ZyXEL P-336M

802.11g Wireless MIMO Router

User's Guide

Version 1.00
Edition 1.00
1/2006

ZyXEL

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.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

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 equipment 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 commercial environment. This equipment 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.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment 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.

Notice 1

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

This product has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

Caution

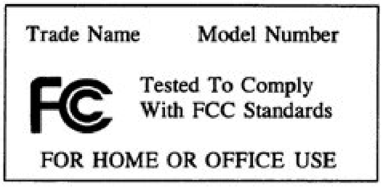
1. The equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).
2. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Certifications

1 Go to www.zyxel.com

2 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page



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。

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 (2) 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 value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is 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 of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Online Registration

Register online at www.zyxel.com for free future product updates and information.

Customer Support

Please have the following information ready when you contact customer support.

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

METHOD	SUPPORT E-MAIL	TELEPHONE[A]	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
CZECH REPUBLIC	info@cz.zyxel.com	+420-241-091-350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská Republika
	info@cz.zyxel.com	+420-241-091-359		
DENMARK	support@zyxel.dk	+45-39-55-07-00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 2860 Soeborg Denmark
	sales@zyxel.dk	+45-39-55-07-07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33-4-72-52-97-97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33-4-72-52-19-20		
GERMANY	support@zyxel.de	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
HUNGARY	support@zyxel.hu	+36-1-3361649	www.zyxel.hu	ZyXEL Hungary 48, Zoldlomb Str. H-1025, Budapest Hungary
	info@zyxel.hu	+36-1-3259100		
KAZAKHSTAN	http://zyxel.kz/support	+7-3272-590-698	www.zyxel.kz	ZyXEL Kazakhstan 43, Dostyk ave.,Office 414 Dostyk Business Centre 050010, Almaty Republic of Kazakhstan
	sales@zyxel.kz	+7-3272-590-689		
NORTH AMERICA	support@zyxel.com	1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	
NORWAY	support@zyxel.no	+47-22-80-61-80	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47-22-80-61-81		

METHOD	SUPPORT E-MAIL	TELEPHONE[A]	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
POLAND	info@pl.zyxel.com	+48-22-5286603	www.pl.zyxel.com	ZyXEL Communications ul.Emilli Plater 53 00-113 Warszawa Poland
		+48-22-5206701		
RUSSIA	http://zyxel.ru/support	+7-095-542-89-29	www.zyxel.ru	ZyXEL Russia Ostrovityanova 37a Str. Moscow, 117279 Russia
	sales@zyxel.ru	+7-095-542-89-25		
SPAIN	support@zyxel.es	+34-902-195-420	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
	sales@zyxel.es	+34-913-005-345		
SWEDEN	support@zyxel.se	+46-31-744-7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
	sales@zyxel.se	+46-31-744-7701		
UKRAINE	support@ua.zyxel.com	+380-44-247-69-78	www.ua.zyxel.com	ZyXEL Ukraine 13, Pimonenko Str. Kiev, 04050 Ukraine
	sales@ua.zyxel.com	+380-44-494-49-32		
UNITED KINGDOM	support@zyxel.co.uk	+44-1344 303044 08707 555779 (UK only)	www.zyxel.co.uk	ZyXEL Communications UK Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)
	sales@zyxel.co.uk	+44-1344 303034	ftp.zyxel.co.uk	

a. “+” is the (prefix) number you enter to make an international telephone call.

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on your purchase of the ZyXEL P-336M 802.11g Wireless MIMO Router.

Note: 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.

Your P-336M is easy to install and configure.

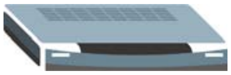
About This User's Guide

This manual is designed to guide you through the configuration of your P-336M for its various applications.

Syntax Conventions

- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- Mouse action sequences are denoted using a comma. For example, "click the Apple icon, **Control Panels** and then **Modem**" means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity's sake, we will use "e.g.," as a shorthand for "for instance", and "i.e.," for "that is" or "in other words" throughout this manual.
- The ZyXEL P-336M 802.11g Wireless MIMO Router may be referred to as the P-336M in this user's guide.

Graphics Icons Key

Wireless Access Point 	Computer 	Notebook Computer
Server 	Modem 	Wireless Signal
Telephone 	Switch 	Router
Internet Cloud 		

Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. They contain hardware installation/connection information.

- ZyXEL Glossary and Web Site

  Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

User Guide Feedback

Help us help you. E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

CHAPTER 1 Getting Started

This chapter introduces the P-336M features and front panel LEDs.

1.1 About Your P-336M

The ZyXEL P-336M 802.11g Wireless MIMO Router is an 802.11g high-performance, wireless router that supports high-speed wireless networking in the Home, SOHO, or SMB network environments.

Unlike most routers, the P-336M provides data transfers at up to 108 Mbps (compared to the standard 54 Mbps) when connecting to other compatible MIMO (Multiple Input Multiple Output) devices. The P-336M is also backwards compatible with older IEEE 802.11b networks making it a true versatile device. This means that there is no need to change your entire network to maintain connectivity. IEEE 802.11b has a lower throughput rate than IEEE 802.11g, but any IEEE 802.11b devices can still connect to an IEEE 802.11g network. You may choose to slowly change your network by gradually replacing IEEE 802.11b devices with IEEE 802.11g devices.

1.2 Features

The following lists the features of your P-336M.

- Supports IEEE 802.11b/g 2.4GHz WLAN with 2.412 to 2.484GHz frequency band operation.
- Supports MIMO to increase both transmission speed (with SuperG) and range of your wireless network.
- Intelligent receiving with directional antennas for faster throughput and longer ranges.
- Intelligent transmissions for a more efficient performing network.
- Built-in StreamEngine™ feature allowing intelligent and automatic traffic prioritizing.
- Data rates of 1,2.5.5,6,9, 11,12,18,24,36,48,54Mbps and Turbo Mode speed at up to 108Mbps.

Note: Turbo Mode is an Atheros^{TM} proprietary speed-boosting technology that must be used in conjunction with other devices using the Atheros^{TM} radio technology.

- Hardware encryption for Wi-Fi Protected Access (WPA2/WPA) and Wired Equivalent Privacy (WEP) without performance degradation.

- WPA2/WPA (Wi-Fi Protected Access) authorizes and identifies users based with a secret key that changes automatically at regular intervals, for example: Pre Shared Key mode means that the home user, without a RADIUS server, will obtain a new security key every time he or she connects to the network, vastly improving the safety of communications on the said network.
- User-friendly configuration and diagnostic utilities.
- Connect multiple computers to a Cable or DSL modem to share a single Internet connection.
- DHCP server enables all networked computers to automatically receive IP addresses.
- Web-based interface for easy management and configuration.
- Supports multi-connection applications.
- Equipped with four 10/100 Ethernet ports, one WAN port all with Auto MDI/MDIX.

1.3 Hardware Connection and Wizard Setup

Follow the instructions in the Quick Start Guide to connect the P-336M and configure the wizard screens.

1.3.1 Front Panel LEDs

The following table describes the front panel LEDs.

Table 1 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR		Off	The P-336M is not receiving power.
	Green	On	The P-336M is receiving power and ready.
		Blinking	The P-336M is resetting to the factory defaults.
LAN		Off	No device is connected to this port.
	Green	On	An Ethernet device is connected to this port.
		Blinking	The P-336M is sending/receiving data on this port.
WAN		Off	The WAN connection is not ready, or has failed.
	Green	On	The P-336M has a successful WAN connection.
		Blinking	The P-336M is sending/receiving data.
WLAN		Off	The WLAN connection is turned off.
	Green	On	The WLAN is active.
		Blinking	The WLAN is sending/receiving data.
USB		Off	The USB port is currently not in use
	Green	Blinking (3 Times)	Windows Connect Now setup is successful.
		Blinking (Continuous)	Windows Connect Now setup is not successful.

CHAPTER 2 The Web Configurator

This chapter introduces you to the P-336M web configurator, gives an overview of the screen menus and describes the common screen buttons.

2.1 Introduction

The web configurator is an HTML-based management interface that allows easy Prestige setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 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.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Note: By default, you can only access the web configurator through a LAN port. To access via the WAN, enable remote management in the **Admin** screen.

2.2 Login

Follow the steps below to log into the web configurator.

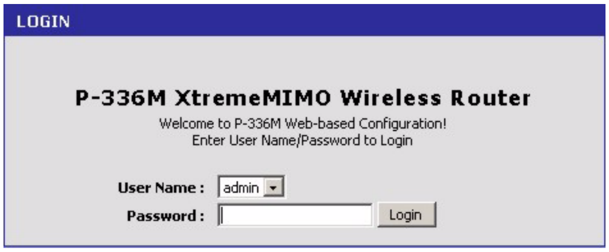
1 Start your web browser.

2 Type "http://" and the IP address of the Prestige (for example, the default is 192.168.1.1) in the Location or Address field. Press [ENTER].

3 The login screen appears. Select **admin** in the **User Name** field to log in as an administrator.

4 Enter the associated password. The default administrative login password is "1234".

Figure 1 Web Configurator: Login



LOGIN

P-336M XtremeMIMO Wireless Router

Welcome to P-336M Web-based Configuration!
Enter User Name/Password to Login

User Name : admin

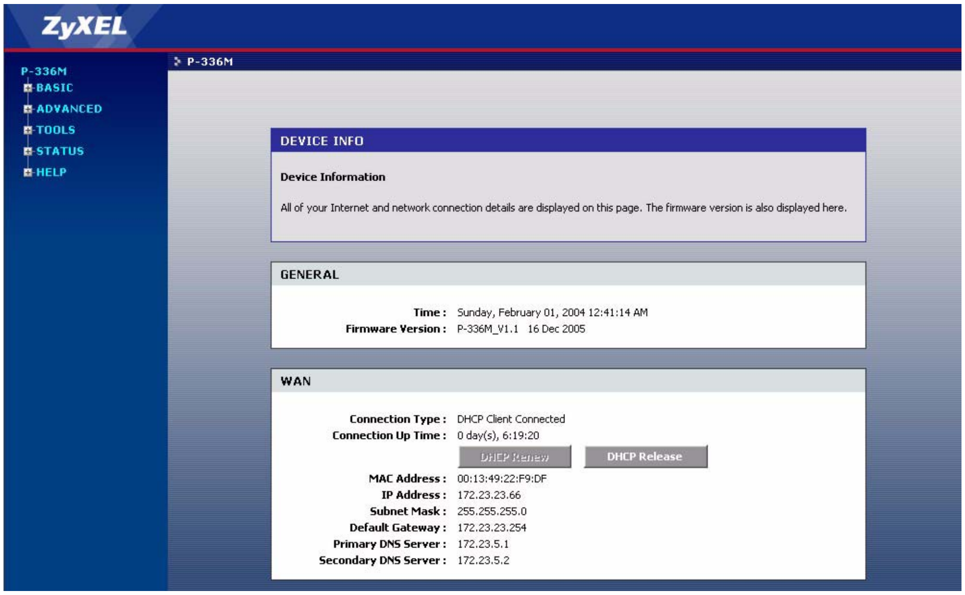
Password :

5 Click **Login** to view the first web configurator screen.

2.3 The DEVICE INFO Screen

The **Device Info** screen is the first screen that displays when you access the web configurator.

Figure 2 Device Info



DEVICE INFO

Device Information

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

GENERAL

Time : Sunday, February 01, 2004 12:41:14 AM
Firmware Version : P-336M_V1.1 16 Dec 2005

WAN

Connection Type : DHCP Client Connected
Connection Up Time : 0 day(s), 6:19:20
MAC Address : 00:13:49:22:F9:DF
IP Address : 172.23.23.66
Subnet Mask : 255.255.255.0
Default Gateway : 172.23.23.254
Primary DNS Server : 172.23.5.1
Secondary DNS Server : 172.23.5.2

The following table lists the various web configurator screens within the sub-links.

Table 2 Web Configurator Screen Sub-Menus

BASIC	ADVANCED	TOOLS	STATUS	HELP
Start WAN LAN DHCP Wireless	Game Hosting Virtual Server Applications StreamEngine Routing Access Control Web Filter MAC Filter Firewall Inbound Filter Wireless Schedules	Admin Time Syslog E-mail System Firmware DDNS	Device Info Wireless Logs Statistics	Menu Basic Advanced Tools Status Glossary

2.4 Web Configurator Screen Buttons

The following table describes the common button in the web configurator.

Table 3 Web Configurator Screen Icons

BUTTON	DESCRIPTION
Save Settings	Click this button to save all changes permanently to the device.
Discard Settings	Click this button to discard all changes. **Note:** All unsaved changes in all screens will be lost.
Save	Click this button to save the changes of a configuration screen for the current session.
Clear	Click this button to start configuring a screen again.
✎	Click this button to change the settings of the selected rule.
⊖	Click this button to remove the selected rule.

2.5 Saving Configuration Changes

Note: You must save the current configuration in the P-336M to make the changes take effect.

Do NOT turn off the P-336M during the updating process, as it may corrupt the firmware and make your P-336M unusable.

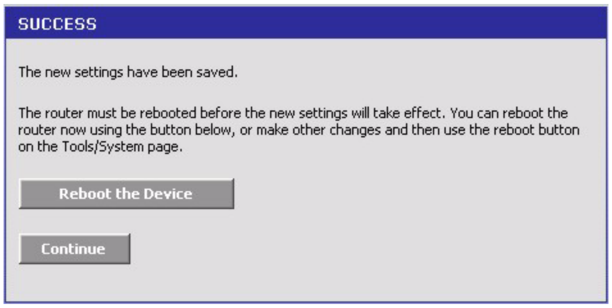
Follow the steps below to save the configuration changes.

1 Click **Save Settings** on the top of a configuration screen.

2 A **Success** screen displays.

- Click **Reboot the Device** to restart the P-336M and make the changes take effect. Wait before the P-336M finishes rebooting before accessing the web configurator again.
- Click **Continue** to return to the previous configuration screen without saving the changes.

Figure 3 Save Settings: Success



SUCCESS

The new settings have been saved.

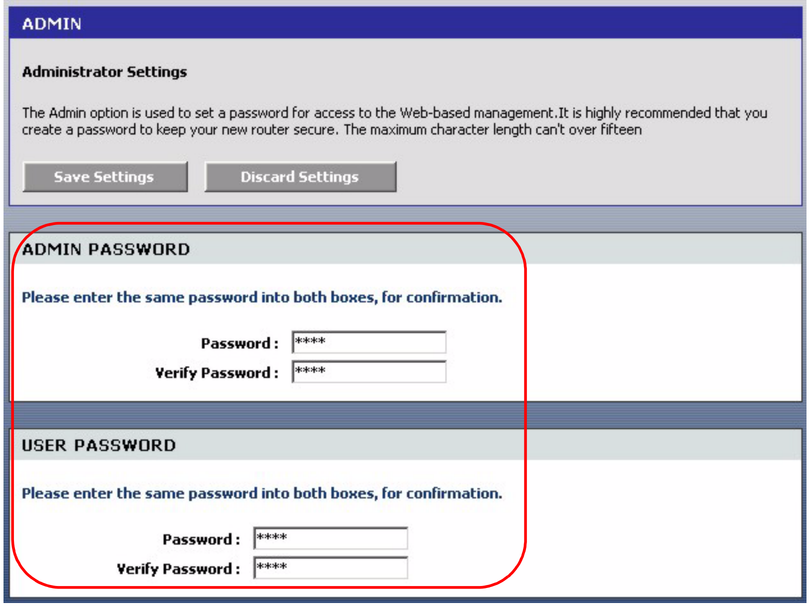
The router must be rebooted before the new settings will take effect. You can reboot the router now using the button below, or make other changes and then use the reboot button on the Tools/System page.

2.6 Changing Your Password

It is highly recommended that you periodically change the password for accessing the Prestige. If you didn't change the default one after you logged in or you want to change to a new password again, then click **Tools** > **Admin** to display the screen as shown next.

Configure the password fields, click **Save Settings** and reboot the device to make the changes take effect.

Figure 4 Change Password



Administrator Settings

The Admin option is used to set a password for access to the Web-based management.It is highly recommended that you create a password to keep your new router secure. The maximum character length can't over fifteen

Please enter the same password into both boxes, for confirmation.

Password : ****
Verify Password : ****

Please enter the same password into both boxes, for confirmation.

Password : ****
Verify Password : ****

The following table describes the related fields in this screen.

Table 4 Change Password

LABEL	DESCRIPTION
Admin Password	
Password	Type the new password in this field.
Verify Password	Type the new password again in this field.
User Password	
Password	Type the new password in this field.
Verify Password	Type the new password again in this field.

