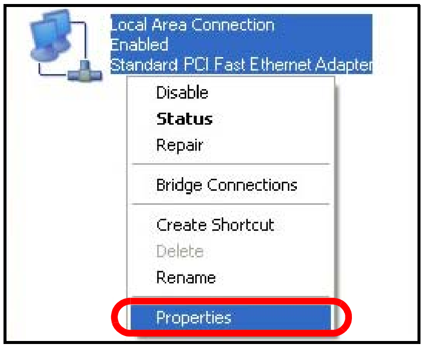
1 Click **Start** > **Control Panel**.



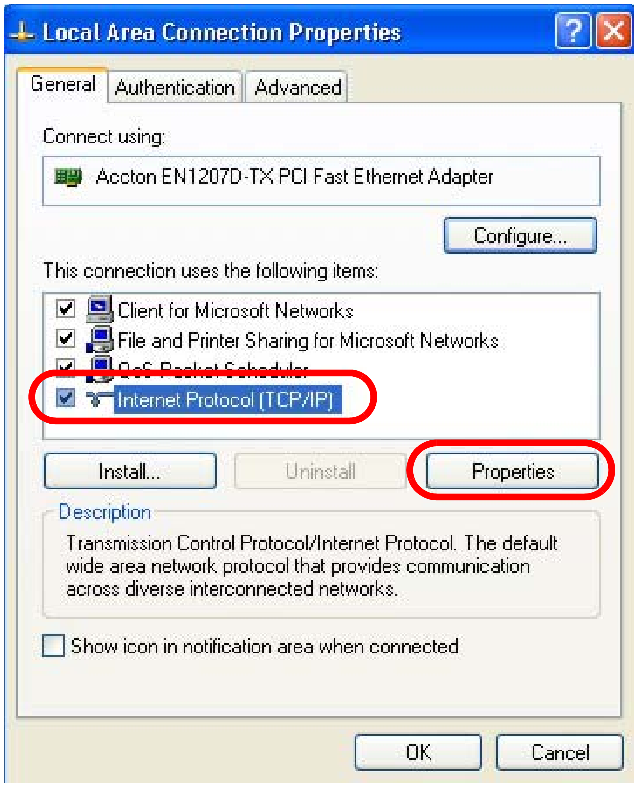
2 In the **Control Panel**, click the **Network Connections** icon.



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



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



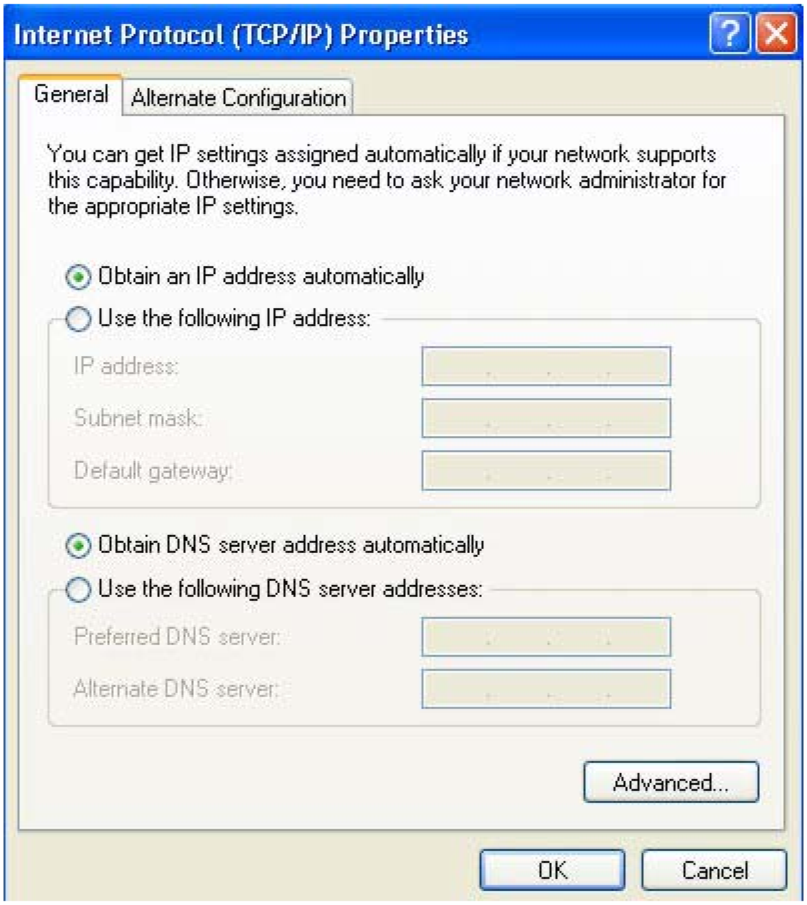
Accton EN1207D-TX PCI Fast Ethernet Adapter

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

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

□ Show icon in notification area when connected

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



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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

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

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

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

Verifying Settings

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

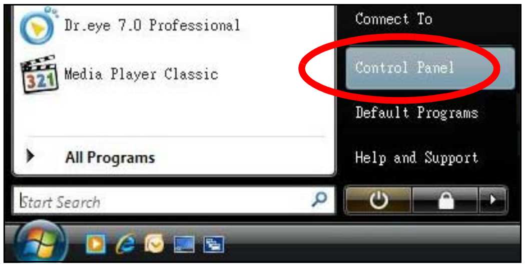
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

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

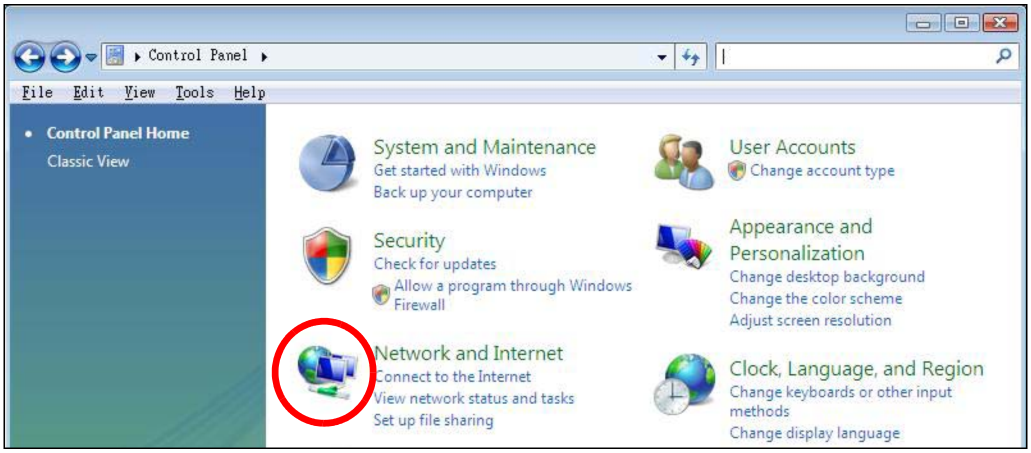
Windows Vista

This section shows screens from Windows Vista Professional.

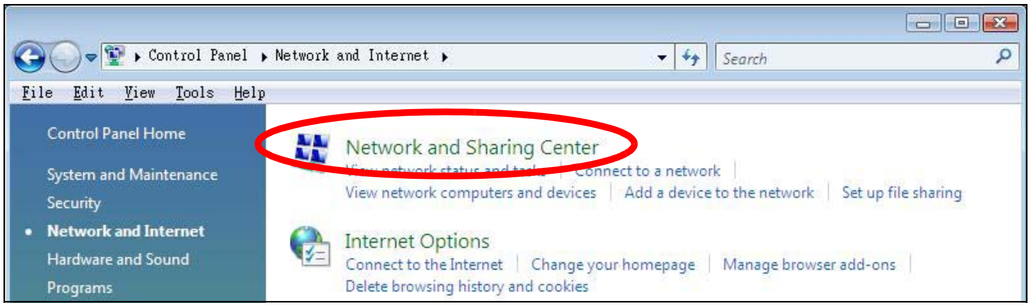
1 Click **Start** > **Control Panel**.



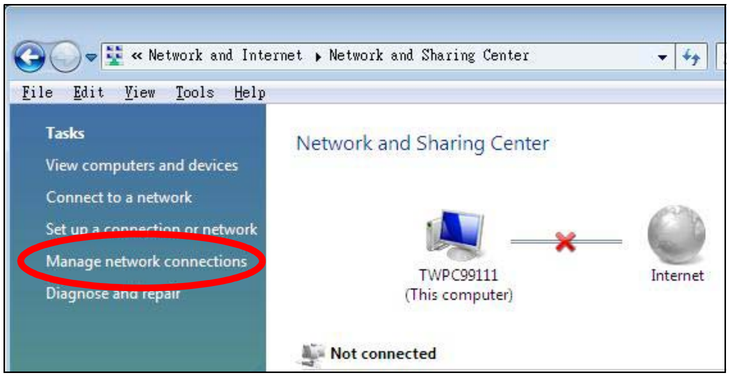
2 In the **Control Panel**, click the **Network and Internet** icon.



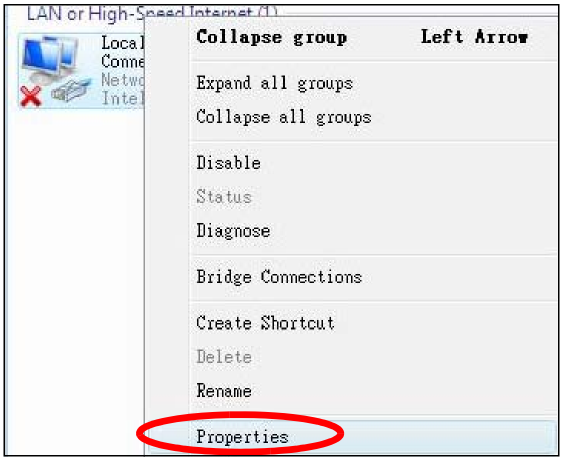
3 Click the **Network and Sharing Center** icon.