CHAPTER 3 Basic

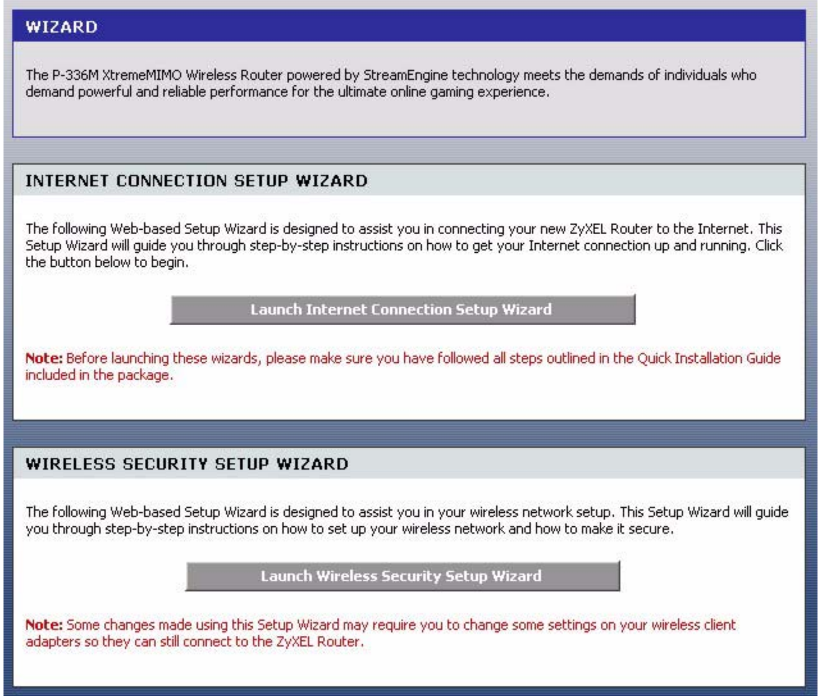
This chapter describes the Basic screens you use to configure the wizards, LAN, WAN and WLAN settings.

3.1 Setup Wizards

You can use the wizard screens to configure the P-336M for Internet access and secure wireless connection.

Click **Basic** > **Start** to display the main **Wizard** screen.

Figure 5 Basic: Start (Wizard)



WIZARD

The P-336M XtremeMIMO Wireless Router powered by StreamEngine technology meets the demands of individuals who demand powerful and reliable performance for the ultimate online gaming experience.

INTERNET CONNECTION SETUP WIZARD

The following Web-based Setup Wizard is designed to assist you in connecting your new ZyXEL Router to the Internet. This Setup Wizard will guide you through step-by-step instructions on how to get your Internet connection up and running. Click the button below to begin.

Note: Before launching these wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

WIRELESS SECURITY SETUP WIZARD

The following Web-based Setup Wizard is designed to assist you in your wireless network setup. This Setup Wizard will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.

Note: Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the ZyXEL Router.

Refer to the Quick Start Guide for how to configure wizard screens. You can configure advanced settings in the **WAN** screen.

3.2 WAN Overview

The P-336M offers three Internet access modes: **Static IP**, **Dynamic IP** and **PPPoE**. To configure advanced Internet access settings, click **Basic > WAN** to display the configuration screen. This screen varies depending on the Internet access mode you select.

3.2.1 WAN IP Address Assignment

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

Table 5 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

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

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

3.2.2 DNS Server Address Assignment

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

The P-336M can get the DNS server addresses in the following ways.

1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.

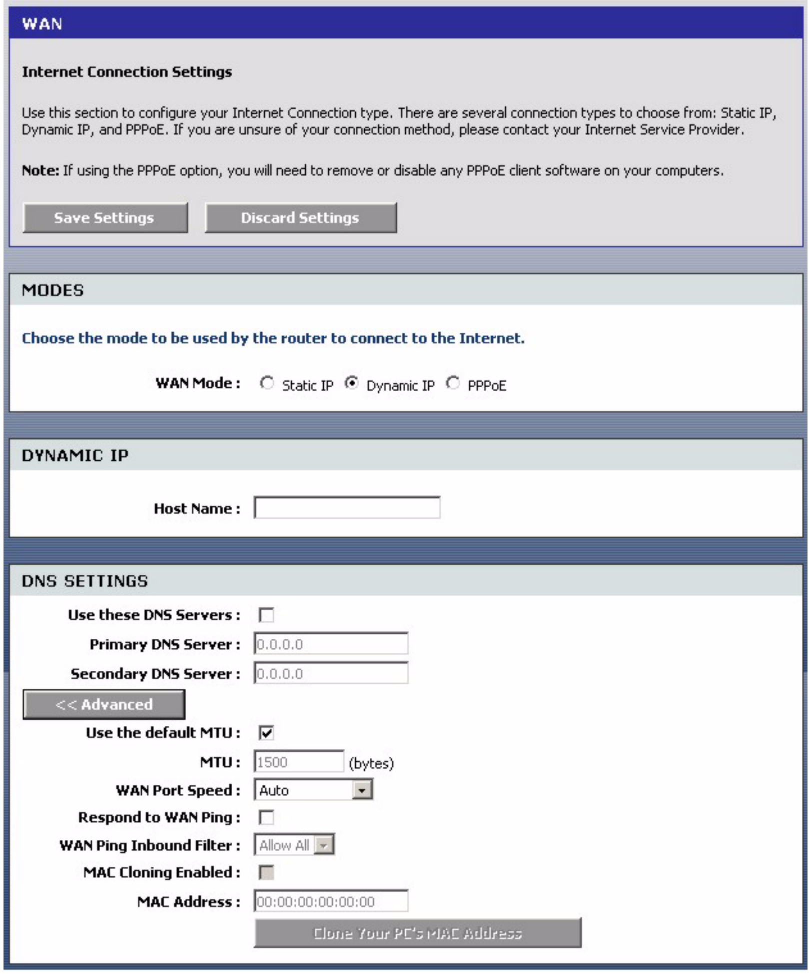
2 If your ISP dynamically assigns the DNS server IP addresses (along with the P-336M's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

3 You can manually enter the IP addresses of other DNS servers. These servers can be public or private. A DNS server could even be behind a remote IPSec router.

3.2.3 WAN Configuration

Select **Dynamic IP** in the **WAN** screen if your ISP does not give you a fixed public IP address and Internet access account information (such as the user name and password).

Figure 6 Basic: WAN: Dynamic IP



WAN

Internet Connection Settings

Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, Dynamic IP, and PPPoE. If you are unsure of your connection method, please contact your Internet Service Provider.

Note: If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.

MODES

Choose the mode to be used by the router to connect to the Internet.

WAN Mode : ○ Static IP ● Dynamic IP ○ PPPoE

DYNAMIC IP

Host Name :

DNS SETTINGS

Use these DNS Servers : □

Primary DNS Server : 0.0.0.0

Secondary DNS Server : 0.0.0.0

Use the default MTU : ☑

MTU : 1500 (bytes)

WAN Port Speed : Auto

Respond to WAN Ping : □

WAN Ping Inbound Filter : Allow All

MAC Cloning Enabled : □

MAC Address : 00:00:00:00:00:00

The following table describes the fields in this screen.

Table 6 Basic: WAN: Dynamic IP

LABEL	DESCRIPTION
MODES	
WAN	Select **Dynamic IP** if you are not given a fixed public IP address and account information (such as the user name and password).
Dynamic IP	

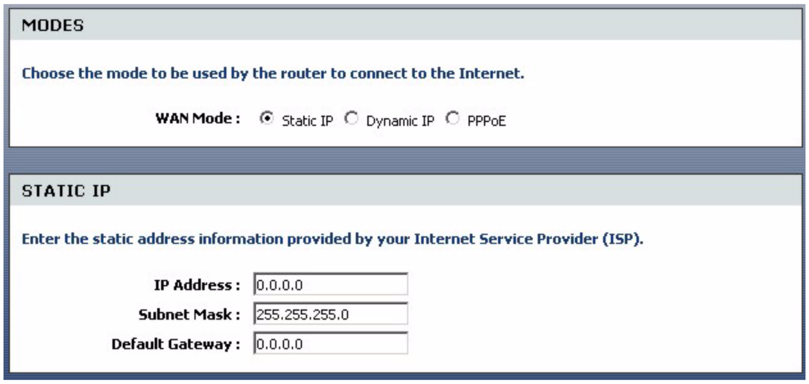
Table 6 Basic: WAN: Dynamic IP (continued)

LABEL	DESCRIPTION
Hostname	This field is optional. Enter your computer's hostname which the ISP checks before Internet access is allowed.
DNS Settings	
Use these DNS Servers	Select this option to manually enter the DNS server IP address(es) in the field(s) provided.
Primary/Secondary DNS Server	Enter the IP address (provided by your ISP) of the DNS server in dotted decimal notation. For example, 192.168.1.1.
Advanced	Click **Advanced** to display advanced WAN configuration fields.
Use the Default MTU	Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the P-336M will send to the WAN. If LAN devices send larger packets, the P-336M will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Select this option to use the default MTU. Clear this checkbox to manually enter an MTU size below.
MTU	Enter the MTU size (between 256 and 2296). Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. Make sure the MTU size matches the ISP's network or Internet connection may fail.
WAN Port Speed	Select a port speed in the field.
Respond to WAN Ping	Select this option to set the P-336M to reply to ping packets. Clear this check box if you don't want the P-336M to send ping replies.
WAN Ping Inbound Filter	Select a control action for accessing the P-336M on the WAN. You can configure the filter settings in the **Advanced > Inbound Filter** screen.
MAC Cloning Enabled	Select this option to set the P-336M to copy the MAC address of your computer.
MAC Address	Enter the IP address of the computer on the LAN whose MAC you are cloning. It is recommended that you clone the MAC address prior to hooking up the WAN port.
Clone Your PC's MAC Address	Click **Clone Your PC's MAC Address** to have the P-336M automatically copy the MAC address from your computer.

3.2.4 WAN Configuration: Static IP

Select **Dynamic IP** in the **WAN** screen when your ISP gives you a fixed public IP address.

Figure 7 Basic: WAN: Static IP



MODES

Choose the mode to be used by the router to connect to the Internet.

WAN Mode : ● Static IP ○ Dynamic IP ○ PPPoE

STATIC IP

Enter the static address information provided by your Internet Service Provider (ISP).

IP Address : 0.0.0.0

Subnet Mask : 255.255.255.0

Default Gateway : 0.0.0.0

The following table describes the related fields in this screen.

Table 7 Basic: WAN: Static IP

LABEL	DESCRIPTION
MODES	
WAN	Select **Static IP** if your ISP gives you a fixed public IP address.
Static IP	
IP Address	Enter your WAN IP address in dotted decimal notation (for example, 192.168.1.1).
Subnet Mask	Enter the IP subnet mask (if your ISP gave you one) in dotted decimal notation (for example, 255.255.255.0).
Default Gateway	Enter the gateway IP address (if your ISP gave you one) in dotted decimal notation.

3.2.5 WAN Configuration: PPPoE

The P-336M supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a computer interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius). PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

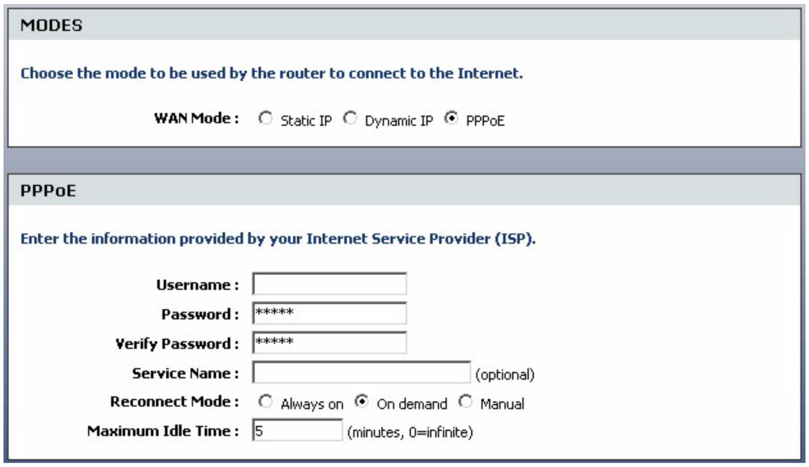
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the P-336M (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the P-336M does that part of the task. Furthermore, with NAT, all of the LAN computers will have access.

Select **PPPoE** in the **WAN** screen.

Figure 8 Basic: WAN: PPPoE



MODES

Choose the mode to be used by the router to connect to the Internet.

WAN Mode : ○ Static IP ○ Dynamic IP ● PPPoE

PPPoE

Enter the information provided by your Internet Service Provider (ISP).

Username :	
Password :	*****
Verify Password :	*****
Service Name :	(optional)
Reconnect Mode :	○ Always on ● On demand ○ Manual
Maximum Idle Time :	5 (minutes, 0=infinite)

The following table describes the related fields in this screen.

Table 8 Basic: WAN: PPPoE

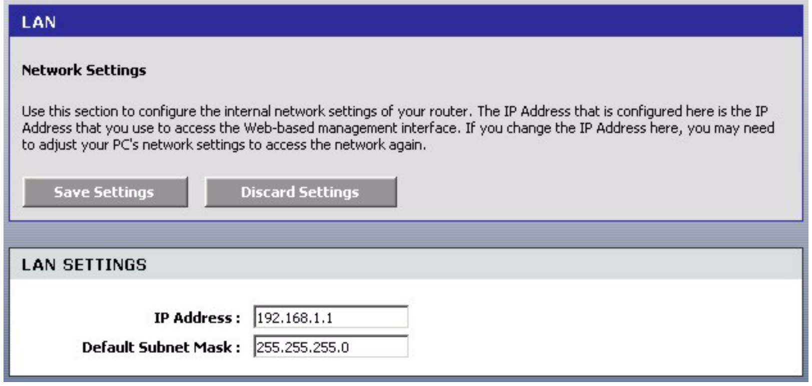
LABEL	DESCRIPTION
MODES	
WAN	Select **PPPoE** if your ISP gives you Internet access account information (such as the username and password).
Username	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Verify Password	Type your password again to make sure that you have entered is correctly.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
Reconnect Mode	Specify how you want to re-establish an Internet connection after the idle timeout. Select **Always On** when you want your connection up all the time. The P-336M will try to bring up the connection automatically if it is disconnected. Select **On Demand** when you don't want the connection up all the time and specify an idle time-out in the **Maximum Idle Timeout** field. Select **Manual** when you want to manually re-establish the connection if it is disconnected.
Maximum Idle Time	This value specifies the time in seconds that elapses before the P-336M automatically disconnects from the PPPoE server.

3.3 LAN Setup

Local Area Network (LAN) is a shared communication system to which many computers are attached. Use **LAN** screen to set the IP address and subnet mask of the LAN interface on the P-336M.

Click **Basic** > **LAN** to display the configuration screen.

Figure 9 Basic: LAN



LAN

Network Settings

Use this section to configure the internal network settings of your router. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

LAN SETTINGS

IP Address : 192.168.1.1

Default Subnet Mask : 255.255.255.0

The following table describes the labels in this screen.

Table 9 Basic: LAN

LABEL	DESCRIPTION
LAN Setting	
IP Address	Type the IP address of your P-336M in dotted decimal notation. 192.168.167.1 is the factory default. Alternatively, click the right mouse button to copy and/or paste the IP address.
Default Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your P-336M automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the P-336M.

3.4 DHCP Overview

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the P-336M as a DHCP server or disable it. When configured as a server, the P-336M provides the TCP/IP configuration for the DHCP client. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

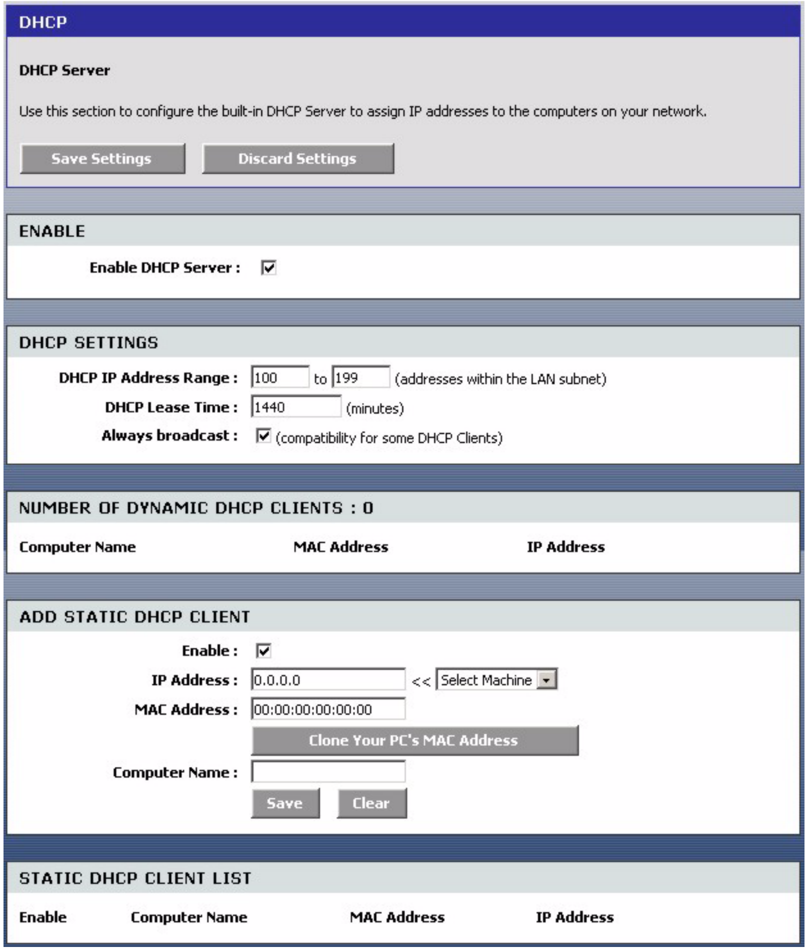
3.4.1 IP Pool Setup

The P-336M is pre-configured to provide IP addresses (ranging from 192.168.1.100 to 192.168.1.199) to DHCP clients. This configuration leaves some IP addresses (excluding the P-336M itself) in the lower and upper ranges for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

3.4.2 DHCP Setup

Click **Basic** > **DHCP** to display the configuration screen.