4 Click **Manage network connections**.

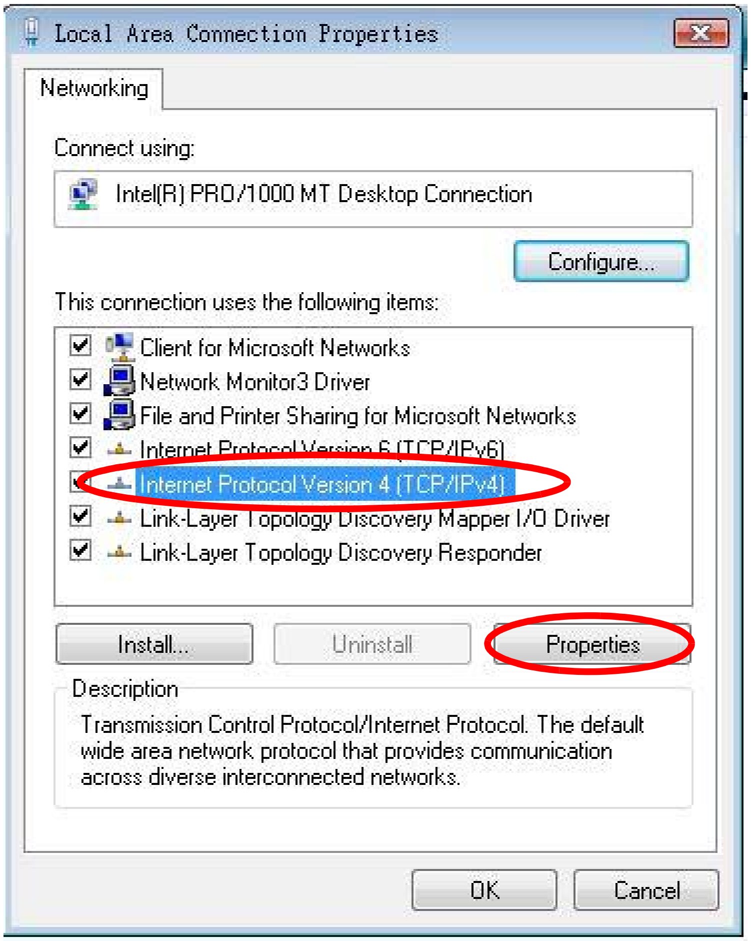

« Network and Internet ▸ Network and Sharing Center
File Edit View Tools Help
Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair
Network and Sharing Center
TWPC99111
(This computer)
Internet
Not connected

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



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

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



Connect using:

Intel(R) PRO/1000 MT Desktop Connection

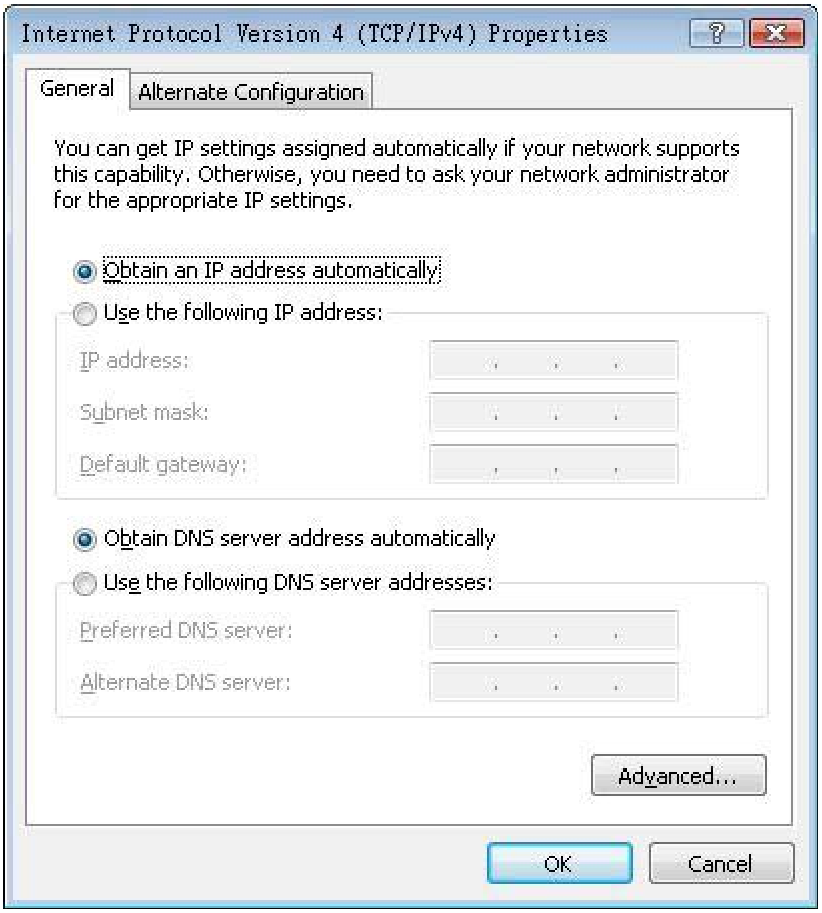
This connection uses the following items:

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

Description

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

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



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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

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

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

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

Verifying Settings

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

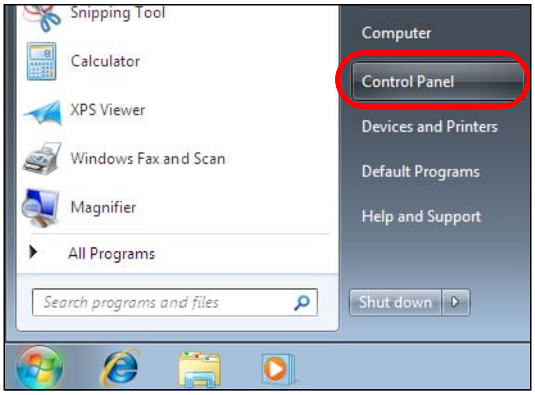
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

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

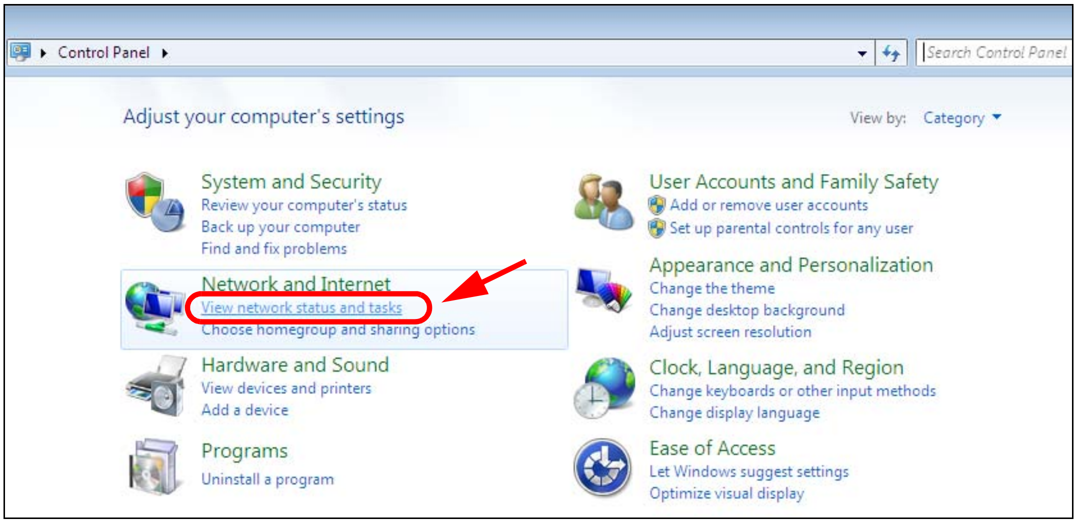
Windows 7

This section shows screens from Windows 7 Enterprise.

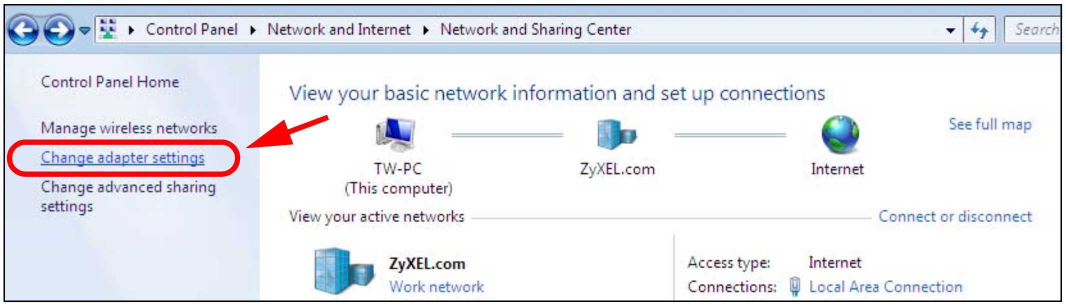
1 Click **Start** > **Control Panel**.



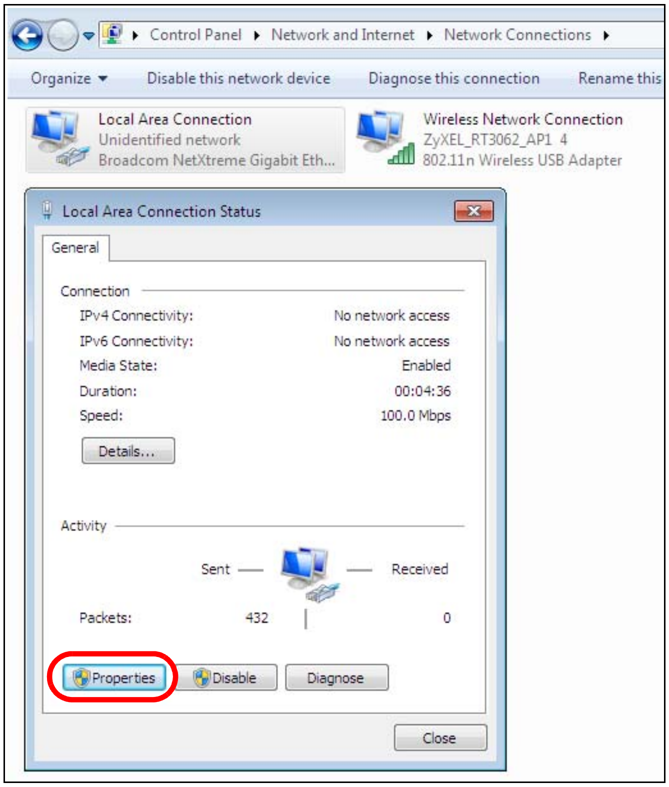
2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.


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

3 Click **Change adapter settings**.


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

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



Local Area Connection
Unidentified network
Broadcom NetXtreme Gigabit Eth...

Wireless Network Connection
ZyXEL_RT3062_AP1 4
802.11n Wireless USB Adapter

Local Area Connection Status

Connection

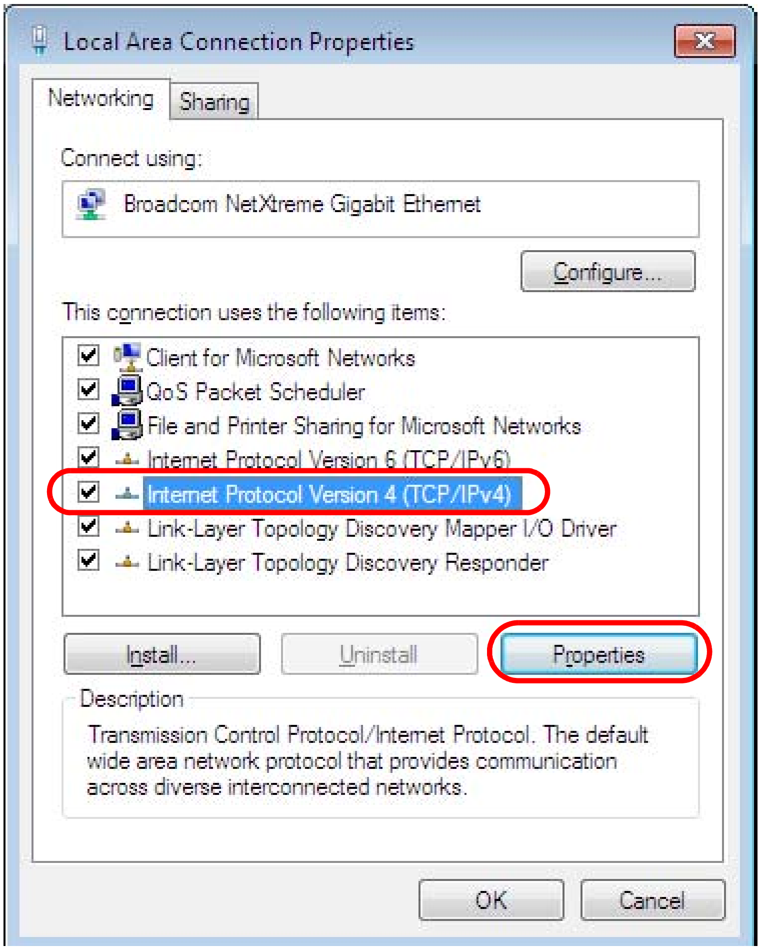
IPv4 Connectivity:	No network access
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	00:04:36
Speed:	100.0 Mbps

Activity

	Sent	Received
Packets:	432	0

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

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



Local Area Connection Properties

Networking | Sharing

Connect using:

Broadcom NetXtreme Gigabit Ethernet

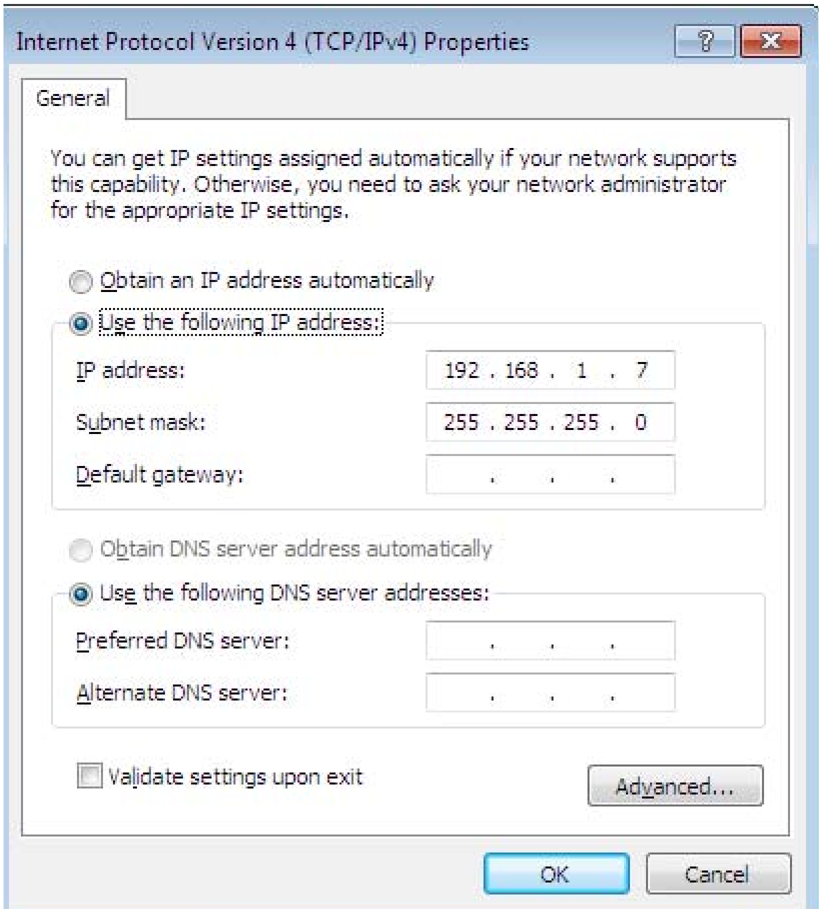
This connection uses the following items:

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

Description

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

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



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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 7

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

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

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

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

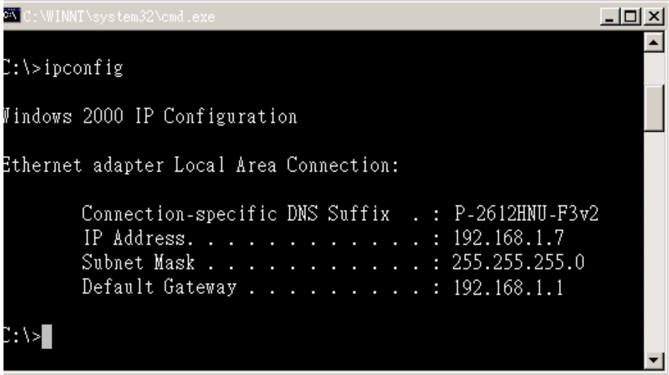
9 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

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

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

3 The IP settings are displayed as follows.

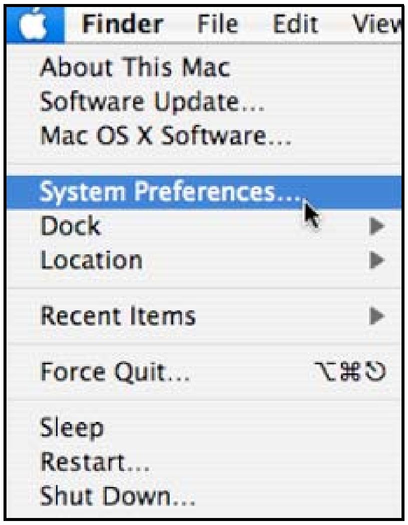


```
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

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

C:\>
```

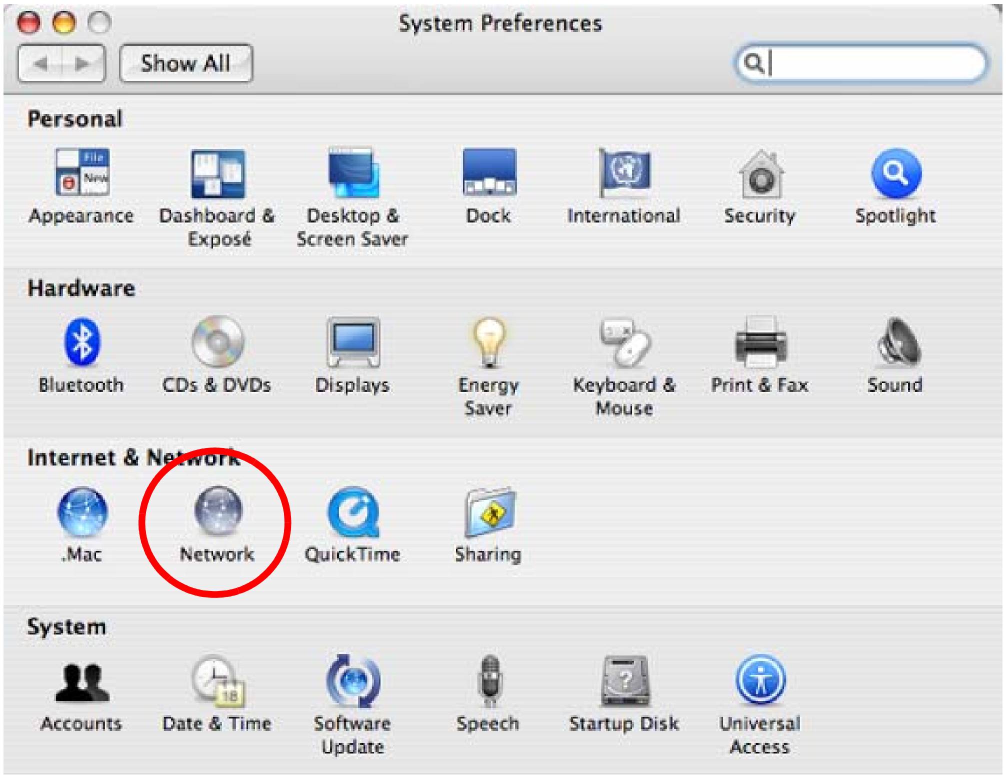
Mac OS X: 10.3 and 10.4

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

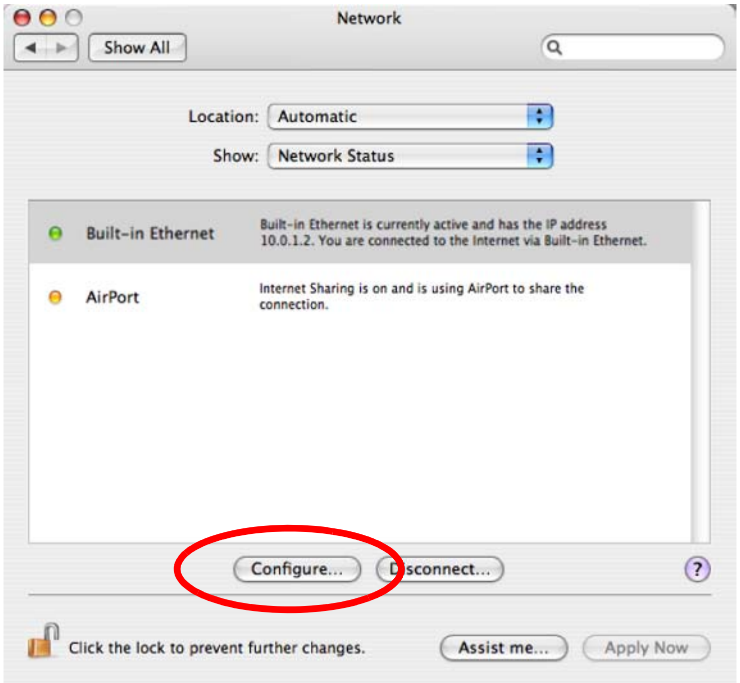
1 Click **Apple** > **System Preferences**.



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.**



Location: Automatic

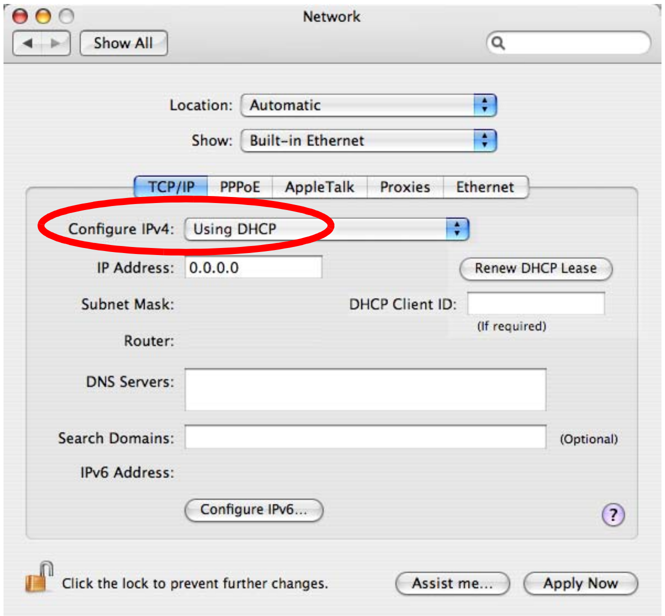
Show: Network Status

Built-in Ethernet — Built-in Ethernet is currently active and has the IP address 10.0.1.2. You are connected to the Internet via Built-in Ethernet.

AirPort — Internet Sharing is on and is using AirPort to share the connection.

Click the lock to prevent further changes.

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



Network

Location: Automatic

Show: Built-in Ethernet

Configure IPv4: Using DHCP

IP Address: 0.0.0.0

Subnet Mask:

Router:

DHCP Client ID: (If required)

DNS Servers:

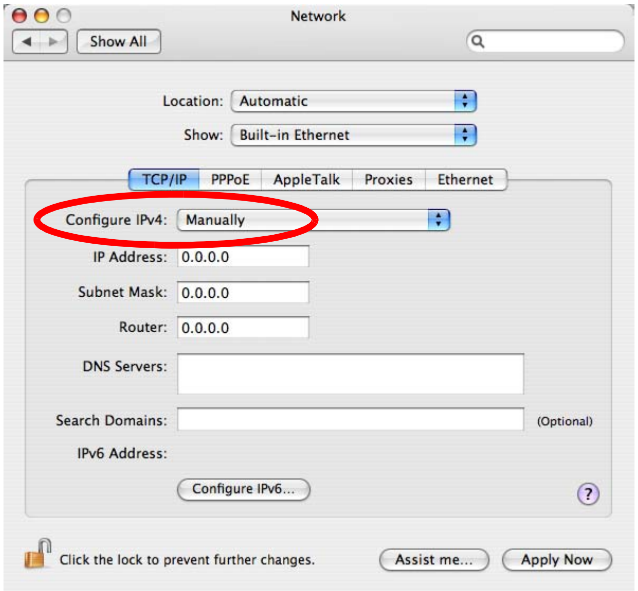
Search Domains: (Optional)

IPv6 Address:

Click the lock to prevent further changes.