Figure 10 Basic: DHCP



DHCP

DHCP Server

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

ENABLE

Enable DHCP Server : ☑

DHCP SETTINGS

DHCP IP Address Range : 100 to 199 (addresses within the LAN subnet)

DHCP Lease Time : 1440 (minutes)

Always broadcast : ☑ (compatibility for some DHCP Clients)

NUMBER OF DYNAMIC DHCP CLIENTS : 0

Computer Name	MAC Address	IP Address

ADD STATIC DHCP CLIENT

Enable : ☑

IP Address : 0.0.0.0 << Select Machine

MAC Address : 00:00:00:00:00:00

Computer Name :

STATIC DHCP CLIENT LIST

Enable	Computer Name	MAC Address	IP Address

The following table describes the labels in this screen.

Table 10 Basic: DHCP

LABEL	DESCRIPTION
ENABLE	
Enable DHCP Server	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Select this option to set the P-336M to assign network information (IP address, DNS information etc.) to an Ethernet device connected to the **LAN** ports. Clear this check box to stop the P-336M from acting as a DHCP server. you must have another DHCP server on your LAN, or else the computer must be manually configured.
DHCP SETTINGS	
DHCP Address Range	Specify the starting and end IP address for the DHCP clients.
DHCP Lease Time	Specify the time (in minutes) a DHCP client is allowed to use the assigned IP address from the P-336M. Once the lease time is up, the DHCP client has to renew the lease.
NUMBER OF DYNMAIC DHCP CLIENTS	This field displays the number of DHCP clients.
Computer Name	This field displays the name of the DHCP client computer.
MAC Address	This field displays the MAC address of the DHCP client computer.
IP Address	This field displays the IP address of the DHCP client computer.
ADD STATIC DHCP CLIENT	
Enable	Select this option to enable static DHCP to set the P-336M to assign one IP address on the LAN to a specific computer based on the MAC address. Clear this check box to disable this feature.
IP Address	Type the IP address that you want to assign to the computer on your LAN. Alternatively, select from the list of dynamic client computer names in the drop-down list box.
MAC Address	Type the MAC address (with colons) of a computer on your LAN. Or click **Clone Your PC’s MAC Address** to copy the MAC address of your computer.
Computer Name	Enter the name of the DHCP client computer. This is for identification purposes.
Save	Click **Save** to save the settings in this part of the screen.
Clear	Click **Clear** to start configuring this part of the screen again.
STATIC DHCP CLIENT LIST	
Enable	This field displays whether this static DHCP setting is active or not.
Computer Name	This field displays the name of the DHCP client computer.
MAC Address	This field displays the MAC address.
IP Address	This field displays the IP address of the MAC address.

3.5 Wireless LAN Overview

This section introduces the wireless LAN features.

3.5.1 SSID

The SSID (Service Set Identity) is a unique name shared among all wireless devices in a wireless network. Wireless devices must have the same SSID to communicate with each other.

3.5.2 Channel

A radio frequency used by a wireless device is called a channel.

3.5.3 Transmission Rate (Tx Rate)

The P-336M provides various transmission (data) rate options for you to select. In most networking scenarios, the factory default **Best (Automatic)** setting proves the most efficient. This setting allows your P-336M to operate at the maximum transmission (data) rate. When the communication quality drops below a certain level, the P-336M automatically switches to a lower transmission (data) rate. Transmission at lower data speeds is usually more reliable. However, when the communication quality improves again, the P-336M gradually increases the transmission (data) rate again until it reaches the highest available transmission rate. You can select any of the above options. If you wish to balance speed versus reliability, select **54 Mbps** in a networking environment where you are certain that all wireless devices can communicate at the highest transmission (data) rate. **1 Mbps** or **2 Mbps** are used often in networking environments where the range of the wireless connection is more important than speed.

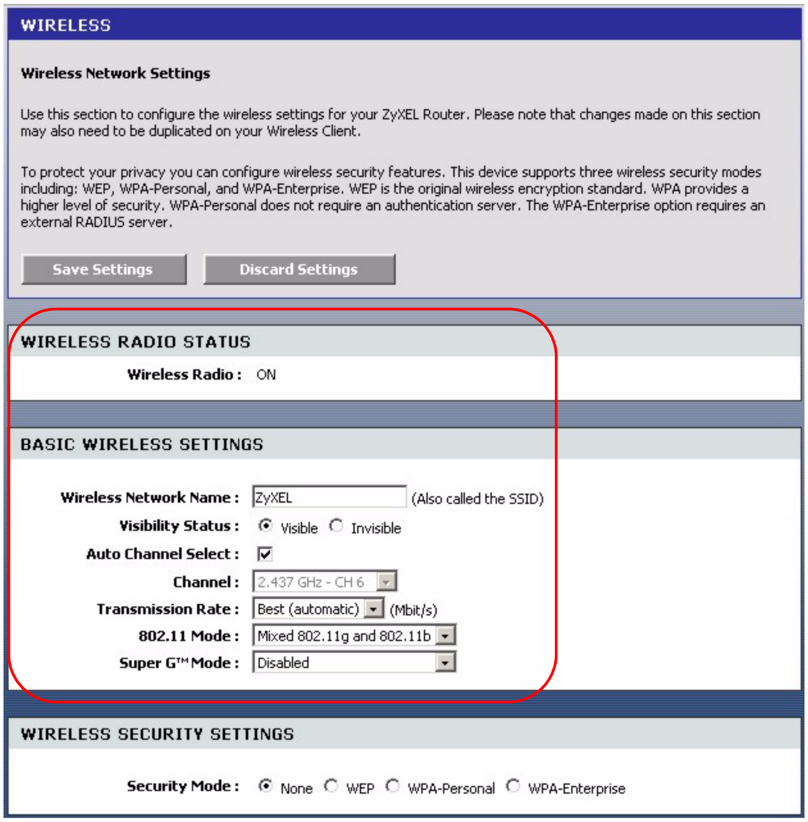
3.5.3.1 SuperG^{TM}

The SuperG technology works with IEEE 802.11 a/b/g products. It doubles IEEE 802.11g performance by bonding two 54Mbps channels and allowing larger frames to be sent. IEEE 802.11g wireless LAN devices using Super G can transmit at up to 108 Mbps.

3.6 Basic Wireless LAN Setup

Click **Basic > Wireless** to display the configuration screen.

Figure 11 Basic: Wireless: Basic Wireless LAN Setup



WIRELESS

Wireless Network Settings

Use this section to configure the wireless settings for your ZyXEL Router. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

WIRELESS RADIO STATUS

Wireless Radio : ON

BASIC WIRELESS SETTINGS

Wireless Network Name : ZyXEL (Also called the SSID)

Visibility Status : ● Visible ○ Invisible

Auto Channel Select : ☑

Channel : 2.437 GHz - CH 6

Transmission Rate : Best (automatic) (Mbit/s)

802.11 Mode : Mixed 802.11g and 802.11b

Super G™ Mode : Disabled

WIRELESS SECURITY SETTINGS

Security Mode : ● None ○ WEP ○ WPA-Personal ○ WPA-Enterprise

THe following table describes the related labels in this screen.

Table 11 Basic: Wireless: Basic WIreless LAN Setup

LABEL	DESCRIPTION
WIRELESS RADIO STATUS	This field displays whether the wireless LAN feature is enabled (**ON**) or disabled (**OFF**). You can enable and disable the wireless LAN feature on the P-336M by using the wireless LAN switch at the rear panel of the P-336M. Refer to the Quick Start Guide for more information.
BASIC WIRELESS SETTINS	
Wireless Network Name	The SSID (Service Set IDentification) is a unique name to identify the P-336M in the wireless LAN. Wireless stations associating to the Prestige must have the same SSID. Enter a descriptive name of up to 32 printable characters (including spaces; alphabetic characters are case-sensitive).
Visibility Status	Select **Invisible** to hide the SSID in so a station cannot obtain the SSID through AP scanning. Select **Visible** to make the ESSID visible so a station can obtain the SSID through AP scanning.
Automatic Channel Select	Select this option to set the P-336M to select the optimum channel in the wireless network.

Table 11 Basic: Wireless: Basic WIreless LAN Setup (continued)

LABEL	DESCRIPTION
Channel	The radio frequency used by IEEE 802.11 wireless devices is called a channel. Select a channel from the drop-down list box.
Transmission Rate	Select a transmission speed from the drop-down list box.
802.11 Mode	Select **802.11b only** to have the P-336M connect to an IEEE 802.11b wireless device only and vice versa. Select **Mixed 802.11b and 802.11g** to have the P-336M connect to either an IEEE 802.11g or IEEE 802.11b wireless device. Select **802.11g only** to have the P-336M connect to an IEEE 802.11g wireless device only and vice versa.
SuperG^{TM} Mode	Select the check box to have the P-336M transmit at up to 108 Mbps when connected to an AP or wireless router with the SuperG feature enabled.

3.7 Wireless LAN Security Overview

Wireless LAN security is vital to your network to protect wireless communications.

Configure the wireless LAN security using the **Wireless** screen. If you do not enable any wireless security on your P-336M, the P-336M’s wireless communications are accessible to any wireless networking device that is in the coverage area.

3.7.1 WEP

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the P-336M and other wireless stations to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

There are two ways to create WEP keys in your P-336M.

- Automatic WEP key generation based on a “password phrase” called a passphrase. The passphrase is case sensitive. You must use the same passphrase for all WLAN adapters with this feature in the same WLAN.
- Enter the WEP keys manually.

  Your P-336M allows you to configure up to four 64-bit or 128-bit WEP keys and only one key is used as the default key at any one time.

3.7.1.1 Authentication Type

The IEEE 802.11b/g standard describes a simple authentication method between the wireless stations and AP. Three authentication modes are defined: **Open** and **Shared Key**.

- **Open** mode is implemented for ease-of-use and when security is not an issue. The wireless station and the AP do *not* share a secret key. Thus the wireless stations can associate with any AP and listen to any data transmitted plaintext.
- **Shared Key** mode involves a shared secret key to authenticate the wireless station to the AP. This requires you to enable the WEP encryption and specify a WEP key on both the wireless station and the AP.

3.7.2 IEEE 802.1x

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using an external RADIUS server.

3.7.2.1 EAP Authentication

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.

3.7.3 WPA(2)

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. Key differences between WPA(2) and WEP are user authentication and improved data encryption.

3.7.3.1 User Authentication

WPA(2) applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database.

Therefore, if you don't have an external RADIUS server, you should use WPA(2)-PSK (WPA - 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 client will be granted access to a WLAN.

3.7.3.2 Encryption

WPA(2) improves data encryption by using Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES), Message Integrity Check (MIC) and IEEE 802.1x.

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates 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 pair-wise key 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.

AES (Advanced Encryption Standard) is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data.

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.

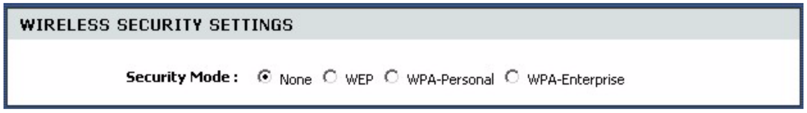
By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

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 an easier-to-use, consistent, single, alphanumeric password.

3.8 WLAN Security Setup

Configure wireless LAN security settings in the Wireless screen. Click **Basic > Wireless** to display the configuration screen. This screen varies depending on the option you select in the **Security Mode** field.

Figure 12 Basic: Wireless: WLAN Security Setup



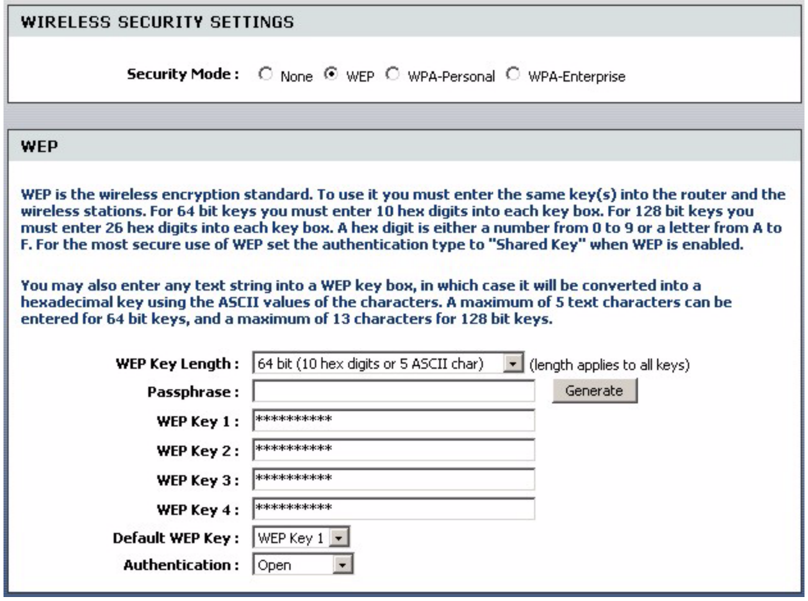
WIRELESS SECURITY SETTINGS

Security Mode : ● None ○ WEP ○ WPA-Personal ○ WPA-Enterprise

3.8.1 WLAN Security Setup: WEP

To configure basic WEP key encryption, select **WEP** in the **Security Mode** field in the **Wireless** screen.

Figure 13 Basic: Wireless: WLAN Security Setup: WEP



WIRELESS SECURITY SETTINGS

Security Mode : ○ None ● WEP ○ WPA-Personal ○ WPA-Enterprise

WEP

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WEP Key Length :	64 bit (10 hex digits or 5 ASCII char) (length applies to all keys)
Passphrase :	Generate
WEP Key 1 :	**********
WEP Key 2 :	**********
WEP Key 3 :	**********
WEP Key 4 :	**********
Default WEP Key :	WEP Key 1
Authentication :	Open

The following table describes the related fields in this screen.

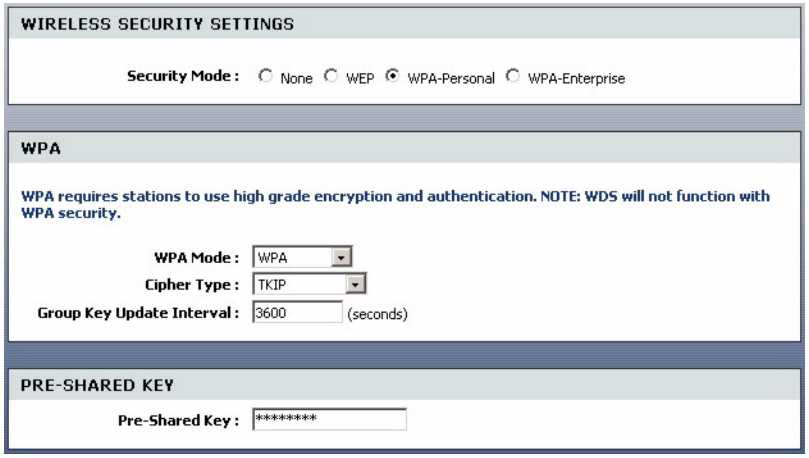
Table 12 Basic: Wireless: WLAN Security Setup: WEP

LABEL	DESCRIPTION
WEP	
WEP Key Length	WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network. Select **64-bit** or **128-bit** to use data encryption.
Passphrase	Enter a "passphrase" (password phrase) of up to 63 case-sensitive printable characters and click **Generate** to have the P-336M create four different WEP keys.
Generate	After you enter the passphrase, click **Generate** to have the P-336M generate four different WEP keys automatically. The keys display in the fields below.
Key 1 .. 4	The WEP keys are used to encrypt data. Both the P-336M and the wireless stations must use the same WEP key for data transmission. If you want to manually set the WEP keys, enter the key in the field provided. If you chose **64-bit**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). The values for the WEP keys must be set up exactly the same on all wireless devices in the same wireless LAN. You must configure all four keys, but only one key can be used at any one time. The default key is key 1.
Default Key	Select a default WEP key to use for data encryption.
Authentication	Select an authentication method. Choices are **Shared Key** and **Open**.

3.8.2 WLAN Security Setup: WPA-Personal

If you want better WLAN security than WEP but do not have a RADIUS server on your network, select **WPA-Personal** in the **Security Mode** field in the **Wireless** screen.

Figure 14 Basic: Wireless: WLAN Security Setup: WPA-Personal



WIRELESS SECURITY SETTINGS

Security Mode : ○ None ○ WEP ● WPA-Personal ○ WPA-Enterprise

WPA

WPA requires stations to use high grade encryption and authentication. NOTE: WDS will not function with WPA security.

WPA Mode : WPA

Cipher Type : TKIP

Group Key Update Interval : 3600 (seconds)

PRE-SHARED KEY

Pre-Shared Key : ********

The following table describes the related labels in this screen.

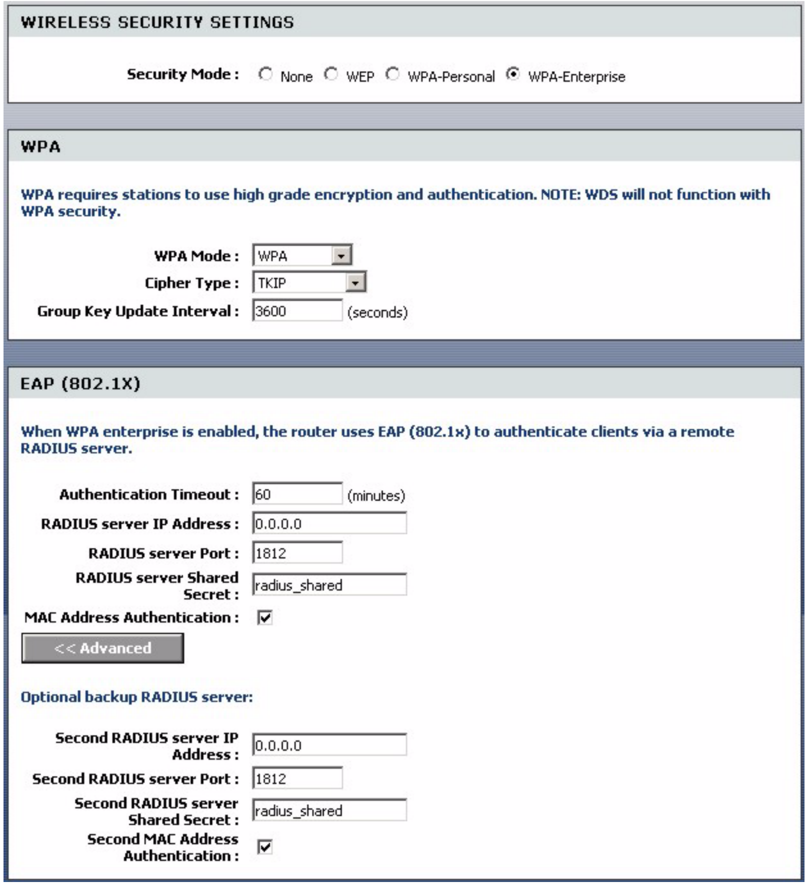
Table 13 Basic: WLAN Security Setup: WPA-Personal

LABEL	DESCRIPTION
WPA	
WPA Mode	Specify a WPA mode. Make sure the peer device(s) is also set to use the same WPA mode. Select **WPA** to set the P-336M to use WPA only. WPA is a older implementation than WPA2. Select **WPA2** to set the P-336M to use WPA2 first and then WPA if connection fails with WPA2. Select **WPA2 Only** to set the P-336M to use WPA2 only.
Cipher Type	Specify the encryption mechanism. Select **TKIP**, **AES** or **TKIP and AES**.
Group Key Update Interval	This is the rate at which an AP or RADIUS server sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Enter an update time in seconds.
PRE SHARED KEY	
Pre-Shared Key	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).

3.8.3 WLAN Security Setup: WPA-Enterprise

If you want better WLAN security than WEP and have a RADIUS server on your network, select **WPA-Enterprise** in the **Security Mode** field in the **Wireless** screen.

Figure 15 Basic: Wireless: WLAN Security Setup: WPA-Enterprise



WIRELESS SECURITY SETTINGS

Security Mode : ○ None ○ WEP ○ WPA-Personal ● WPA-Enterprise

WPA

WPA requires stations to use high grade encryption and authentication. NOTE: WDS will not function with WPA security.

WPA Mode : WPA

Cipher Type : TKIP

Group Key Update Interval : 3600 (seconds)

EAP (802.1X)

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

Authentication Timeout : 60 (minutes)

RADIUS server IP Address : 0.0.0.0

RADIUS server Port : 1812

RADIUS server Shared Secret : radius_shared

MAC Address Authentication : ☑

Optional backup RADIUS server:

Second RADIUS server IP Address : 0.0.0.0

Second RADIUS server Port : 1812

Second RADIUS server Shared Secret : radius_shared

Second MAC Address Authentication : ☑

The following table describes the related labels in this screen.

Table 14 Basic: WLAN Security Setup: WPA-Enterprise

LABEL	DESCRIPTION
WPA	
WPA Mode	Specify a WPA mode. Make sure the peer device(s) is also set to use the same WPA mode. Select **WPA** to set the P-336M to use WPA only. WPA is a older implementation than WPA2. Select **WPA2** to set the P-336M to use WPA2 first and then WPA if connection fails with WPA2. Select **WPA2 Only** to set the P-336M to use WPA2 only.
Cipher Type	Specify the encryption mechanism. Select **TKIP**, **AES** or **TKIP and AES**.
Group Key Update Interval	This is the rate at which an AP or RADIUS server sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Enter an update time in seconds.
PRE SHARED KEY	
Pre-Shared Key	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).

CHAPTER 4 Advanced

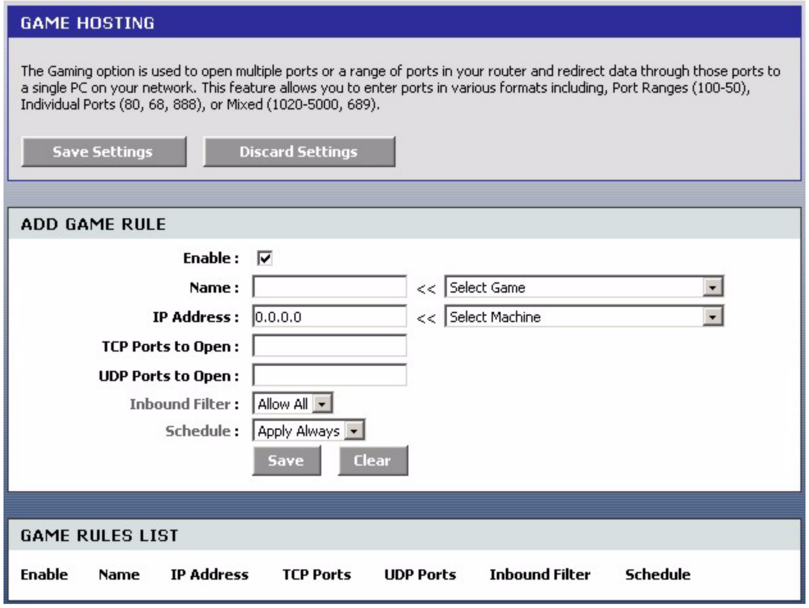
This chapter describes the Advanced screens you use to configure routing and security features.

4.1 Game Hosting

Some Internet applications (such as video conferencing and Internet games) require multiple connections between the clients and the server. These applications do not work through NAT-enabled networks. Your P-336M is a NAT-enabled device. In order to allow these applications to work in your network, you have to configure the P-336M to forward these applications to ports on a computer hosting that service.

To set the P-336M to forward applications to allowed ports, click **Advanced** > **Game Hosting**. A configuration screen displays.

Figure 16 Advanced: Game Hosting



GAME HOSTING

The Gaming option is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. This feature allows you to enter ports in various formats including, Port Ranges (100-50), Individual Ports (80, 68, 888), or Mixed (1020-5000, 689).

ADD GAME RULE

Enable :	☑		
Name :		<<	Select Game
IP Address :	0.0.0.0	<<	Select Machine
TCP Ports to Open :			
UDP Ports to Open :			
Inbound Filter :	Allow All		
Schedule :	Apply Always		

GAME RULES LIST

Enable	Name	IP Address	TCP Ports	UDP Ports	Inbound Filter	Schedule

The following table describes the fields in this screen.

Table 15 Advanced: Game Hosting

LABEL	DESCRIPTION
Enable	Click **Enable** to activate this feature. Clear this check box to deactivate this feature. Note that some Internet applications may not work in your network behind the P-336M.
Name	Enter a descriptive name for this setting. Alternatively, select a pre-defined application name from the drop-down list box. The pre-configured port number ranges for the selected application will be automatically displayed below.
IP Address	Enter the IP address (in dotted decimal notation) of a local computer hosting the selected service. Alternatively, select from the drop-down list box. The IP address of the selected computer will be displayed in this field.
TCP Ports to Open	Specify the TCP port(s) for the application. You can enter a port number and/or a range of ports. For example, 6159-6180, 99.
UDP Ports to Open	Specify the UDP port(s) for the application. You can enter a port number and/or a range of ports. For example, 6159-6180, 99.
Inbound Filter	Select a filter action on the traffic. Select You can configure filter actions in the **Inbound Filter** screen.
Schedule	Select the name of a time setting during which this setting is active. You can configure schedules in the **Schedules** screen.
Save	Click **Save** to save the changes of a configuration screen for the current session.
Clear	Click **Clear** to start configuring a screen again.
Game Rules List	
Enable	Select this option to activate this setting. Clear this checkbox to disable this setting.
Name	This field displays the descriptive name for this setting.
IP Address	This field displays the IP address of the local computer to which the specified traffic is forwarded.
TCP Ports	This field displays the TCP port(s) the specified traffic is forwarded.
UDP Ports	This field displays the UDP port(s) the specified traffic is forwarded.
Inbound Filter	This field displays the name of the filter on the incoming traffic.
Schedule	This field displays the name of the schedule to use.

4.2 Virtual Server

With the virtual server (also known as port forwarding) feature, you can make inside (behind NAT on the LAN) servers, for example, web or FTP, visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

4.2.1 Common Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers.

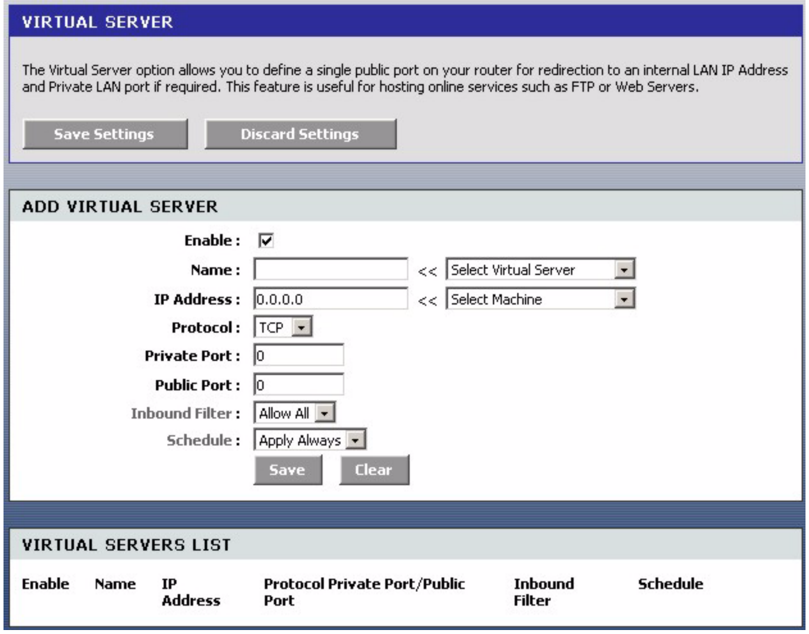
Table 16 Virtual Server: Common Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

4.2.2 Configuring Virtual Server

To set the virtual server settings, click **Advanced > Virtual Server** to display the configuration screen.

Figure 17 Advanced: Virtual Server



VIRTUAL SERVER

The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.

ADD VIRTUAL SERVER

Enable : ☑

Name : << Select Virtual Server

IP Address : 0.0.0.0 << Select Machine

Protocol : TCP

Private Port : 0

Public Port : 0

Inbound Filter : Allow All

Schedule : Apply Always

VIRTUAL SERVERS LIST

Enable	Name	IP Address	Protocol	Private Port/Public Port	Inbound Filter	Schedule

The following table describes the labels in this screen.

Table 17 Advanced: Virtual Server

LABEL	DESCRIPTION
Active	Select this check box to enable this virtual server setting. Clear this check box to disallow forwarding of these ports to an inside server without having to delete the entry.
Name	Enter a name to identify this port-forwarding rule. Alternatively, select a pre-defined name from the drop-down list box to have the P-336M fill in the default port numbers for the selected service.
IP Address	Enter the inside IP address of the inside server.
Protocol	Select the protocol type (**TCP**, **UDP** or **Both**).
Private Port	Enter the port number to which you want the P-336M to translate the public port.
Public Port	Enter the incoming port number for the selected service.
Inbound Filter	Select a filter action on the traffic. Select You can configure filter actions in the **Inbound Filter** screen.
Schedule	Select the name of a time setting during which this setting is active. You can configure schedules in the **Schedules** screen.
Save	Click this button to save the changes of a configuration screen for the current session.
Clear	Click this button to start configuring a screen again.
Virtual Server List	
Enable	Select this check box to enable this virtual server setting. Clear this check box to disallow forwarding of these ports to an inside server without having to delete the entry.
Name	This field displays the descriptive name for this setting.

Table 17 Advanced: Virtual Server (continued)

LABEL	DESCRIPTION
IP Address	This field displays the IP address of the inside server.
Protocol	This field displays the protocol type.
Private Port	This field displays the port number to which you want the P-336M to translate the public port.
Public Port	This field displays the incoming port number.
Inbound Filter	This field displays the name of the filter on the incoming traffic.
Schedule	This field displays the name of the schedule to use.

4.3 Applications

You can enable Application Layer Gateway (ALG) to allow certain NAT un-friendly applications (such as SIP) to operate properly through the P-336M. Alternatively, you can configure port triggering to allow computers on the LAN to dynamically take turns using the service

4.3.1 ALG

Some applications cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets’ data payload. The P-336M examines and uses IP address and port number information embedded in the data stream. When a device behind the P-336M uses an application for which the P-336M has ALG service enabled, the P-336M translates the device’s private IP address inside the data stream to a public IP address. It also records session port numbers and dynamically creates implicit NAT port forwarding and firewall rules for the application’s traffic to come in from the WAN to the LAN.

You may have to configure the server setting for an application in the Virtual Server screen (see Chapter 4 on page 43).

4.3.2 Port Triggering

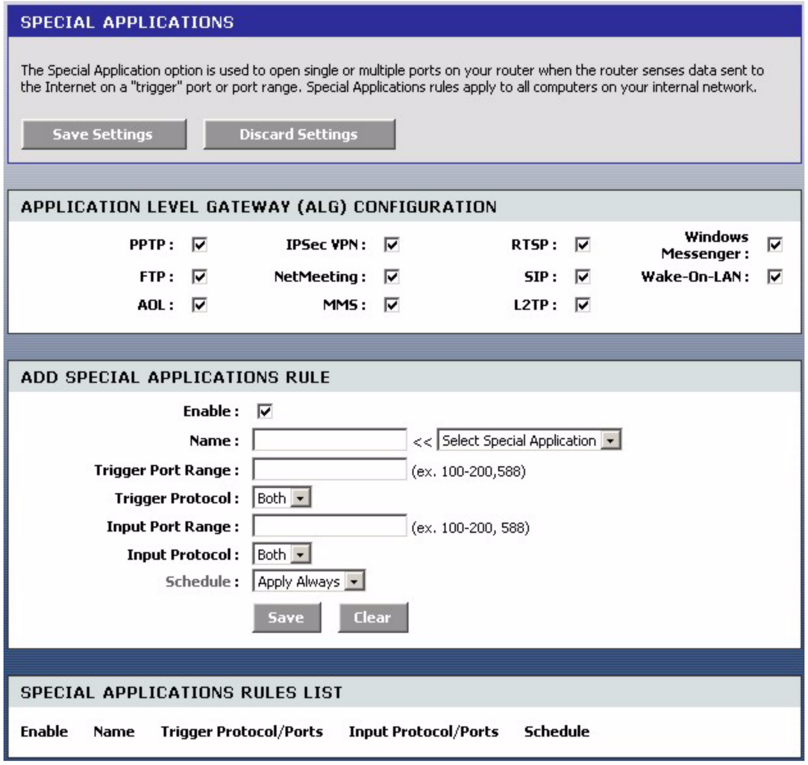
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding (or virtual server setup) you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The P-336M records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol ("trigger" port and protocol). When the P-336M's WAN port receives a response with a specific port number and protocol ("input" port and protocol), the P-336M forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

4.3.3 Configuring Special Applications

To allow ALG passthroughs and configure port triggering, click **Advanced** > **Applications** to display the configuration screen.