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.



Network

Location: Automatic

Show: Built-in Ethernet

Configure IPv4: Manually

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Router: 0.0.0.0

DNS Servers:

Search Domains: (Optional)

IPv6 Address:

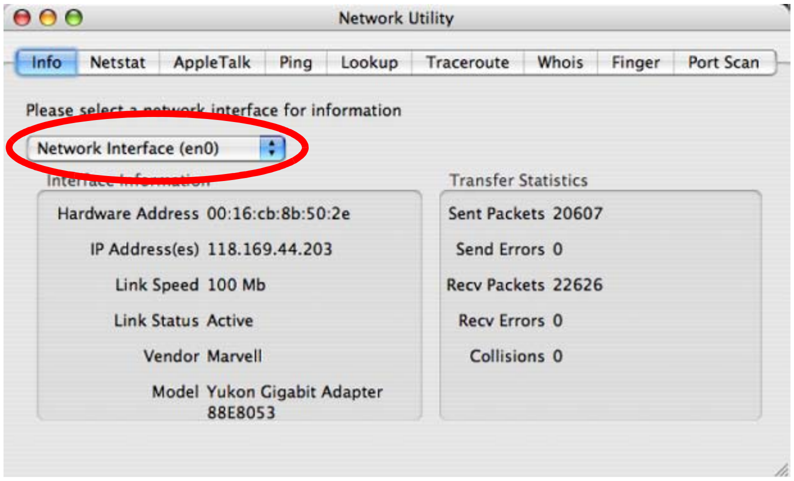
Click the lock to prevent further changes.

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 51 Mac OS X 10.4: Network Utility



Please select a network interface for information

Network Interface (en0)

Interface Information

Hardware Address 00:16:cb:8b:50:2e

IP Address(es) 118.169.44.203

Link Speed 100 Mb

Link Status Active

Vendor Marvell

Model Yukon Gigabit Adapter 88E8053

Transfer Statistics

Sent Packets 20607

Send Errors 0

Recv Packets 22626

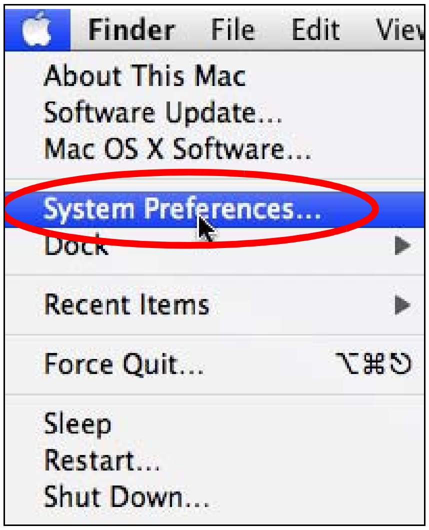
Recv Errors 0

Collisions 0

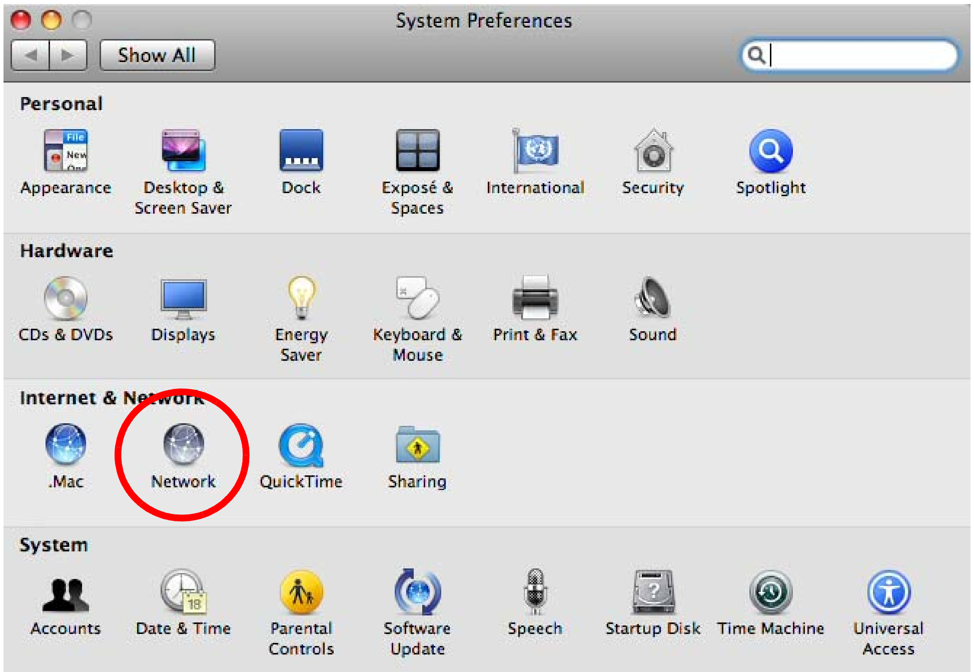
Mac OS X: 10.5 and 10.6

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

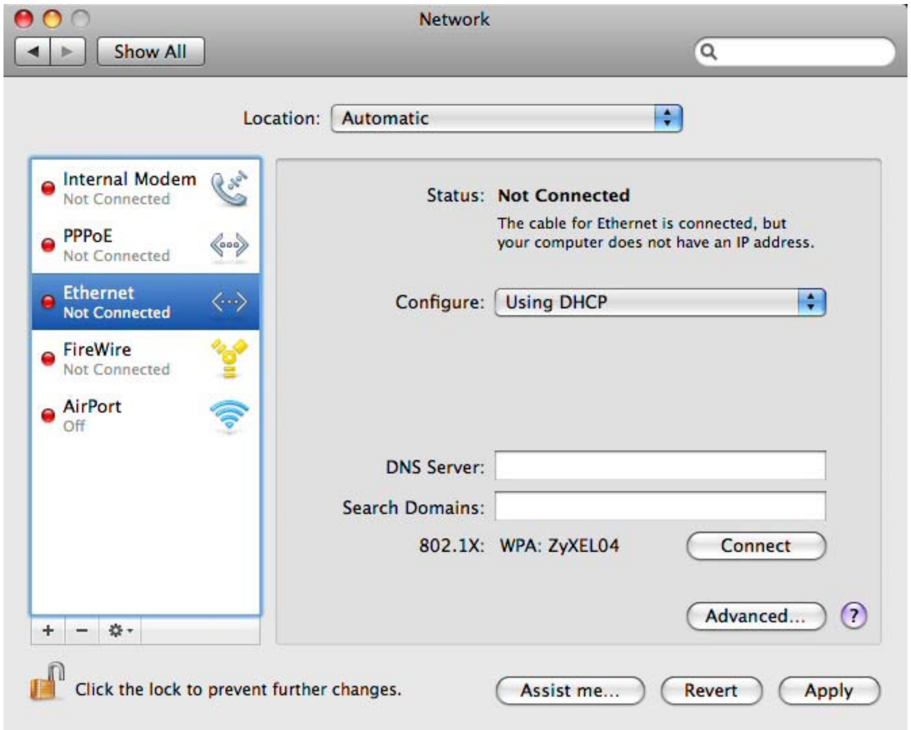
1 Click **Apple** > **System Preferences**.



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



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



Location: Automatic

Status: Not Connected

The cable for Ethernet is connected, but your computer does not have an IP address.

Configure: Using DHCP

DNS Server:

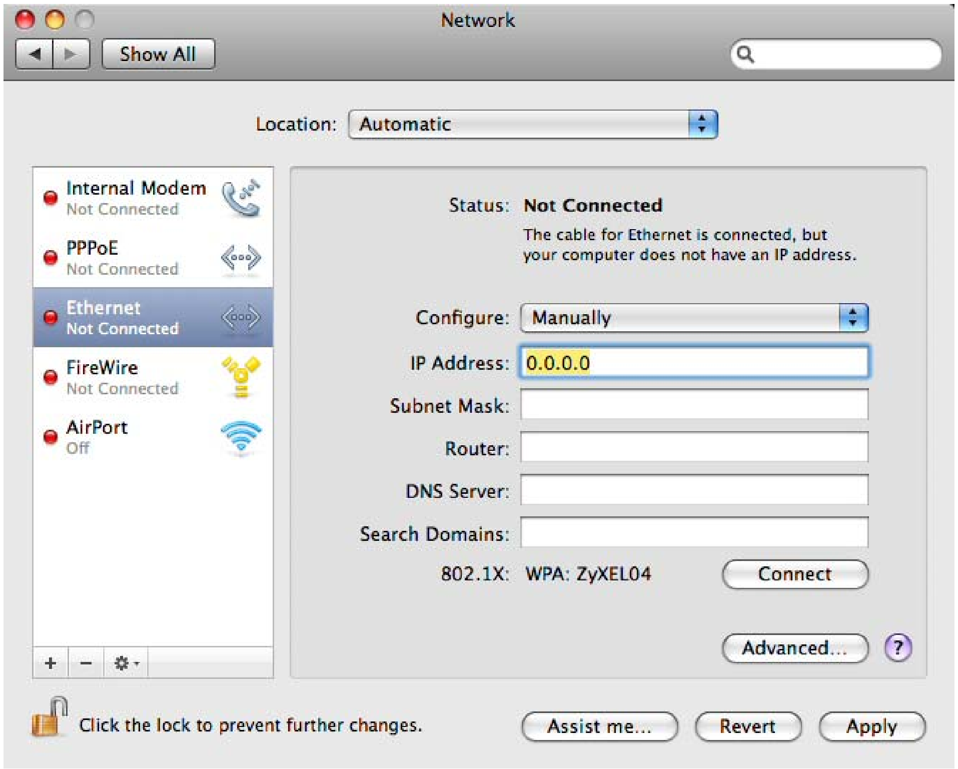
Search Domains:

802.1X: WPA: ZyXEL04

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 WAP5805.



Location: Automatic

Status: **Not Connected**

The cable for Ethernet is connected, but your computer does not have an IP address.

Configure: Manually

IP Address: 0.0.0.0

Subnet Mask:

Router:

DNS Server:

Search Domains:

802.1X: WPA: ZyXEL04

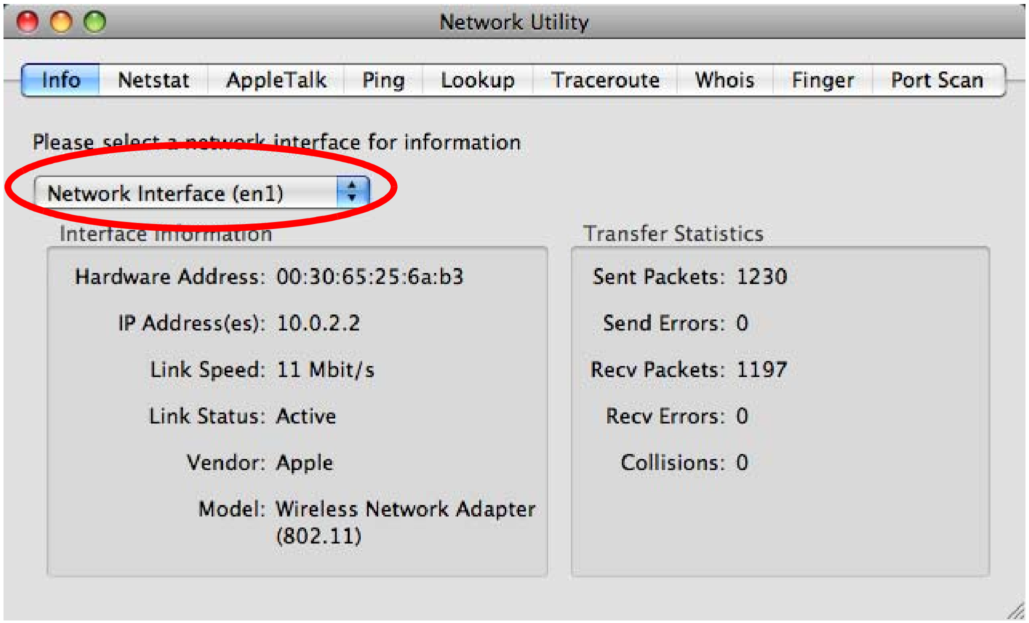
Click the lock to prevent further changes.