Figure 18 Advanced: Applications



SPECIAL APPLICATIONS

The Special Application option is used to open single or multiple ports on your router when the router senses data sent to the Internet on a "trigger" port or port range. Special Applications rules apply to all computers on your internal network.

APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION

PPTP : ☑ IPSec VPN : ☑ RTSP : ☑ Windows Messenger : ☑
FTP : ☑ NetMeeting : ☑ SIP : ☑ Wake-On-LAN : ☑
AOL : ☑ MMS : ☑ L2TP : ☑

ADD SPECIAL APPLICATIONS RULE

Enable : ☑
Name : << Select Special Application
Trigger Port Range : (ex. 100-200,588)
Trigger Protocol : Both
Input Port Range : (ex. 100-200, 588)
Input Protocol : Both
Schedule : Apply Always

SPECIAL APPLICATIONS RULES LIST

Enable	Name	Trigger Protocol/Ports	Input Protocol/Ports	Schedule

The following table describes the labels in this screen.

Table 18 Advanced: Applications

LABEL	DESCRIPTION
Application Level Gateway (ALG) Application	
PPTP	Select this option to allow multiple computers on the LAN to connect to a remote network using the PPTP protocol.
IPSec VPN	Select this option to allow multiple VPN clients to connect to a remote network using the IPSec protocol. This ALG may affect VPN connections for VPN clients using NAT traversal. In this case, clear this check box to disable this ALG.

Table 18 Advanced: Applications (continued)

LABEL	DESCRIPTION
RTSP	Select this option to allow applications (such as QuickTime and Real Player) that use Real Time Streaming Protocol (RTSP) to receive streaming media from the Internet.
Windows Messenger	Select this feature to allow the use of Microsoft Windows Messenger on computers in the LAN. **Note:** You must also enable the SIP ALG.
FTP	Select this option to allow FTP data transfer through a NAT-enabled network. You must also set up the FTP server settings in the **Virtual Server** screen.
NetMeeting	Select this option to allow Microsoft NetMeeting clients to communicate through a NAT-enabled network. You must also set up the NetMeeting server settings in the **Virtual Server** screen.
SIP	Select this option to allow devices and applications using VoIP (Voice over IP) to communicate over NAT. Clear this check box to disable this ALG if the devices/applications use NAT traversal.
Wake-On-LAN	Select this option to forward "magic packets" or wake-up packets from the WAN to a LAN computer or device with Wake-on-LAN (WOL) feature. You must also define the WOL server settings in the **Virtual Server** screen. The LAN IP address for the virtual server is typically set to the broadcast address of 192.168.0.255. The computer on the LAN whose MAC address is contained in the magic packet will be awakened.
AOL	Select this option if you are experiencing frequent line disconnections from the AOL server due to inactivity timeout.
MMS	Select this option to allow Windows Media Player, using MMS protocol, to receive streaming data from the Internet.
L2TP	Select this option to allow multiple computers on the LAN to connect to a remote network using the L2TP protocol.
Add Special Applications Rule	
Enable	Select this option to activate this rule.
Name	Enter a descriptive name for identification purposes. Alternatively, select a pre-defined application name from the drop-down list box to have the P-336M fill in the default port numbers and protocol type for the selected application.
Trigger Port Range	The trigger port is a port (or a range of ports) that causes (or triggers) the P-336M to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Specify a port or a range of ports.
Trigger Protocol	Select a protocol type for the application.
Input Port Range	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The P-336M forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Specify a port or a range of ports.
Input Protocol	Select the protocol used by the traffic coming to the router through the opened port range.
Schedule	Select the name of a time setting during which this setting is active. You can configure schedules in the **Schedules** screen.

Table 18 Advanced: Applications (continued)

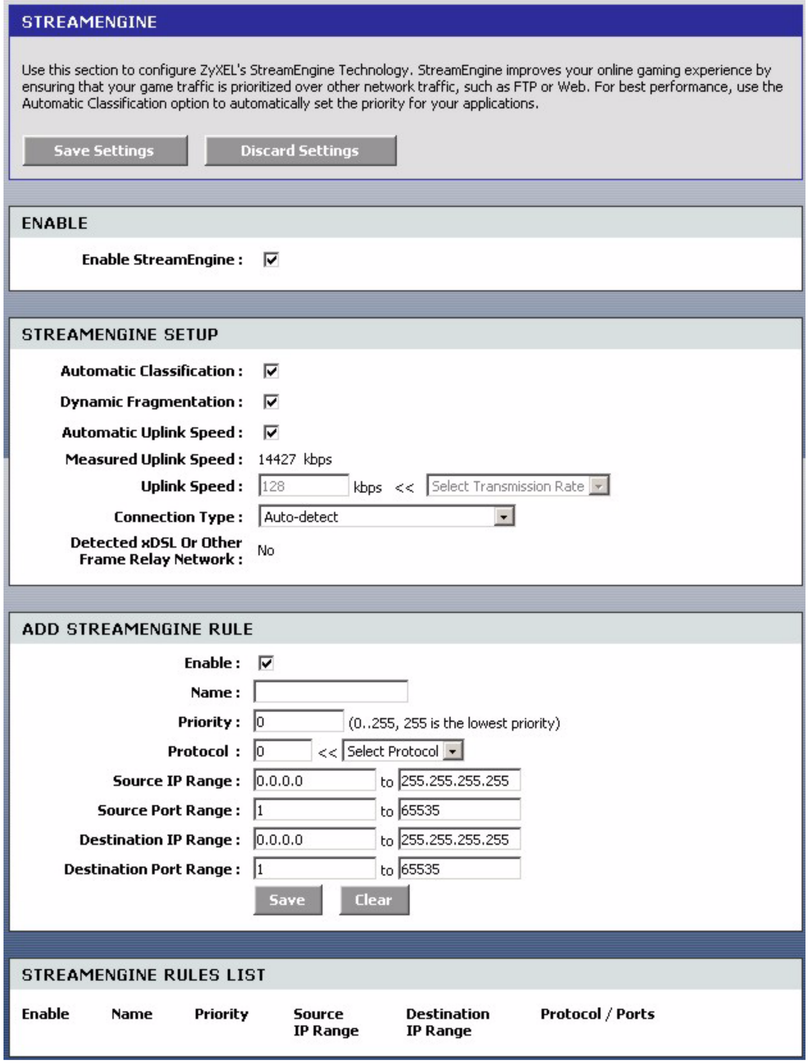
LABEL	DESCRIPTION
Save	Click **Save** to save the changes of a configuration screen for the current session.
Clear	Click **Clear** to start configuring a screen again.
Special Applications Rule List	
Enable	Select this check box to enable this trigger port setting. Clear this setting to deactivate it.
Name	This field displays the descriptive name of this trigger port setting.
Trigger Protocol/ Ports	This field displays the trigger port (or port range) and the trigger protocol type.
Input Protocol/Ports	This field displays the input port (or port range) and the input protocol type.
Schedule	This field displays the name of the schedule to use.

4.4 StreamEngine

Use the **StreamEngine** screen to configure traffic priorities. This improves network quality for your applications (such as online gaming). StreamEngine improves your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web. For better performance, use the **Automatic Classificatio**n option to automatically set the priority for your applications.

Click **Advanced** > **StreamEngine** to display the configuration screen.

Figure 19 Advanced: StreamEgine



STREAMENGINE

Use this section to configure ZyXEL's StreamEngine Technology. StreamEngine improves your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web. For best performance, use the Automatic Classification option to automatically set the priority for your applications.

ENABLE

Enable StreamEngine : ☑

STREAMENGINE SETUP

Automatic Classification : ☑

Dynamic Fragmentation : ☑

Automatic Uplink Speed : ☑

Measured Uplink Speed : 14427 kbps

Uplink Speed : 128 kbps << Select Transmission Rate

Connection Type : Auto-detect

Detected xDSL Or Other Frame Relay Network : No

ADD STREAMENGINE RULE

Enable : ☑

Name :

Priority : 0 (0..255, 255 is the lowest priority)

Protocol : 0 << Select Protocol

Source IP Range : 0.0.0.0 to 255.255.255.255

Source Port Range : 1 to 65535

Destination IP Range : 0.0.0.0 to 255.255.255.255

Destination Port Range : 1 to 65535

STREAMENGINE RULES LIST

Enable	Name	Priority	Source IP Range	Destination IP Range	Protocol / Ports

The following table describes the labels in this screen.

Table 19 Advanced: StreamEngine

LABEL	DESCRIPTION
Enable StreamEngine	Select this option to enable this feature.
StreamEngine	
Automatic Classification	Select this option to set the P-336M to automatically classify the traffic based on the default
Dynamic Fragmentation	Select this option to set the P-336M to break up large packets with high priority. This improves transmission quality.
Automatic Uplink Speed	Select this option to set the P-336M to automatically detect and set the optimum WAN connection speed.
Measured Uplink Speed	This field displays the detected transmission speed of the WAN connection that was last established. This uplink speed may be different from the actual transmission speed depending on your network environment and line condition.

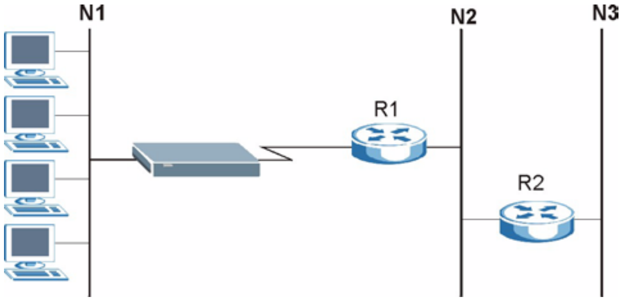
Table 19 Advanced: StreamEngine (continued)

LABEL	DESCRIPTION
Uplink Speed	This field is not applicable when you select the **Automatic Uplink Speed** option above. Enter a number to manually set the uplink speed for the WAN connection. Alternatively, select a pre-defined choice from the drop-down list box.
Connection Type	Select **Auto-detect** to set the P-336M to automatically detect the Internet connection type. Select **xDSL or Other Frame Relay Network** if the P-336M connects to the Internet via a DSL modem. Select **Cable or Other Broadband Network** if the P-336M connects to the Internet via a cable modem.
Detected xDSL or Framerelay Network	This field is applicable when you select **Auto-detect** in the **Connection Type** field. This field displays the name of the detected line connection type.
Add StremEngine Rule	
Enable	Select this option to enable this rule.
Name	Enter a descriptive name for identification purposes.
Priority	Specify a priority for the traffic type specified below. Enter a number between 1 (highest) and 255 (lowest).
Protocol	Enter the protocol number or select a pre-defined protocol type from the drop-down list box.
Source IP Range	Specify one or a range of source IP addresses in the fields provided. Enter the same IP address in the **to** field if you want to specify one IP address.
Source Port Range	Specify one or a range of source port numbers. Enter the same number in the **to** field if you want to specify one source port.
Destination IP Range	Specify one or a range of destination IP addresses in the fields provided. Enter the same IP address in the **to** field if you want to specify one IP address.
Destination Port Range	Specify one or a range of destination port numbers. Enter the same number in the **to** field if you want to specify one destination port.
Save	Click **Save** to save the settings.
Clear	Click **Clear** to start configuring this part of the screen again.
StreamEngine Rule List	
Enable	Select this option to activate this rule. Clear this check box to disable this rule without deleting it.
Name	THis field displays the descriptive name for the rule.
Priority	This field displays the priority level (1 to 255) of this rule.
Source IP Range	This field displays one or a range of source IP addresses.
Destination IP Range	This field displays one or a range of destination IP addresses.
Protocol/Ports	This field displays the protocol and port numbers.

4.5 Routing

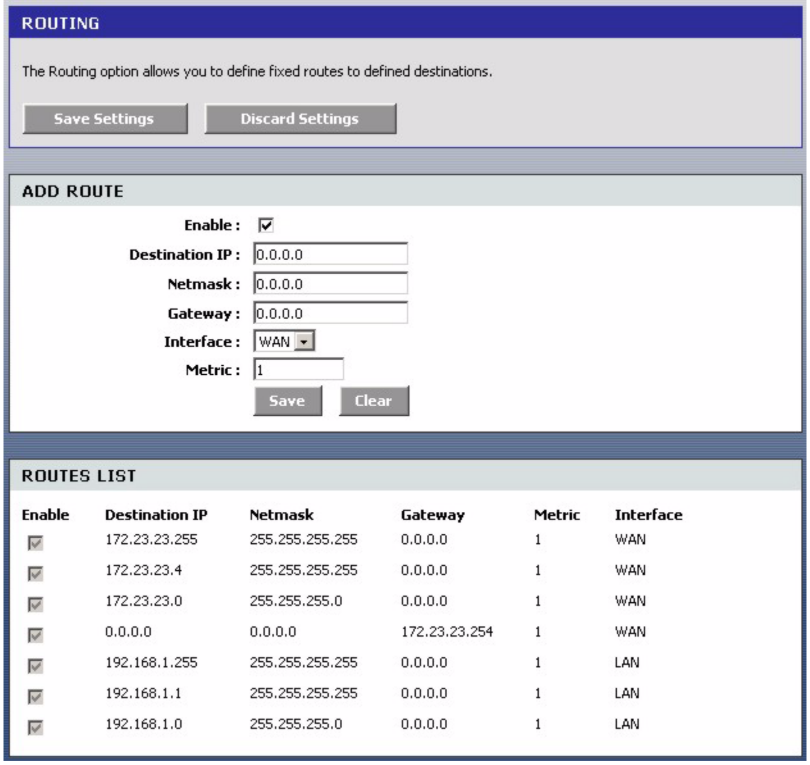
Each remote node specifies only the network to which the gateway is directly connected, and the P-336M has no knowledge of the networks beyond. For instance, the P-336M knows about network N2 in the following figure through remote node Router 1. However, the P-336M is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the P-336M about the networks beyond the remote nodes.

Figure 20 Example of Static Routing Topology



To view the routing table configure static routes, click **Advanced** > **Routing** to display the configuration screen.

Figure 21 Advanced: Routing


ROUTING

The Routing option allows you to define fixed routes to defined destinations.

ADD ROUTE

Enable :	☑
Destination IP :	0.0.0.0
Netmask :	0.0.0.0
Gateway :	0.0.0.0
Interface :	WAN
Metric :	1

ROUTES LIST

Enable	Destination IP	Netmask	Gateway	Metric	Interface
☑	172.23.23.255	255.255.255.255	0.0.0.0	1	WAN
☑	172.23.23.4	255.255.255.255	0.0.0.0	1	WAN
☑	172.23.23.0	255.255.255.0	0.0.0.0	1	WAN
☑	0.0.0.0	0.0.0.0	172.23.23.254	1	WAN
☑	192.168.1.255	255.255.255.255	0.0.0.0	1	LAN
☑	192.168.1.1	255.255.255.255	0.0.0.0	1	LAN
☑	192.168.1.0	255.255.255.0	0.0.0.0	1	LAN

The following table describes the labels in this screen.

Table 20 Advanced: Routing

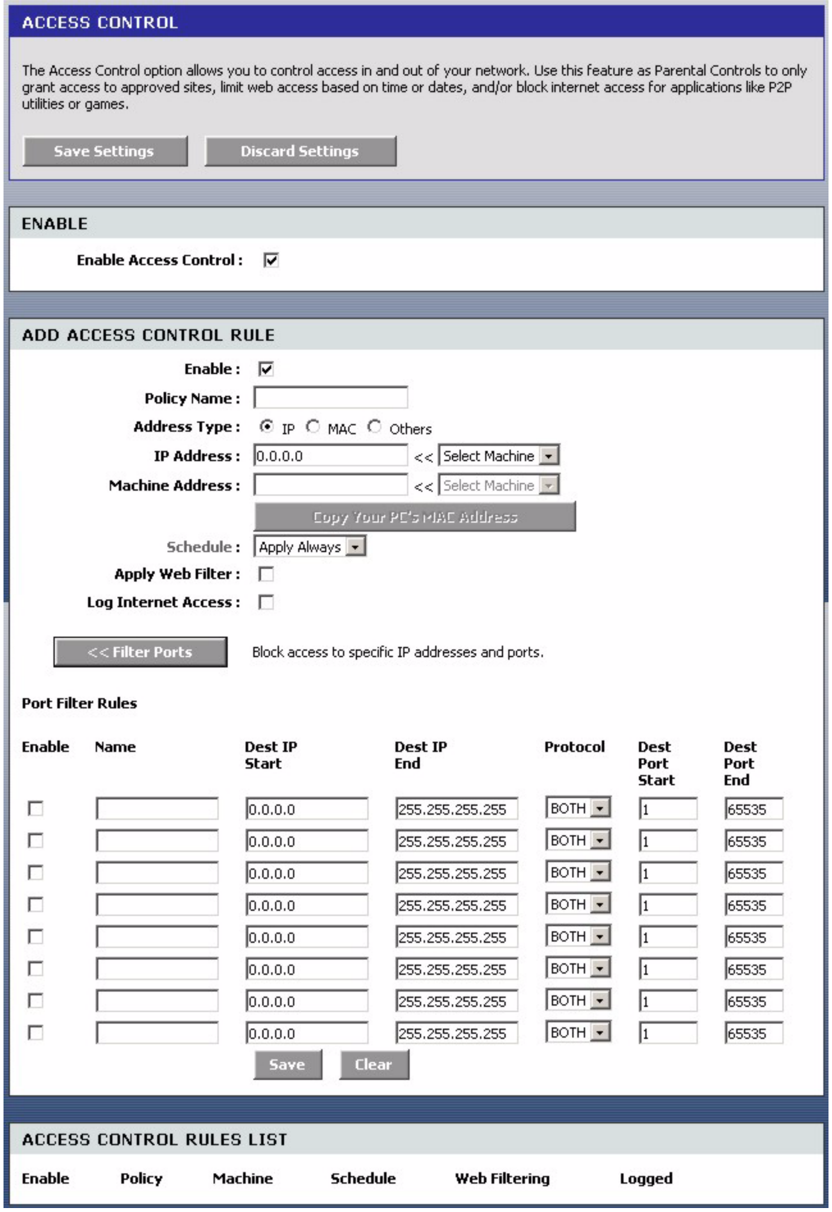
LABEL	DESCRIPTION
Add Route	
Enable	Select this option to activate this setting. This field is not applicable for pre-defined routes.
Destination IP	Enter the destination IP address in dotted decimal notation.
Netmask	Enter the subnet mask.
Gateway	Enter the IP address of the gateway device for the selected interface below.
Interface	Select an interface to which you want to apply the setting.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Save	Click **Save** to save the settings.
Clear	Click **Clear** to start configuring this part of the screen again.
Routes List	
Enable	Select this option to activate this rule. Clear this check box to disable this rule without deleting it.
Destination IP	This field displays the destination IP address.
Netmask	This field displays the subnet mask for the destination IP address above.
Gateway	This field displays the IP address of the gateway device.
Metric	This field displays the “cost” of this route.
Interface	This field displays the interface to which this routing setting is applied.

4.6 Access Control

Internet access control allows you to create and enforce Internet access policies tailored to your needs. Access control gives you the ability to block specified computers and/or applications from accessing the Internet. You can also set a schedule for when the P-336M performs content filtering.

Click **Advanced > Access Control** to display the configuration screen as shown.

Figure 22 Advanced: Access Control



ACCESS CONTROL

The Access Control option allows you to control access in and out of your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block internet access for applications like P2P utilities or games.

ENABLE

Enable Access Control : ☑

ADD ACCESS CONTROL RULE

Enable : ☑

Policy Name :

Address Type : ● IP ○ MAC ○ Others

IP Address : 0.0.0.0 << Select Machine

Machine Address : << Select Machine

Schedule : Apply Always

Apply Web Filter : □

Log Internet Access : □

Block access to specific IP addresses and ports.

Port Filter Rules

Enable	Name	Dest IP Start	Dest IP End	Protocol	Dest Port Start	Dest Port End
□		0.0.0.0	255.255.255.255	BOTH	1	65535
□		0.0.0.0	255.255.255.255	BOTH	1	65535
□		0.0.0.0	255.255.255.255	BOTH	1	65535
□		0.0.0.0	255.255.255.255	BOTH	1	65535
□		0.0.0.0	255.255.255.255	BOTH	1	65535
□		0.0.0.0	255.255.255.255	BOTH	1	65535
□		0.0.0.0	255.255.255.255	BOTH	1	65535
□		0.0.0.0	255.255.255.255	BOTH	1	65535

ACCESS CONTROL RULES LIST

Enable	Policy	Machine	Schedule	Web Filtering	Logged

The following table describes the labels in this screen.

Table 21 Advanced: Access Control

LABEL	DESCRIPTION
Enable	Select **Enable Access Control** to activate this feature.
Add Access Control Rule	Set the following fields to configure an access control rule.
Enable	Select this option to enable this rule. Clear this check box to disable this rule.
Policy Name	Enter a descriptive name for identification purposes.
Address Type	Select the address type this rule checks.

Table 21 Advanced: Access Control (continued)

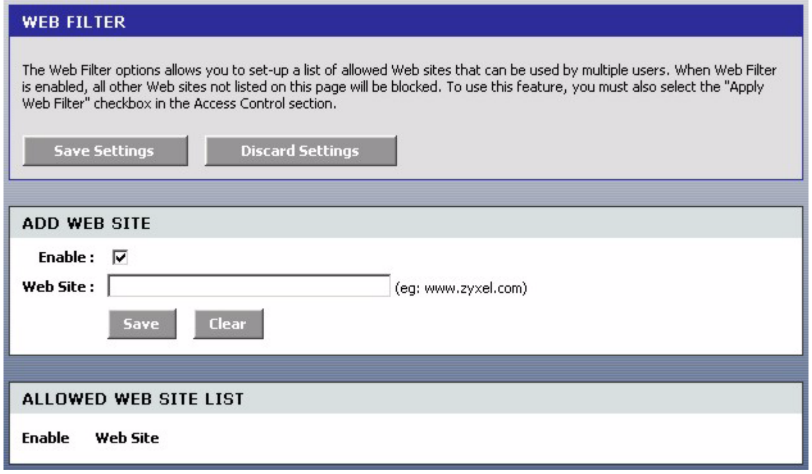
LABEL	DESCRIPTION
IP Address	This field is applicable when you select **IP** in the **Address Type** field above. Enter the IP address of a device to which you want to apply this rule. Alternatively, select a device name from the drop-down list box.
MAC Address	This field is applicable when you select **MAC** in the **Address Type** field. Enter the MAc address of the device to which you want to apply this rule. Alternatively, select a device name from the drop-down list box.
Copy Your PC's MAC Address	This button is applicable when you select **MAC** in the **Address Type** field. Click this button to copy the MAC address of your computer.
Schedule	Specify the time this rule is active. Select the name of a schedule from the drop-down list box. You can configure a schedule in the **Schedule** screen.
Apply Web Filter	Select this option to apply the web filters you configure in the Web Filter screen.
Log Internet Access	Select this option to set the P-336M to create logs for Internet access activity.
Filter Ports	Click this button to display the fields you use to configure port filters.
Port Filter Rules	
Enable	Select this option to activate this rule. Clear this check box to deactivate this rule.
Name	Enter a descriptive name for identification purposes.
Dest IP Start	Enter the start of the destination IP address range.
Dest IP End	Enter the end of the destination IP address range.
Protocol	Select a protocol type from the drop-down list box.
Dest Port Start	Enter the start of the destination port range.
Dest Port End	Enter the end of the destination port range.
Save	Click **Save** to save the settings in this part of the screen.
Clear	Click **Clear** to start configuring this part of the screen again.
Access Control Rules List	
Enable	Select this option to activate the rule. Clear this check box to disable the rule without deleting it.
Policy	This field displays the name of the port filter policy you configured for this access control rule.
Machine	This field displays the IP or MAC address of the device to which this access control rule is applied.
Schedule	This field displays the name of the schedule to use.
Web Filter	This field indicates whether web filters apply to this access control rule.
Logged	This field indicates whether Internet access activities are logged.

4.7 Web Filter

The **Web Filter** screen gives you the ability to allow access only to web sites that you specify.

Click **Advanced** > **Web Filter** to display the configuration screen.

Figure 23 Advanced: Web Filter



WEB FILTER

The Web Filter options allows you to set-up a list of allowed Web sites that can be used by multiple users. When Web Filter is enabled, all other Web sites not listed on this page will be blocked. To use this feature, you must also select the "Apply Web Filter" checkbox in the Access Control section.

Enable : ☑

Web Site : (eg: www.zyxel.com)

The following table describes the labels in this screen.

Table 22 Advanced: Web Filter

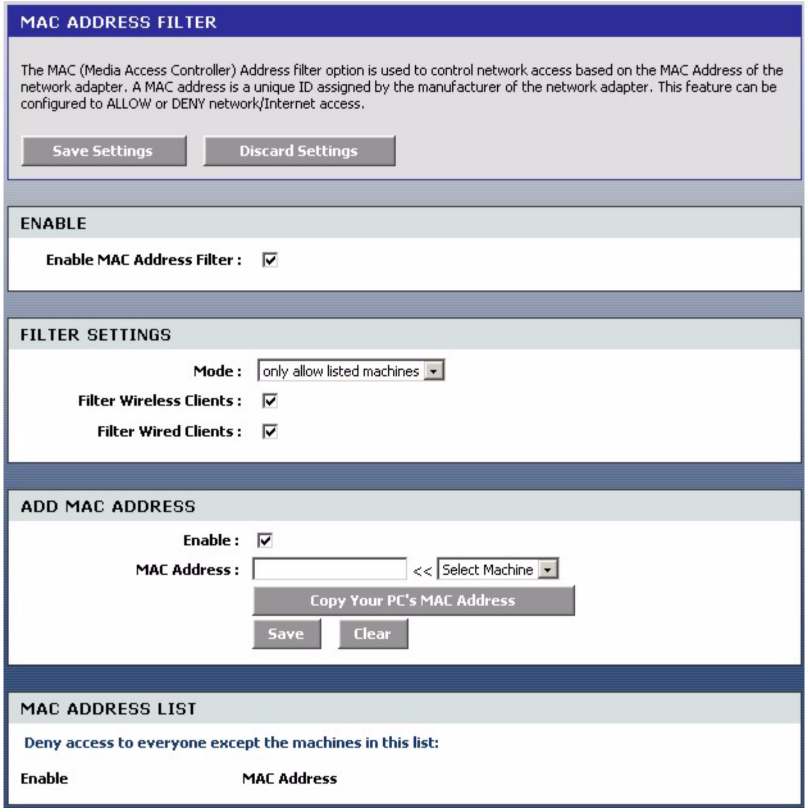
LABEL	DESCRIPTION
Add Web Site	
Enable	Select this option to activate this setting. Clear this check box to disable it.
Web Site	Enter the web site address to which you want to restrict access. For example, www.zyxel.com. For web sites that obtain data from another web site, you need to allow access to those web sites too. For example, if www.zyxel.com gets a graphic file from mysite.zyxel.com, then you must also enter mysite.zyxel.com in this screen. **Note:** Do NOT enter http://.
Save	Click **Save** to save the settings in this part of the screen.
Clear	Click **Clear** to start configuring this part of the screen again.
Allowed Web Site List	This table lists the addresses of the web sites that you want to allow access.
Enable	Select this option to allow access to this web site. Clear this check box to block access.
Web Site	This field displays the web site address.

4.8 MAC Filter

MAC address filtering means sifting traffic going through the P-336M based on the source and/or destination MAC addresses. You can set the P-336M to filter packets from connected wireless clients or computers on the wired LAN.

Click **Advanced** > **MAC Filter** to display the configuration screen.

Figure 24 Advanced: MAC Filter



MAC ADDRESS FILTER

The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/Internet access.

ENABLE

Enable MAC Address Filter : ☑

FILTER SETTINGS

Mode : only allow listed machines

Filter Wireless Clients : ☑

Filter Wired Clients : ☑

ADD MAC ADDRESS

Enable : ☑

MAC Address : << Select Machine

MAC ADDRESS LIST

Deny access to everyone except the machines in this list:

Enable	MAC Address

The following table describes the labels in this screen.

Table 23 Advanced: MAC Filter

LABEL	DESCRIPTION
Enable	Select **Enable MAC Address Filter** to activate this setting. Clear this check box to disable it.
Filter Settings	
Mode	Select **only deny listed machines** to block frames to/from the specified MAC address(es). Select **only allow listed machines** to forward frames to/from the specified MAC address(es).
Filter Wireless Clients	Select this option to apply the filter settings to the wireless clients.
Filter Wired Clients	Select this option to apply the filter settings to the wired computers on the LAN.
Add MAC Address	
Enable	Select **Enable** to activate this filter setting. Clear this check box to disable it.
MAC Address	Enter the MAC address (in six pairs of dotted haxidecimal notation) of a computer whose traffic you want to filter. Or select a computer from the drop-down list box.

Table 23 Advanced: MAC Filter (continued)

LABEL	DESCRIPTION
Copy Your PC's MAC Address	Click this button to copy the MAC address of your computer. **Note:** In order for the P-336M to copy your computer's MAC address, your computer must be connected directly to the P-336M.
Save	Click **Save** to save the settings in this part of the screen.
Clear	Click **Clear** to start configuring this part of the screen again.
MAC Address List	
Enable	Select this option to activate this filter setting. Clear this check box to disable it without deleting it.
MAC Address	This field displays the MAC address of a computer whose traffic you want to filter.

4.9 Firewall

Stateful packet inspection (SPI) firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support.

The P-336M firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated. The P-336M's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The P-336M can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network. The P-336M also has packet-filtering capabilities.

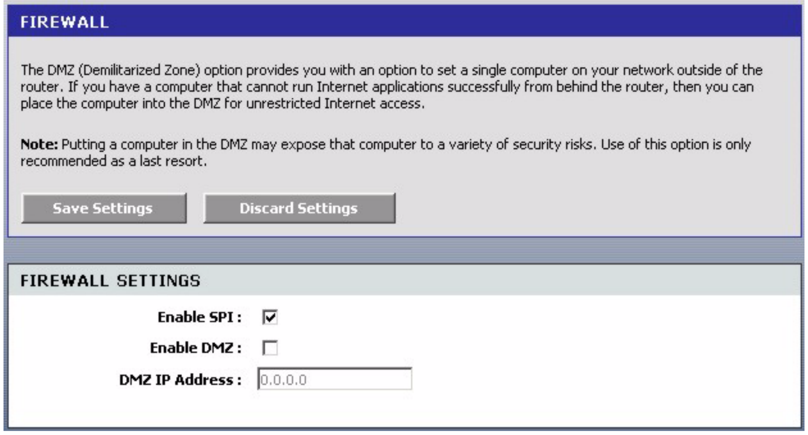
4.9.1 DMZ

The DeMilitarized Zone (DMZ) provides a way for public servers (Web, e-mail, FTP, etc.) to be visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death). These public servers can also still be accessed from the secure LAN.

4.9.2 Configuring Firewall

To configure the firewall and DMZ settings, click **Advanced > Firewall** to display the configuration screen.

Figure 25 Advanced: Firewall



FIREWALL

The DMZ (Demilitarized Zone) option provides you with an option to set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.

Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

FIREWALL SETTINGS

Enable SPI : ☑

Enable DMZ : □

DMZ IP Address : 0.0.0.0

The following table describes the labels in this screen.

Table 24 Advanced: Firewall

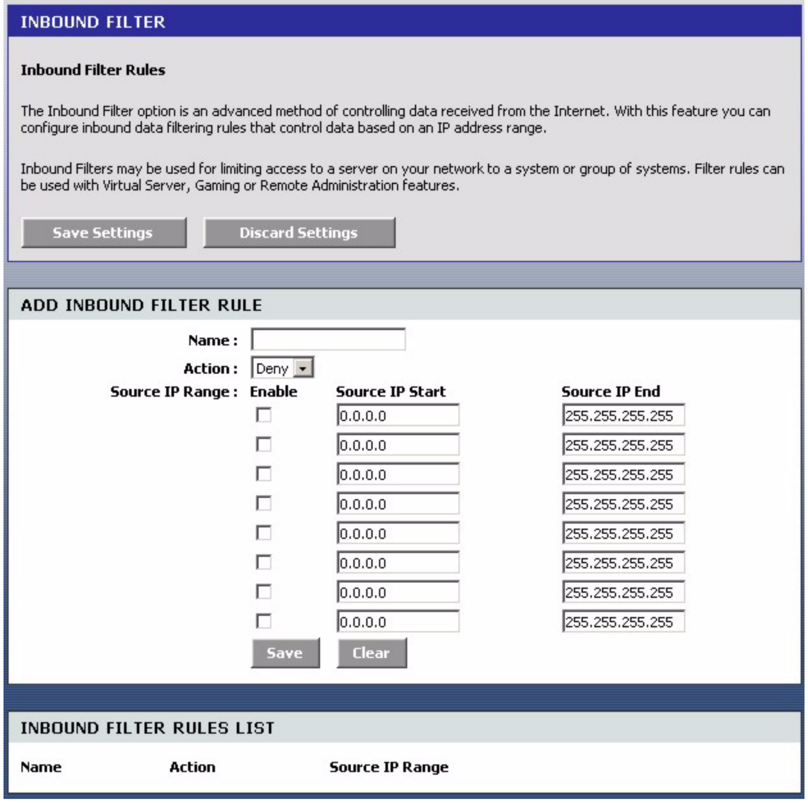
LABEL	DESCRIPTION
Enable SPI	Select this option to activate Stateful packet inspection. Clear this check box to disable this feature.
Enable DMZ	Select this option to activate the DMZ feature to protect the specified device on the LAN.
DMZ IP Address	Enter the IP address (in dotted decimal notation) of a computer which you want to protect on the LAN.