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 52 Mac OS X 10.5: Network Utility



Please select a network interface for information

Network Interface (en1)

Interface Information

Hardware Address: 00:30:65:25:6a:b3

IP Address(es): 10.0.2.2

Link Speed: 11 Mbit/s

Link Status: Active

Vendor: Apple

Model: Wireless Network Adapter (802.11)

Transfer Statistics

Sent Packets: 1230

Send Errors: 0

Recv Packets: 1197

Recv Errors: 0

Collisions: 0

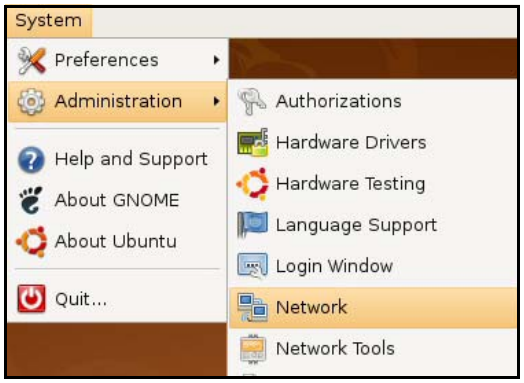
Linux: Ubuntu 8 (GNOME)

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.

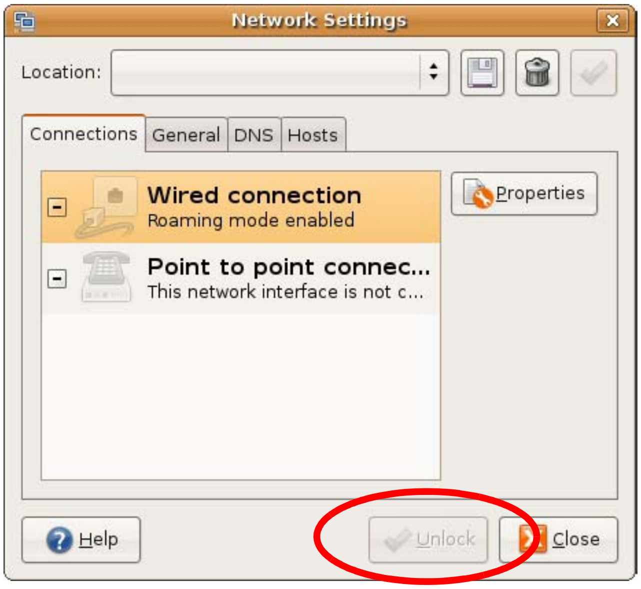
Note: Make sure you are logged in as the root administrator.

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

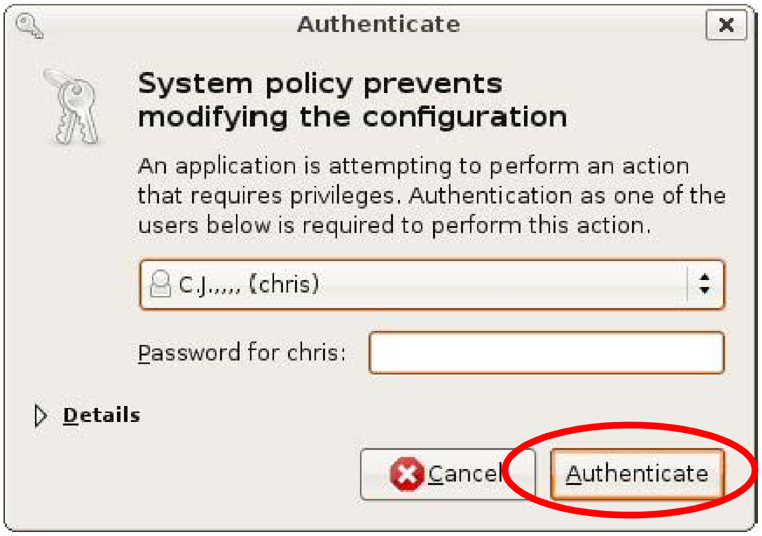
1 Click **System > Administration > Network**.



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.



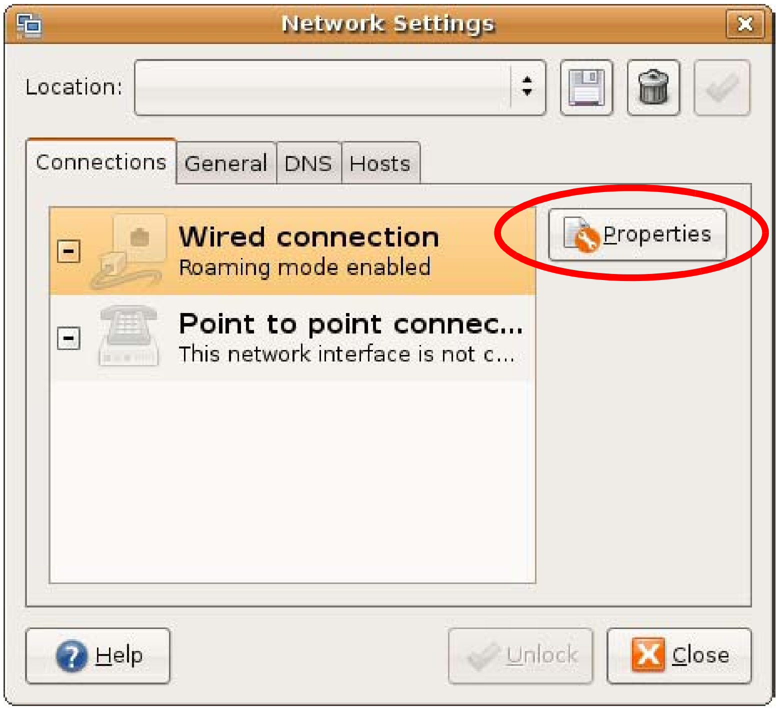
System policy prevents modifying the configuration

An application is attempting to perform an action that requires privileges. Authentication as one of the users below is required to perform this action.

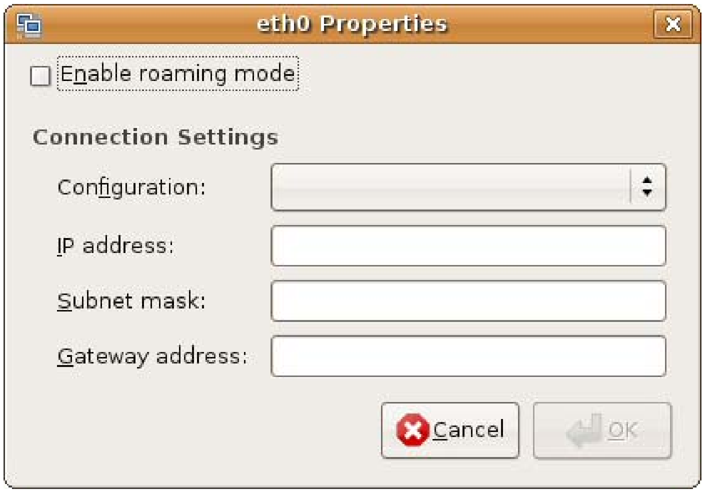
C.J....., (chris)

Password for chris:

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



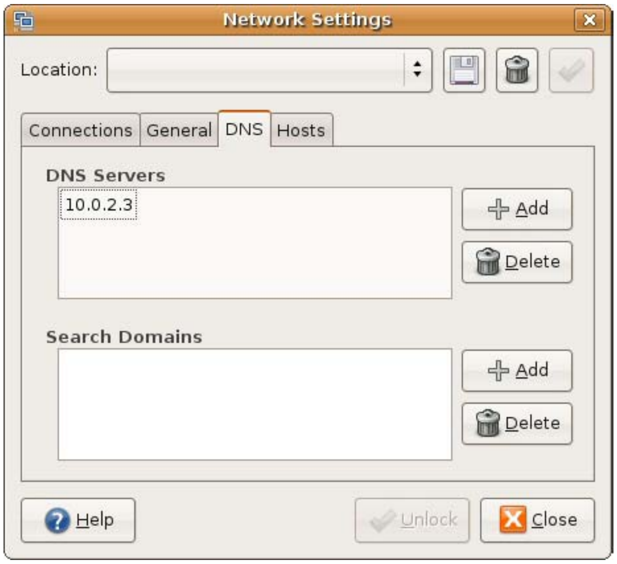
5 The **Properties** dialog box opens.



- 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.



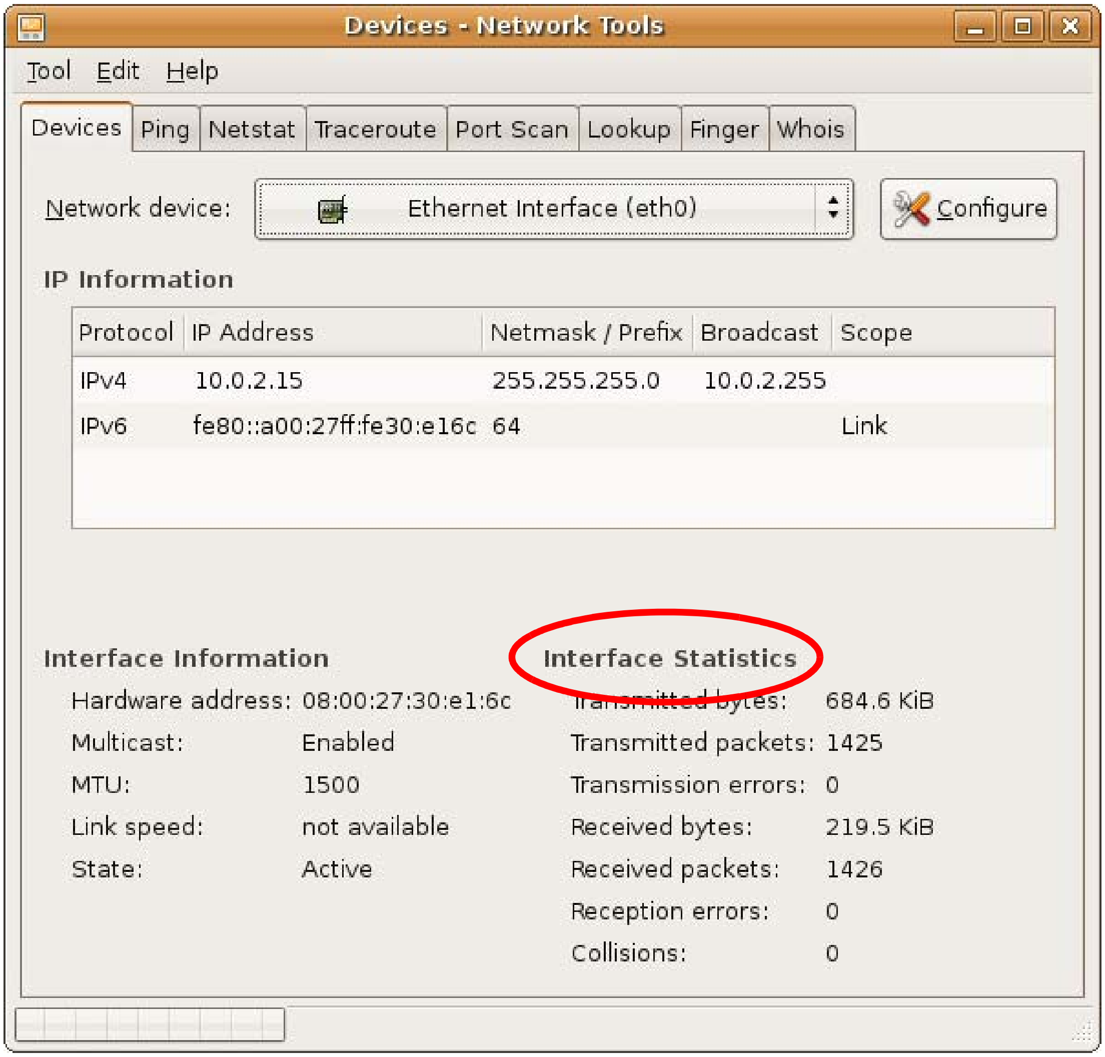
10.0.2.3

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 53 Ubuntu 8: Network Tools



Network device: Ethernet Interface (eth0)