4.10 Inbound Filter

An inbound filter allows you to filter packets based on IP addresses. You can use inbound filters to control access to network resources (such as a web server) or for remote management of the device.

Click **Advanced** > **Inbound Filter** to display the configuration screen.

Figure 26 Advanced: Inbound Filter



INBOUND FILTER

Inbound Filter Rules

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range.

Inbound Filters may be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Gaming or Remote Administration features.

ADD INBOUND FILTER RULE

Name :

Action : Deny

Source IP Range : Enable	Source IP Start	Source IP End
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255

INBOUND FILTER RULES LIST

Name	Action	Source IP Range

The following table describes the labels in this screen.

Table 25 Advanced: Inbound Filter

LABEL	DESCRIPTION
Add Inbound Filter Rule	
Name	Enter a descriptive name (up to 16 characters) for this filter setting. This is for identification purposes only.
Action	Select **Deny** to block packets from the specified IP address(es). Select **Allow** to forward packets from the specified IP address(es).
Source IP Range	
Enable	Select this option to activate the filter action on the specified IP address range. Clear this check box to disable the filter action on the IP address range.
Source IP Start	Enter the start of the source IP address range.
Source IP End	Enter the end of the source IP address range.
Save	Click **Save** to save the settings in this part of the screen.
Clear	Click **Clear** to start configuring this part of the screen again.
Inbound Filter Rules List	
Name	This field displays the name of the inbound filter.

Table 25 Advanced: Inbound Filter (continued)

LABEL	DESCRIPTION
Action	This field displays the action on the packets from the specified IP address range.
Source IP Range	This field displays the source IP address range(s).

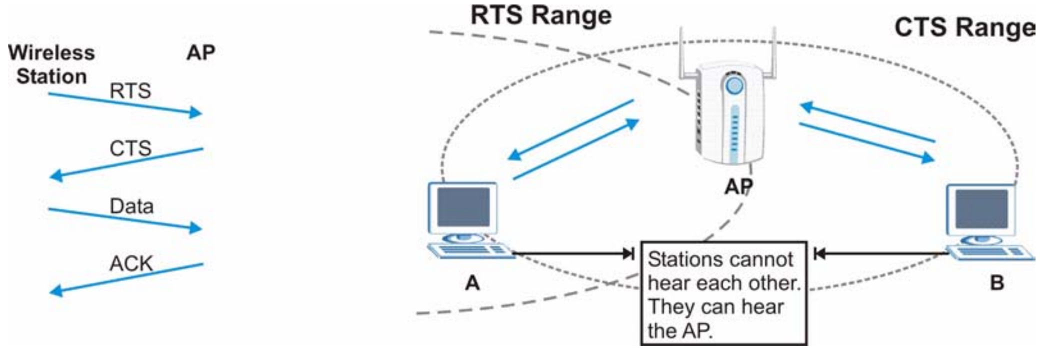
4.11 Wireless

This section describes advanced wireless LAN features. For more information, refer to Section 3.5 on page 33.

4.11.1 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 27 RTS/CTS



When station A sends data to the Prestige, 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.

4.11.2 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 Prestige will fragment the packet into smaller data frames.

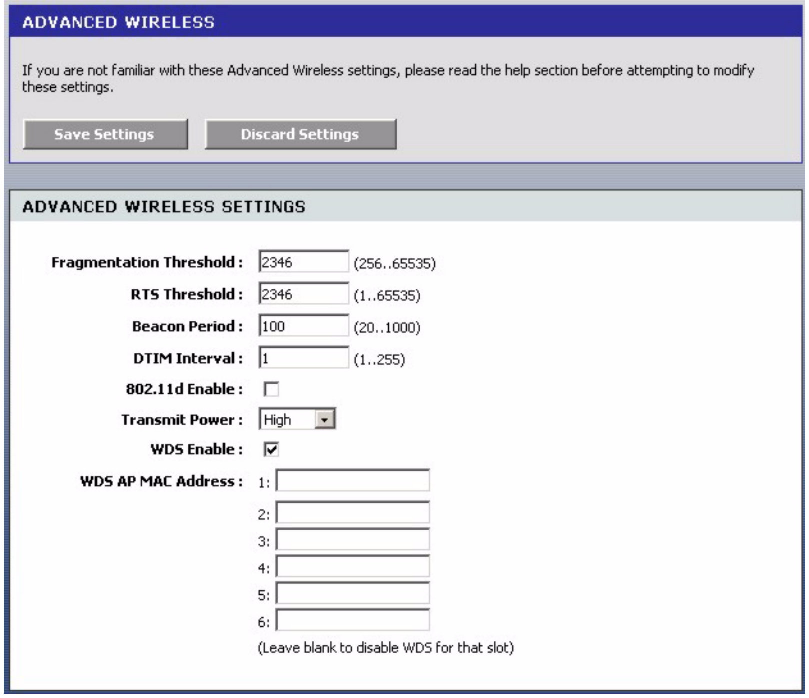
A large Fragmentation Threshold is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

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.

4.11.3 Configuring Advanced Wireless Settings

To configure advanced wireless settings, click **Advanced** > **Wireless** to display the screen.

Figure 28 Advanced: Wireless '



ADVANCED WIRELESS

If you are not familiar with these Advanced Wireless settings, please read the help section before attempting to modify these settings.

ADVANCED WIRELESS SETTINGS

Fragmentation Threshold :	2346	(256..65535)
RTS Threshold :	2346	(1..65535)
Beacon Period :	100	(20..1000)
DTIM Interval :	1	(1..255)
802.11d Enable :	□	
Transmit Power :	High	
WDS Enable :	☑	
WDS AP MAC Address :	1: 2: 3: 4: 5: 6:	

(Leave blank to disable WDS for that slot)

The following table describes the labels in this screen.

Table 26 Advanced: Wireless

LABEL	DESCRIPTION
Advanced Wireless Settings	
Fragmentation Threshold	This is the threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
RTS Threshold	The RTS (Request To Send) threshold (number of bytes) is for enabling RTS/CTS. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this value to be larger than the maximum MSDU (MAC service data unit) size turns off RTS/CTS. Setting this value to zero turns on RTS/CTS. Enter a new value between 0 and 2432.
Beacon Period	A wireless AP sets out a beacon to announce its presence and maintain an orderly communication between other wireless devices. Enter the time (between 20 and 1000 ms) the P-336M waits before sending a beacon to the wireless clients.
DTIM Interval	A DTIM (Delivery Traffic Indication Message) is included in a beacon to synchronize wireless transmission. DTIM is a countdown information for wireless clients to listen to the next broadcast or multicast messages. Enter the time (between 1 and 255 ms) the P-336M waits between sending a beacon with DTIM.
802.11d Enable	802.11d is a wireless communication specification for countries where other IEEE802.11 devices are not allowed. 802.11d is suitable if you want global roaming (that is using your wireless devices worldwide). Select this option to enable this feature.

Table 26 Advanced: Wireless (continued)

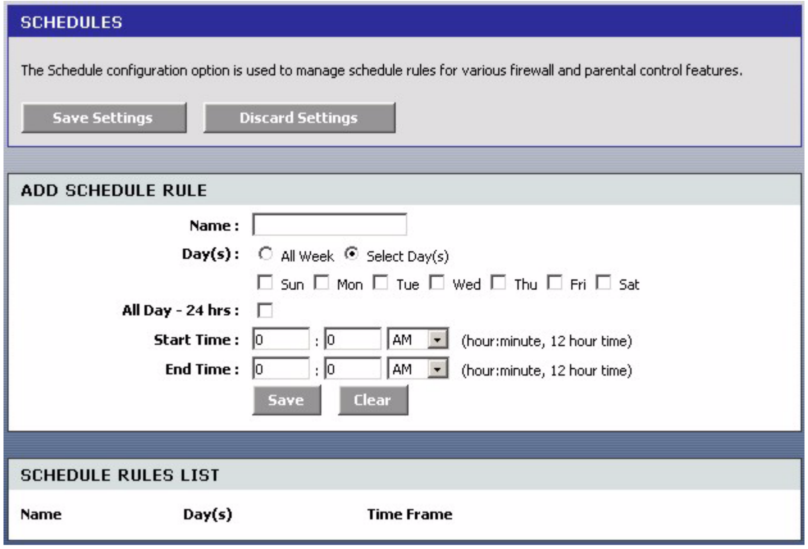
LABEL	DESCRIPTION
Transmission Power	Select an option in this field to set the transmission power of the antennas to reduce your wireless coverage area.
WDS Enable	Select this option to activate the WDS (Wireless Distribution System) feature. A Distribution System (DS) is a wired connection between two or more APs, while a WDS is a wireless connection. An AP using WDS can function as a wireless network bridge allowing you to wirelessly connect two wired network segments. **Note:** You cannot enable WPA and WDS at the same time.
WDS AP MAC Address	Enter the MAC address (in six paris of dotted haxidecimal notation) of the neighboring AP(s) that participates in the WDS.

4.12 Schedule

You can define schedule settings on the P-336M and apply these schedule settings in other configuration screens (such as Game Hosting and Virtual Server).

Click **Advanced** > **Schedule** to display the configuration screen.

Figure 29 Advanced: Schedule



SCHEDULES

The Schedule configuration option is used to manage schedule rules for various firewall and parental control features.

ADD SCHEDULE RULE

Name :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

All Day - 24 hrs : □

Start Time : 0 : 0 AM (hour:minute, 12 hour time)

End Time : 0 : 0 AM (hour:minute, 12 hour time)

SCHEDULE RULES LIST

Name	Day(s)	Time Frame

The following table describes the labels in this screen.

Table 27 Advanced: Schedule

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 16 characters) for this schedule setting. This is for identification purposes only.
Day(s)	Select **All Week** or **Select Day(s)** to specify the day(s) of the week.
All Day - 24 hrs	Select this option to enable the schedule for the entire day for the specified day(s).

Table 27 Advanced: Schedule (continued)

LABEL	DESCRIPTION
Start Time	Set the start of the schedule.
End Time	Set the end of the schedule.
Save	Click **Save** to save the settings in this part of the screen.
Clear	Click **Clear** to start configuring this part of the screen again.

CHAPTER 5 Tools

This chapter describes the Tools screens you use to configure login passwords, system time, logs, DDNS and firmware and configuration settings.

5.1 Administrator Settings

You can change the login account passwords, enable UPnP and configure remote access settings in the **Admin** screen.

5.1.1 Login Accounts

You can log into the web configurator using one of the following accounts.

- Administrator (admin)

  This is the system administrator’s account with full access rights. You can view system status and set the configuration screens using this account.

- Normal User (user)

  This account allows you to view device system status and configuration settings in the web configurator. configuration is allowed.

5.1.2 UPnP

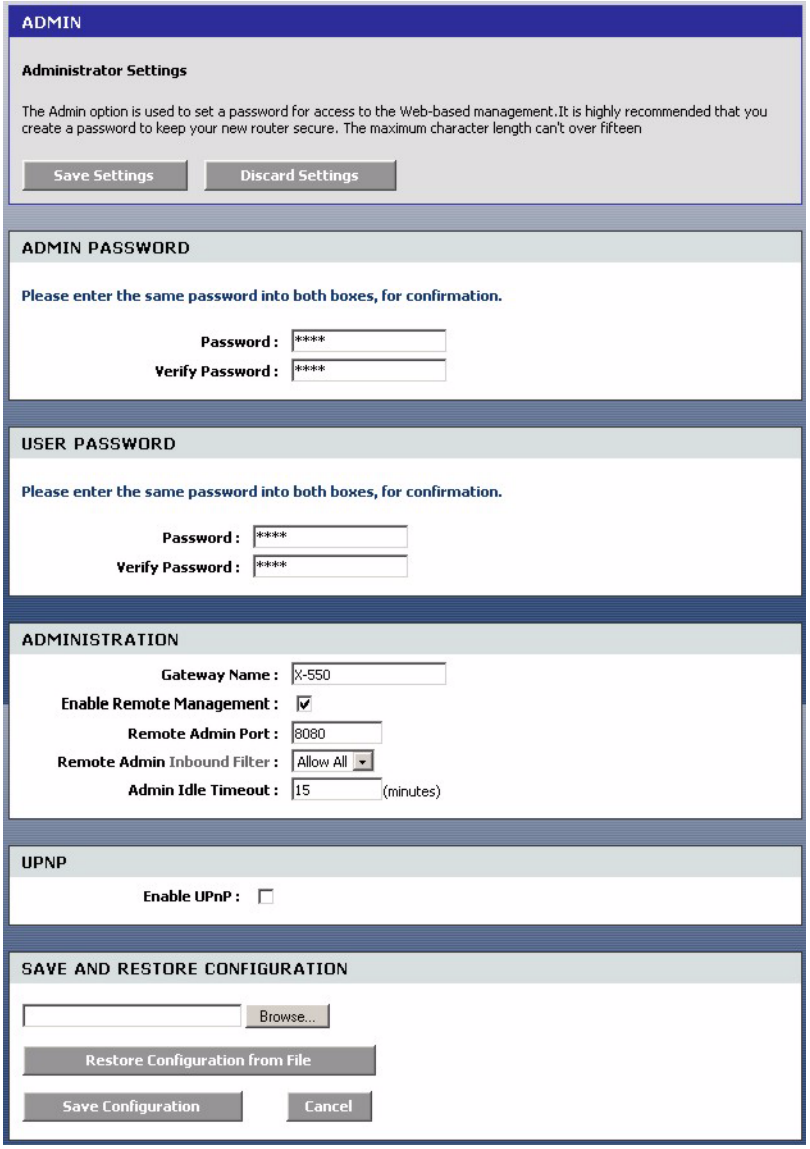
Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

5.1.3 The Admin Screen

Use the **Admin** screen to configure login passwords, remote management and UPnP. You can also restore and backup the device configuration in this screen.

Click **Tools** > **Admin** to display the configuration screen.

Figure 30 Tools: Admin



ADMIN

Administrator Settings

The Admin option is used to set a password for access to the Web-based management.It is highly recommended that you create a password to keep your new router secure. The maximum character length can't over fifteen

ADMIN PASSWORD

Please enter the same password into both boxes, for confirmation.

Password : ****
Verify Password : ****

USER PASSWORD

Please enter the same password into both boxes, for confirmation.

Password : ****
Verify Password : ****

ADMINISTRATION

Gateway Name : X-550
Enable Remote Management : ☑
Remote Admin Port : 8080
Remote Admin Inbound Filter : Allow All
Admin Idle Timeout : 15 (minutes)

UPNP

Enable UPnP : ☐

SAVE AND RESTORE CONFIGURATION

The following table describes the labels in this screen.

Table 28 Tools: Admin

LABEL	DESCRIPTION
Admin Password	
Password	Type the new password in this field.
Verify Password	Type the new password again in this field.
User Password	
Password	Type the new password in this field.
Verify Password	Type the new password again in this field.
Administration	

Table 28 Tools: Admin

LABEL	DESCRIPTION
Gateway Name	Enter a descriptive name (up to 32 characters) for your P-336M. This is for identification purposes only.
Enable Remote Management	Remote management allows you to allow access to the P-336M web configurator from the WAN. Select this option to activate this feature. Clear this check box to disable this feature.
Remote Admin Port	Specify the port number of the embedded web server on the P-336M for accessing the web configurator. Enter a port number to access the web configurator. If you enter a number other than 80, you need to append the port number to the **WAN** port IP address to access the web configurator. For example, if you enter "8080" as the web server port number, then you must enter "http://10.10.1.1:8080" where 10.10.1.1 is the WAN port IP address.
Remote Admin Inbound Filter	Select a filter action on the traffic. Select You can configure filter actions in the **Inbound Filter** screen.
Admin Idle Timeout	Specify how many minutes the web configuration can be left idle before the session times out. After it times out you have to log in with your username and password again. Very long idle timeouts may have security risks.
UPNP	
Enable UPNP	Select this option to activate this feature.
Save and Restore Configuration	
Restore Configuration From File	You can restore a previously save configuration file to the P-336M. Enter the name of the configuration file or click **Browse** to locate it and click **Restore Configuration From File** to start the file upload process.
Save Configuration	Click **Save Configuration** to save the current device configuration to your computer.
Cancel	Click **Cancel** to start configuring this screen again.

5.1.4 Configuration Backup

Note: Do not turn off the P-336M while the file transfer process is taking place.

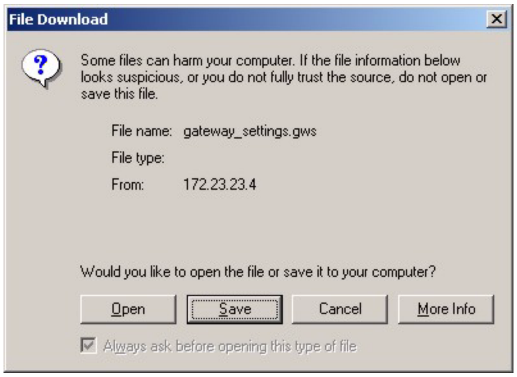
Follow the steps below to back up the current configuration of the P-336M.