IP Information

Protocol	IP Address	Netmask / Prefix	Broadcast	Scope
IPv4	10.0.2.15	255.255.255.0	10.0.2.255	
IPv6	fe80::a00:27ff:fe30:e16c	64		Link

Interface Information		Interface Statistics	
Hardware address:	08:00:27:30:e1:6c	Transmitted bytes:	684.6 KiB
Multicast:	Enabled	Transmitted packets:	1425
MTU:	1500	Transmission errors:	0
Link speed:	not available	Received bytes:	219.5 KiB
State:	Active	Received packets:	1426
		Reception errors:	0
		Collisions:	0

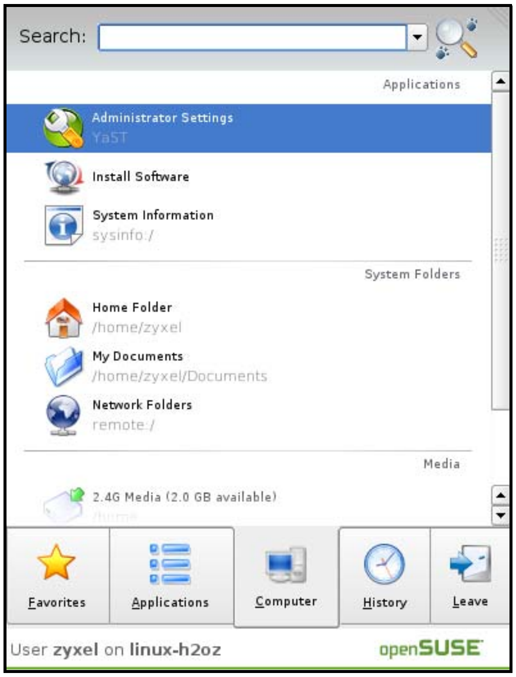
Linux: openSUSE 10.3 (KDE)

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.

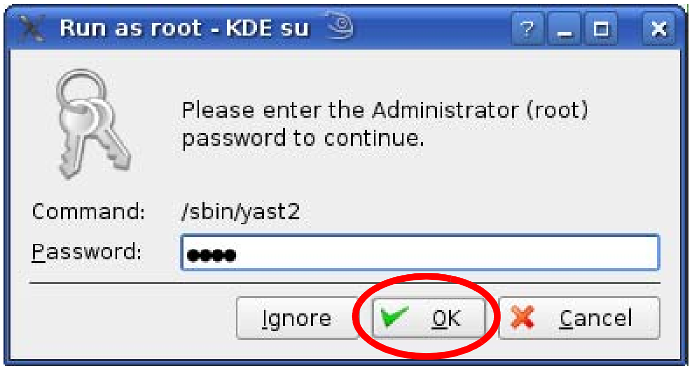
Note: Make sure you are logged in as the root administrator.

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**.

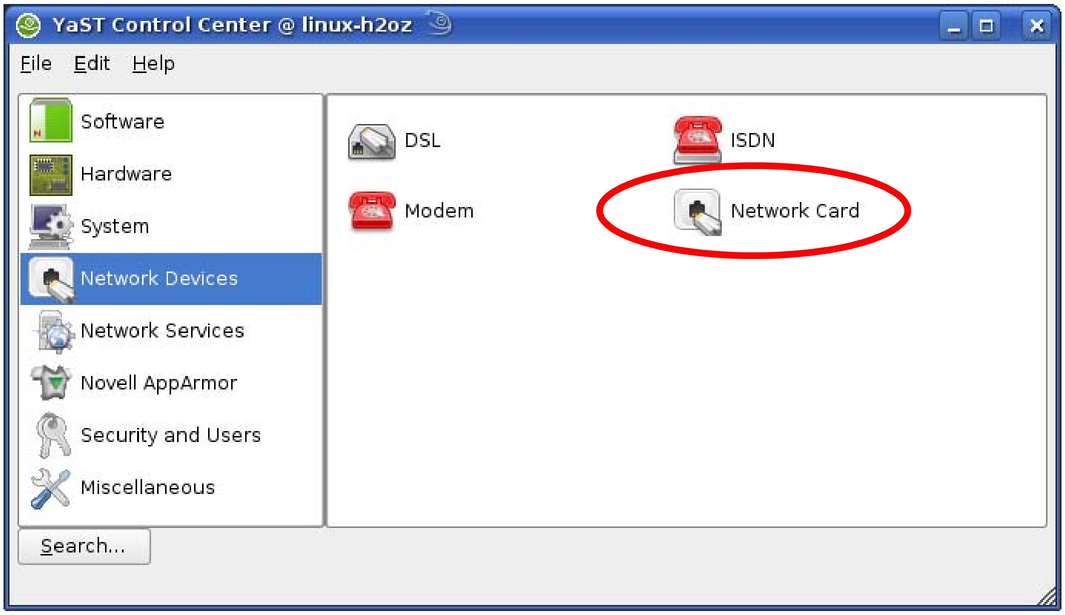


Please enter the Administrator (root) password to continue.

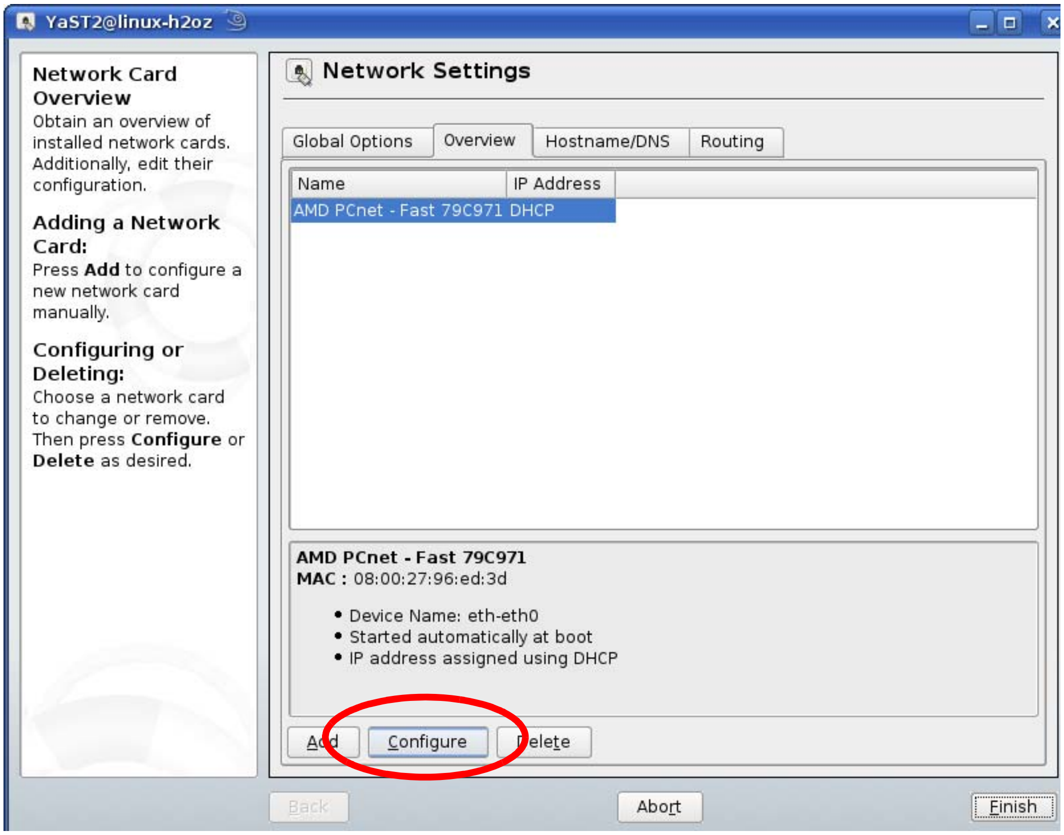
Command: /sbin/yast2

Password: ●●●●

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.



Network Card Overview
Obtain an overview of installed network cards. Additionally, edit their configuration.

Adding a Network Card:
Press **Add** to configure a new network card manually.

Configuring or Deleting:
Choose a network card to change or remove. Then press **Configure** or **Delete** as desired.

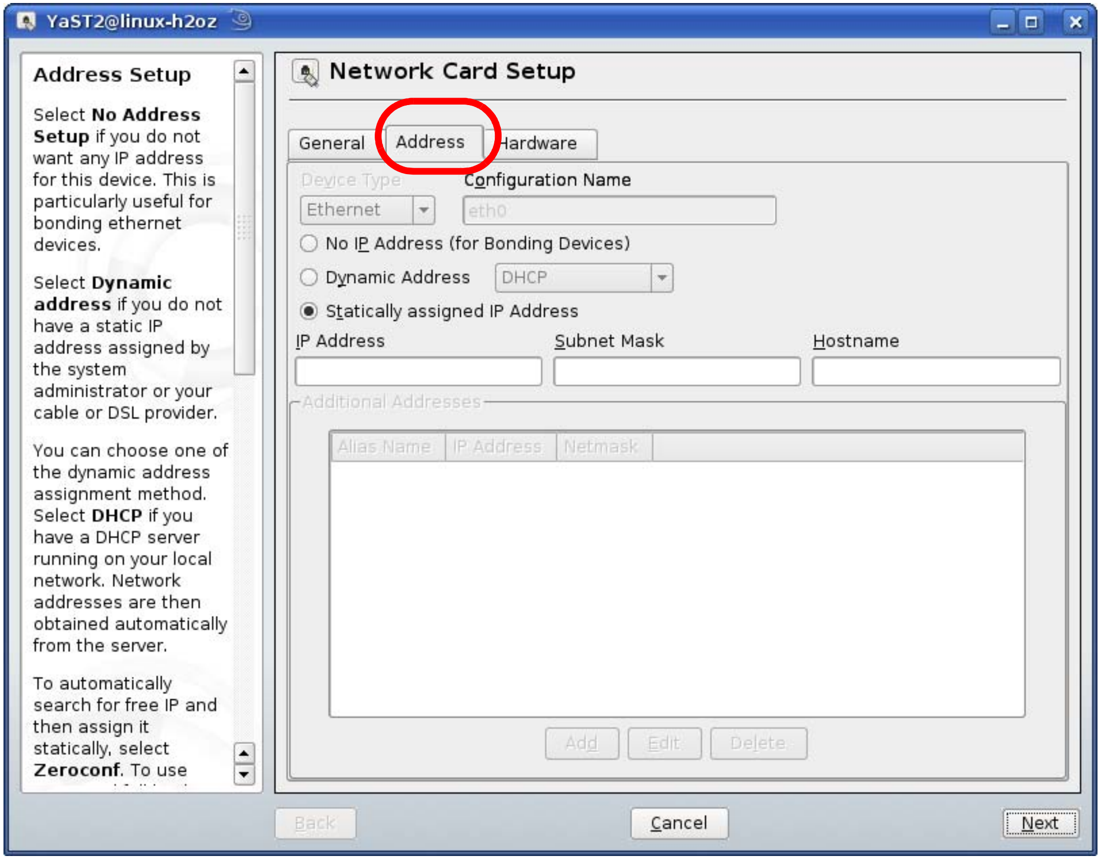
Name	IP Address
AMD PCnet - Fast 79C971	DHCP

AMD PCnet - Fast 79C971
MAC : 08:00:27:96:ed:3d

- Device Name: eth-eth0
- Started automatically at boot
- IP address assigned using DHCP

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

Figure 54 openSUSE 10.3: Network Card Setup



Address Setup

Select **No Address Setup** if you do not want any IP address for this device. This is particularly useful for bonding ethernet devices.

Select **Dynamic address** if you do not have a static IP address assigned by the system administrator or your cable or DSL provider.

You can choose one of the dynamic address assignment method. Select **DHCP** if you have a DHCP server running on your local network. Network addresses are then obtained automatically from the server.

To automatically search for free IP and then assign it statically, select **Zeroconf**. To use

Device Type: Ethernet

Configuration Name: eth0

○ No IP Address (for Bonding Devices)

○ Dynamic Address DHCP

● Statically assigned IP Address

IP Address:

Subnet Mask:

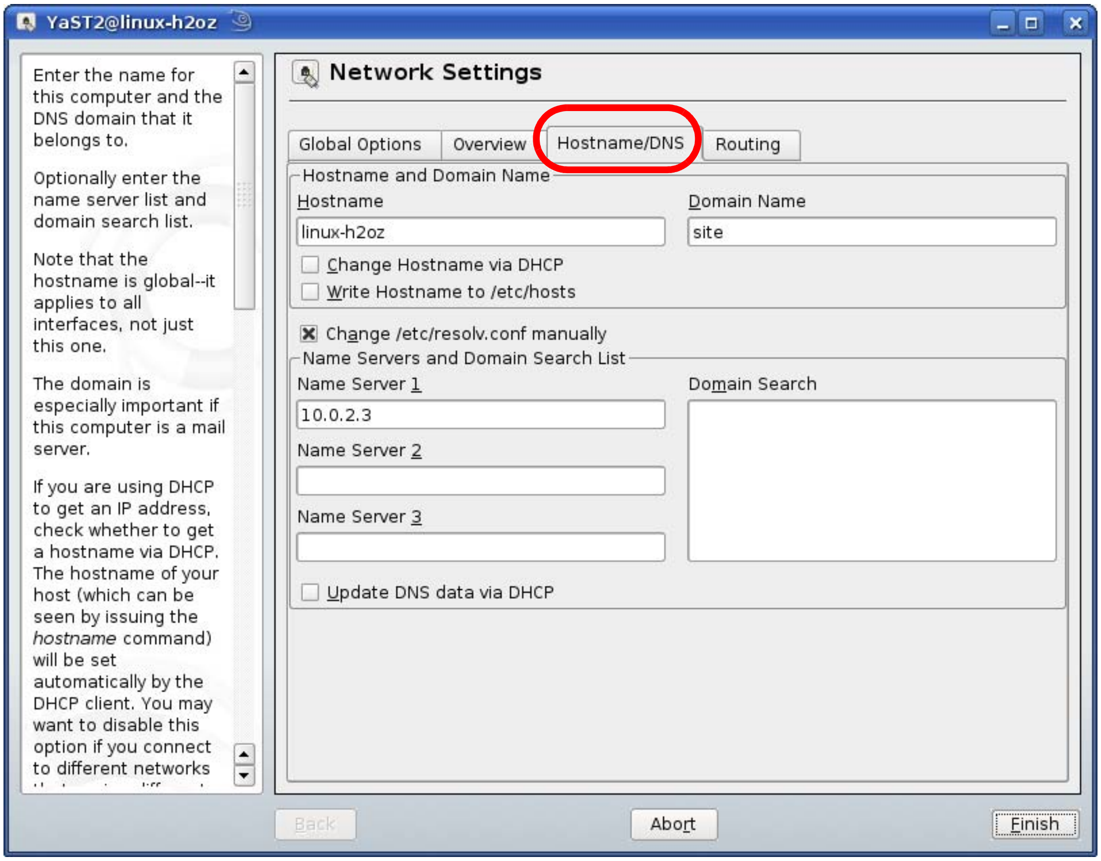
Hostname:

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.



Enter the name for this computer and the DNS domain that it belongs to.

Optionally enter the name server list and domain search list.

Note that the hostname is global--it applies to all interfaces, not just this one.

The domain is especially important if this computer is a mail server.

If you are using DHCP to get an IP address, check whether to get a hostname via DHCP. The hostname of your host (which can be seen by issuing the *hostname* command) will be set automatically by the DHCP client. You may want to disable this option if you connect to different networks

Hostname and Domain Name

Hostname: linux-h2oz

Domain Name: site

☐ Change Hostname via DHCP

☐ Write Hostname to /etc/hosts

☒ Change /etc/resolv.conf manually

Name Servers and Domain Search List

Name Server 1: 10.0.2.3

Name Server 2:

Name Server 3:

Domain Search:

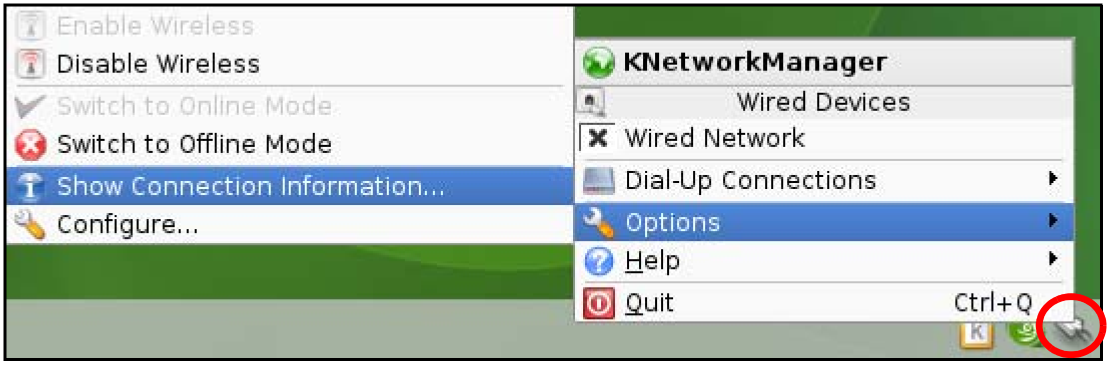
☐ Update DNS data via DHCP

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

Verifying Settings

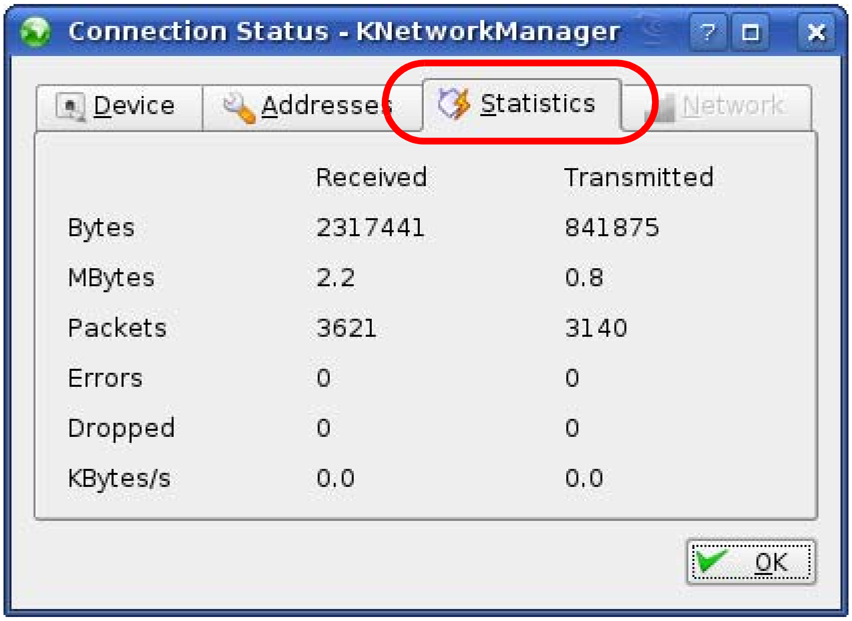
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 55 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 56 openSUSE: Connection Status - KNetwork Manager



	Received	Transmitted
Bytes	2317441	841875
MBytes	2.2	0.8
Packets	3621	3140
Errors	0	0
Dropped	0	0
KBytes/s	0.0	0.0

Wireless LANs

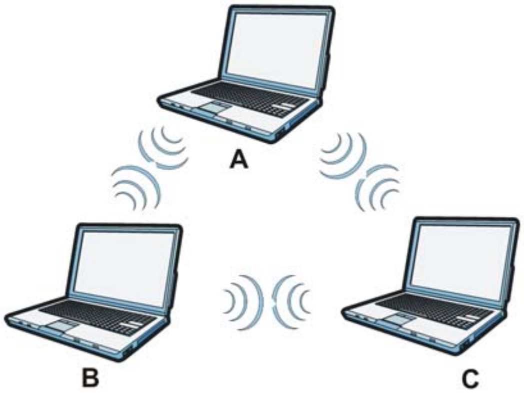
Wireless LAN Topologies

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

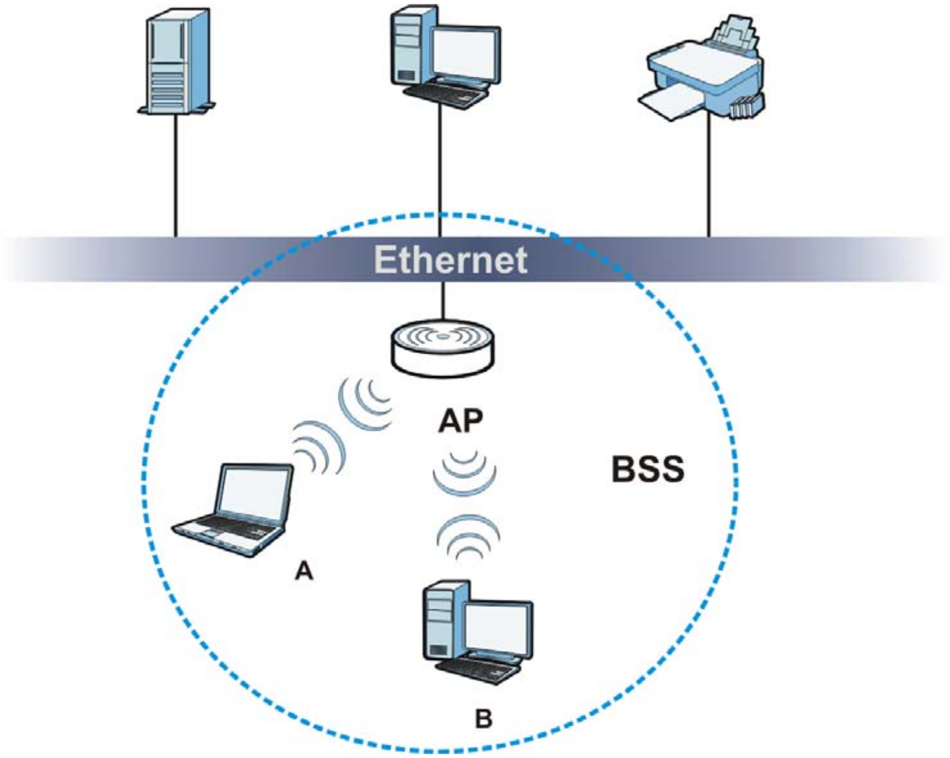


BSS

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 58 Basic Service Set



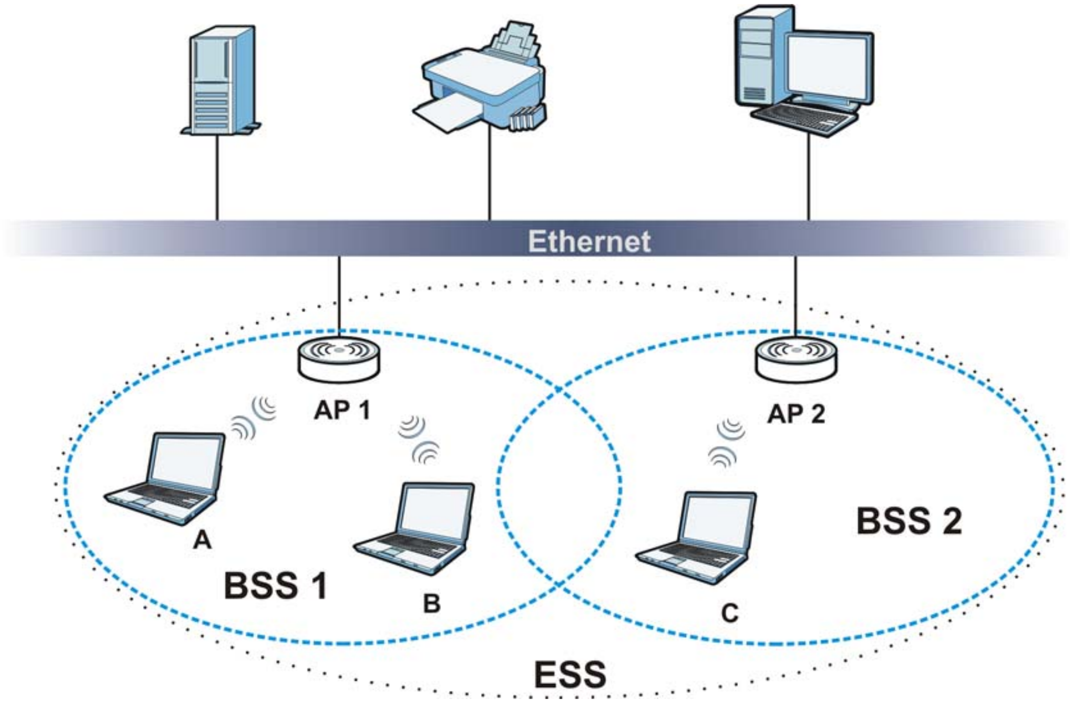
ESS

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 59 Infrastructure WLAN



Channel

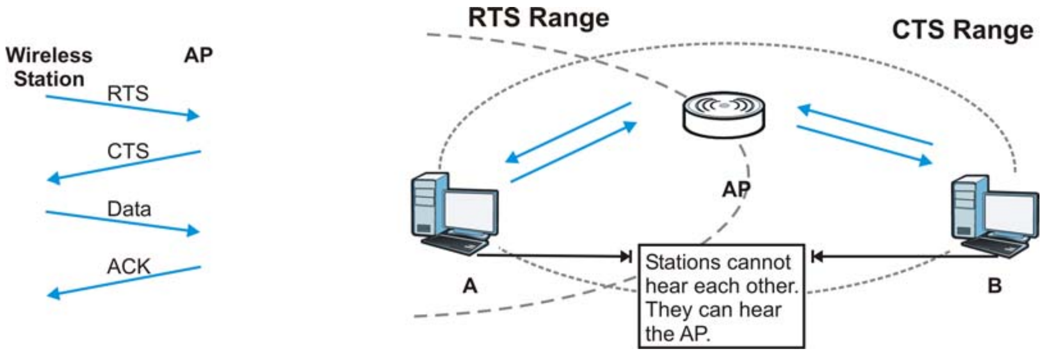
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference 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 60 RTS/CTS



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

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

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

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

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

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

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

Fragmentation Threshold

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

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

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

Preamble Type

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

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

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

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

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the WAP5805 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 35 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 WAP5805 are data encryption, wireless client authentication, restricting access by device MAC address and hiding the WAP5805 identity.

The following figure shows the relative effectiveness of these wireless security methods available on your WAP5805.

Table 36 Wireless Security Levels

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

Note: You must enable the same wireless security settings on the WAP5805 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 reauthentication times out. A new WEP key is generated each time reauthentication 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 37 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.

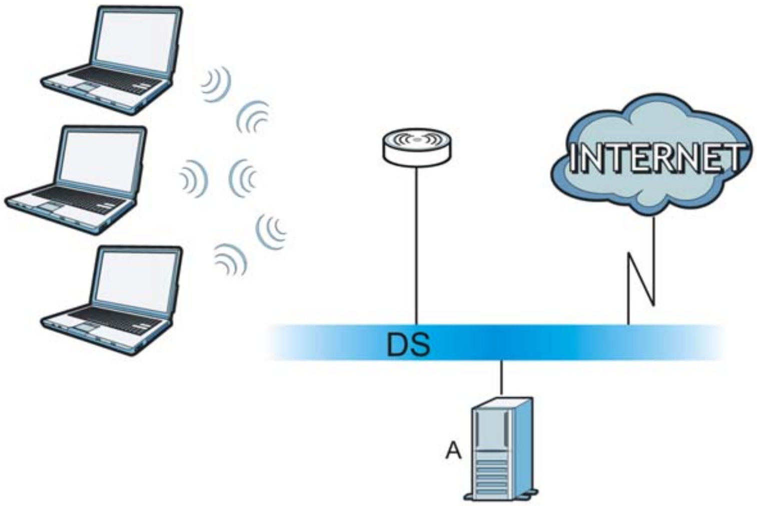
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

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 61 WPA(2) with RADIUS Application Example



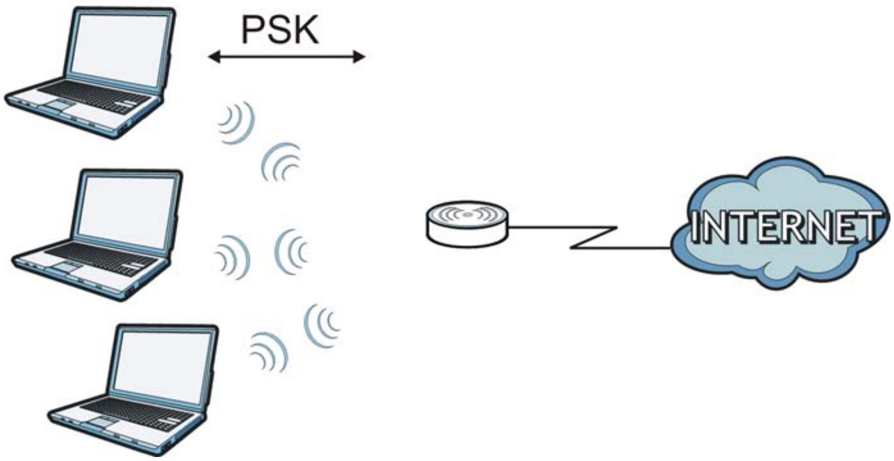
WPA(2)-PSK Application Example

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 62 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 38 Wireless Security Relational Matrix

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

Antenna Overview

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

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

Antenna Characteristics

Frequency

An antenna in the frequency of 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.

C

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.

Certifications

Federal Communications Commission (FCC) Interference Statement

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

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits 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 in accordance with 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/television reception, which can be determined 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:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11n (20MHz) operation of this product in the U.S.A. is firmware-limited to channels 1 through 11. IEEE 802.11n (40MHz) operation of this product in the U.S.A. is firmware-limited to channels 3 through 9.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意 ！

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用
者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現
有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍
受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device is designed for the WLAN 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

Ce produit est conçu pour les bandes de fréquences 5 GHz conformément à la législation Européenne. En France métropolitaine, suivant les décisions n°03-908 et 03-909 de l'ARCEP, la puissance d'émission ne devra pas dépasser 10 mW (10 dB) dans le cadre d'une installation WiFi en extérieur pour les fréquences comprises entre 2454 MHz et 2483,5 MHz.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

1 this device may not cause interference and
2 this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 2dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

IMPORTANT NOTE

Device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems; users should also be cautioned to take note that high-power radars are allocated as primary users (meaning they have priority) of the bands 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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 materials or workmanship for a period of up to two years from the date of purchase. 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.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Regulatory Information

European Union

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

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

Compliance Information for 2.4GHz and 5GHz Wireless Products Relevant to the EU and Other Countries Following the EU Directive 1999/5/EC (R&TTE Directive)

[Czech]	ZyXEL tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
[Danish]	Undertegnede ZyXEL erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
[German]	Hiermit erklärt ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
[Estonian]	Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.

English	Hereby, ZyXEL declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
[Spanish]	Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
[Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ZyXEL ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EC.
[French]	Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.
[Italian]	Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
[Latvian]	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
[Lithuanian]	Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
[Dutch]	Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
[Maltese]	Hawnhekk, ZyXEL, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
[Hungarian]	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EK irányelv egyéb elõírásainak.
[Polish]	Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
[Portuguese]	ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.
[Slovenian]	ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
[Slovak]	ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.
[Finnish]	ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[Swedish]	Härmed intygar ZyXEL att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
[Bulgarian]	С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/EC.
[Icelandic]	Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.
[Norwegian]	Erklærer herved ZyXEL at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 1999/5/EF.
[Romanian]	Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 1999/5/EC.

National Restrictions

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

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

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

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1995/5/CE folgen) mit Außnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2, 4- and 5-GHz 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 inwhich additional restrictions or requirements or both are applicable.

The requirements for any country may evolve. ZyXEL recommends that you check with the local authorities for the latest status of their national regulations for both the 2,4- and 5-GHz wireless LANs.

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

Overview of Regulatory Requirements for Wireless LANs			
Frequency Band (MHz)	Max Power Level (EIRP)[1] (mW)	Indoor ONLY	Indoor and Outdoor

2400-2483.5	100		V
5150-5350	200	V	
5470-5725	1000		V

Belgium

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

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

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

Denmark

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

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

France

For 2.4 GHz, the output power is restricted to 10 mW EIRP when the product is used outdoors in the band 2454 - 2483.5 MHz. There are no restrictions when used indoors or in other parts of the 2.4 GHz band. Check http://www.arcep.fr/ for more details.

Pour la bande 2.4 GHz, la puissance est limitée à 10 mW en p.i.r.e. pour les équipements utilisés en extérieur dans la bande 2454 - 2483.5 MHz. Il n'y a pas de restrictions pour des utilisations en intérieur ou dans d'autres parties de la bande 2.4 GHz. Consultez http://www.arcep.fr/ pour de plus amples détails.

R&TTE 1999/5/EC		
WLAN 2.4 – 2.4835 GHz		
IEEE 802.11 b/g/n		
Location	Frequency Range(GHz)	Power (EIRP)
Indoor (No restrictions)	2.4 – 2.4835	100mW (20dBm)
Outdoor	2.4 – 2.454	100mW (20dBm)
	2.454 – 2.4835	10mW (10dBm)

Italy

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

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

Latvia

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

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

Notes:

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

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

List of national codes

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

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- 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.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. 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.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Index