1 In the web configurator, click **Tools** > **Admin** (see Figure 30 on page 67).

2 Scroll to the bottom of the **ADMIN** screen and click **Save Configuration**.

3 A **File Download** screen displays. Click **Save**.

Figure 31 Tools: Admin: File Download



File Download

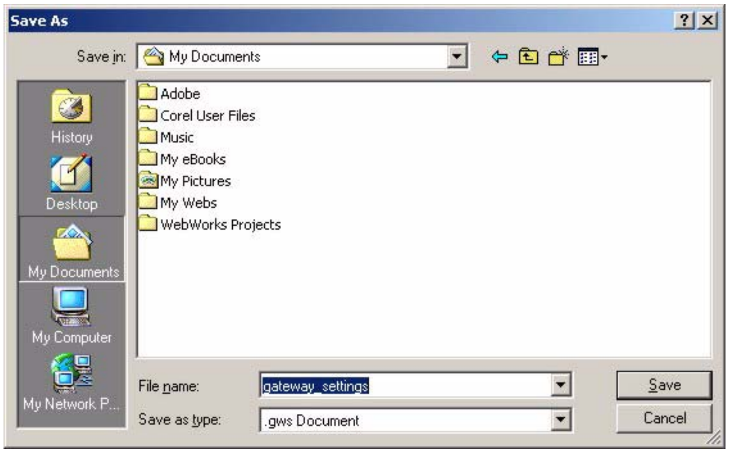
Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: gateway_settings.gws
File type:
From: 172.23.23.4

Would you like to open the file or save it to your computer?

4 A **Save As** screen displays. Accept the default file location and name or specify a location and name. Click **Save** to back up the configuration file.

Figure 32 Tools: Admin: Save As



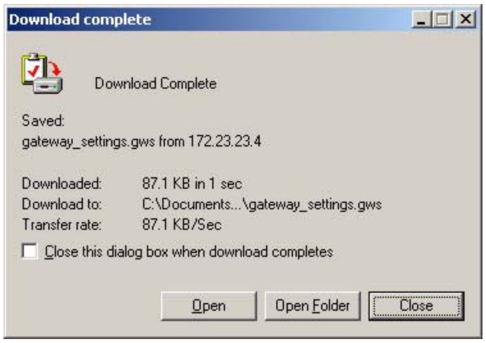
Save As

Save in: My Documents

File name: gateway_settings
Save as type: .gws Document

5 After the back up process is complete, a **Download complete** screen displays. Click **Close** to close the screen.

Figure 33 Tools: Admin:



Download complete

Download Complete

Saved:
gateway_settings.gws from 172.23.23.4

Downloaded: 87.1 KB in 1 sec
Download to: C:\Documents...\gateway_settings.gws
Transfer rate: 87.1 KB/Sec

□ Close this dialog box when download completes

5.1.5 Configuration Restore

Note: Do not turn off the P-336M while the file transfer process is taking place.

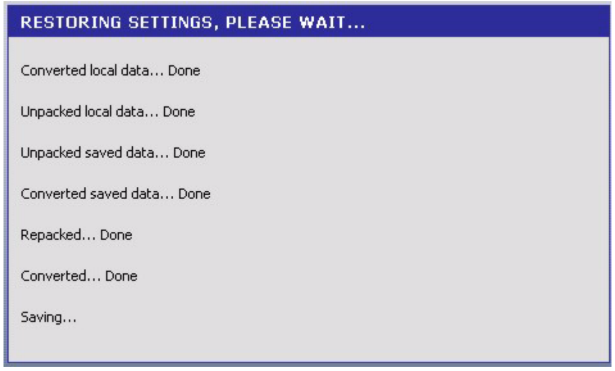
Follow the steps below to restore a previously saved configuration file to the P-336M.

1 In the web configurator click **Tools** > **Admin** (see Figure 30 on page 67).

2 Scroll to the bottom of the **Admin** screen. Enter a configuration file name in the field provided or click **Browse** to locate it.

3 Click **Restore a Configuration File** to start the file upload process. A status screen displays showing the restoration progress.

Figure 34 Tools: Admin: Configuration Restore Progress



RESTORING SETTINGS, PLEASE WAIT...

Converted local data... Done

Unpacked local data... Done

Unpacked saved data... Done

Converted saved data... Done

Repacked... Done

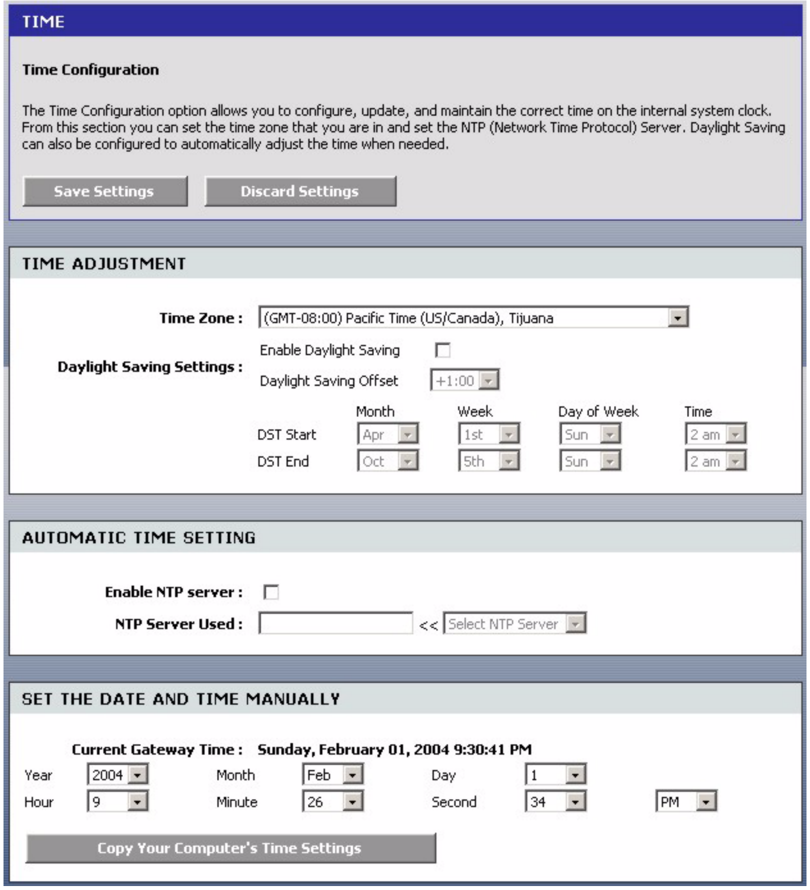
Converted... Done

Saving...

5.2 System Time and Date

To change your P-336M's time and date, click **Tools** > **Time**. Use this screen to configure the P-336M's system time based on your local time zone.

Figure 35 Tools: Time



TIME

Time Configuration

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

TIME ADJUSTMENT

Time Zone : (GMT-08:00) Pacific Time (US/Canada), Tijuana

Daylight Saving Settings :

Enable Daylight Saving □

Daylight Saving Offset +1:00

	Month	Week	Day of Week	Time
DST Start	Apr	1st	Sun	2 am
DST End	Oct	5th	Sun	2 am

AUTOMATIC TIME SETTING

Enable NTP server : □

NTP Server Used : << Select NTP Server

SET THE DATE AND TIME MANUALLY

Current Gateway Time : Sunday, February 01, 2004 9:30:41 PM

Year	2004	Month	Feb	Day	1	
Hour	9	Minute	26	Second	34	PM

The following table describes the labels in this screen.

Table 29 Tools: Time

LABEL	DESCRIPTION
Time Adjustment	
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 Saving Settings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Enable Daylight Saving	Select this option to if you use Daylight Saving Time.
Daylight Saving Offset	Enter the off set time for daylight saving time.

Table 29 Tools: Time (continued)

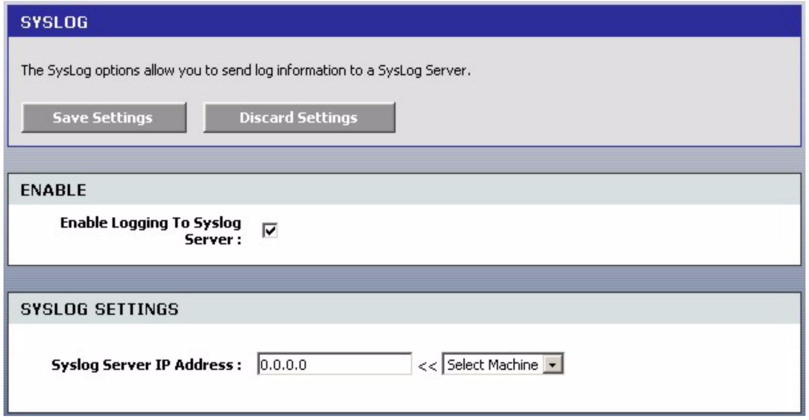
LABEL	DESCRIPTION
DST Start	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **Time** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each 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 **1st**, **Sun**, **Apr** and select **2 am** in the **Time** 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 the last **Sun**, **Mar**. The time you select in the **Time** 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).
DST End	Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **Time** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. 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 the last **Sun**, **Oct** and select **2 am** in the **Time** 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 the last **Sun**, **Oct**. The time you select in the **Time** 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).
Automatic Time Setting	
Enable NTP Server	Select this option to have the P-336M get the time and date from the Network Time Protocol (NTP) time server you specified below.
NTP Server Used	Enter the IP address (in dotted decimal notation) of the time server or select one from the pre-defined list.
Set the Date and Time Manually	These fields display when you clear the **Enable NTP Server** checkbox.
Current Gateway Time	This field displays the current system time and date.
Year/ Month/ Day/ Hour/ Minute/ Second	Set these fields to configure the system date and time.
Copy Your Computer’s Time Settings	Click this button to get the system date and time from your computer.

5.3 Syslog

Use the **Syslog** screen to configure to where the P-336M is to send logs.

Click **Tools > Syslog**.

Figure 36 Tools: Syslog



SYSLOG

The SysLog options allow you to send log information to a SysLog Server.

ENABLE

Enable Logging To Syslog Server : ☑

SYSLOG SETTINGS

Syslog Server IP Address : 0.0.0.0 << Select Machine

The following table describes the labels in this screen.

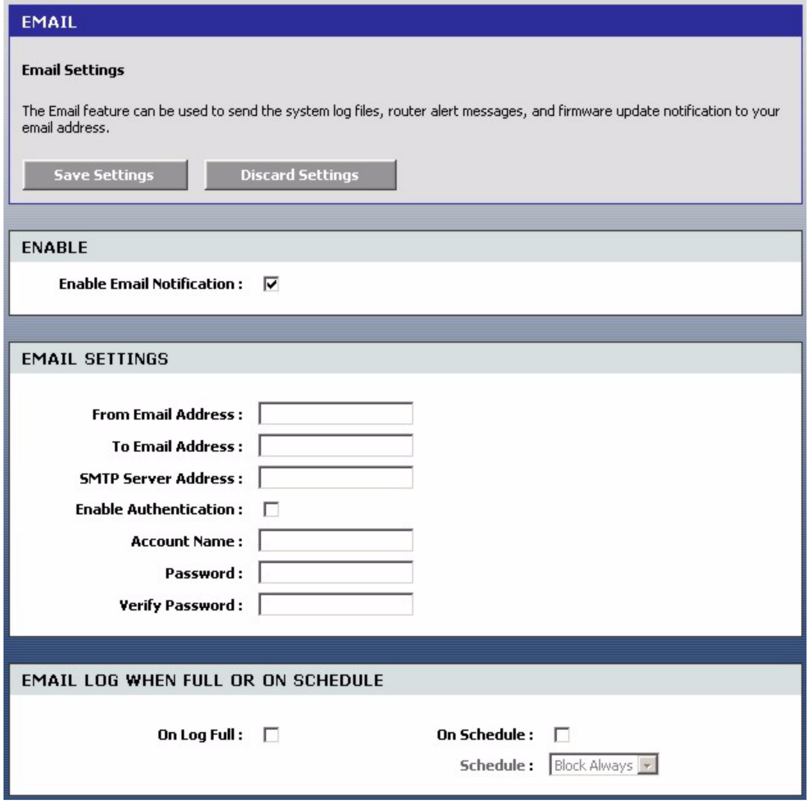
Table 30 Tools: Syslog

LABEL	DESCRIPTION
Enable	Select **Enable Logging To Syslog Server** to activate this feature.
Syslog Settings	
Syslog Server IP Address	Enter the IP address (in dotted decimal notation) of the syslog server to which the P-336M is to send logs. Alternatively, select a computer from the drop-down list box.

5.4 E-mail

Click Tools > E-mail configure where the P-336M is to send logs and alerts.

Figure 37 Tools: E-mail



EMAIL

Email Settings

The Email feature can be used to send the system log files, router alert messages, and firmware update notification to your email address.

ENABLE

Enable Email Notification : ☑

EMAIL SETTINGS

From Email Address :

To Email Address :

SMTP Server Address :

Enable Authentication : □

Account Name :

Password :

Verify Password :

EMAIL LOG WHEN FULL OR ON SCHEDULE

On Log Full : □

On Schedule : □

Schedule : Block Always

The following table describes the labels in this screen.

Table 31 Tools: E-mail

LABEL	DESCRIPTION
Enable	Select **Enable Email Notification** to activate this feature.
Email Settings	
From Email Address	Enter an e-mail as the sender.
To Email Address	Enter the e-mail address to which notifications are sent.
SMTP Server Address	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. Enter the IP address (in dotted decimal notation) of the mail server.
Enable Authentication	Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail logs.
Account Name	Enter the user name (up to 31 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Verify Password	Enter the password again for verification.
Email Log When Full or On Schedule	

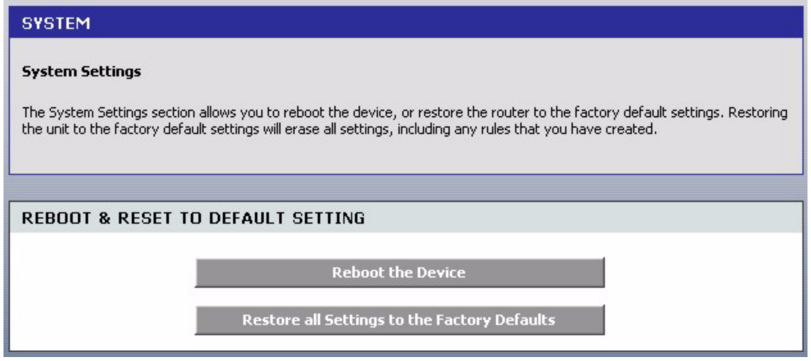
Table 31 Tools: E-mail (continued)

LABEL	DESCRIPTION
On Log Full	Select this option to send logs when all log entries are filled.
On Schedule	Select this option to send logs at the time defined in the selected schedule.

5.5 System

Use the **System** screen to reboot or reset your P-336M. Click **Tools** > **System** to display the screen as shown.

Figure 38 Tools: System



SYSTEM

System Settings

The System Settings section allows you to reboot the device, or restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you have created.

REBOOT & RESET TO DEFAULT SETTING

5.5.1 Rebooting Your P-336M

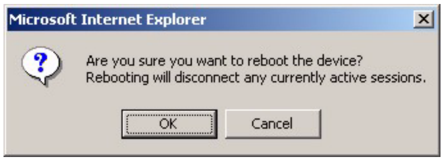
Note: When you reboot the device, all unsaved changes will be lost.

Follow the steps below to restart your P-336M.

1 In the web configurator, click **Tools** > **System** and click **Reboot the Device**.

2 A screen displays. Click **OK** to continue.

Figure 39 Tools: System: Reboot the Device



Microsoft Internet Explorer

Are you sure you want to reboot the device?
Rebooting will disconnect any currently active sessions.

3 Wait until the P-336M finishes rebooting before accessing the web configurator.

5.5.2 Device Reset

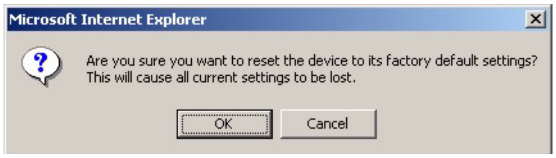
Note: When you reset the device, all custom changes will be lost.

Follow the steps below to reset your P-336M.

1 In the web configurator, click **Tools** > **System** and click **Restore all Settings to the Factory Defaults**.

2 A screen displays. Click **OK** to continue.

Figure 40 Tools: System: Reset



Microsoft Internet Explorer

Are you sure you want to reset the device to its factory default settings?
This will cause all current settings to be lost.

3 Wait until the P-336M finishes rebooting before accessing the web configurator.

5.6 Firmware

Use the Firmware screen to update the firmware on your P-336M.

1 Download the latest firmware file from www.zyxel.com.

2 In the web configurator, click **Tools** > **Firmware**.

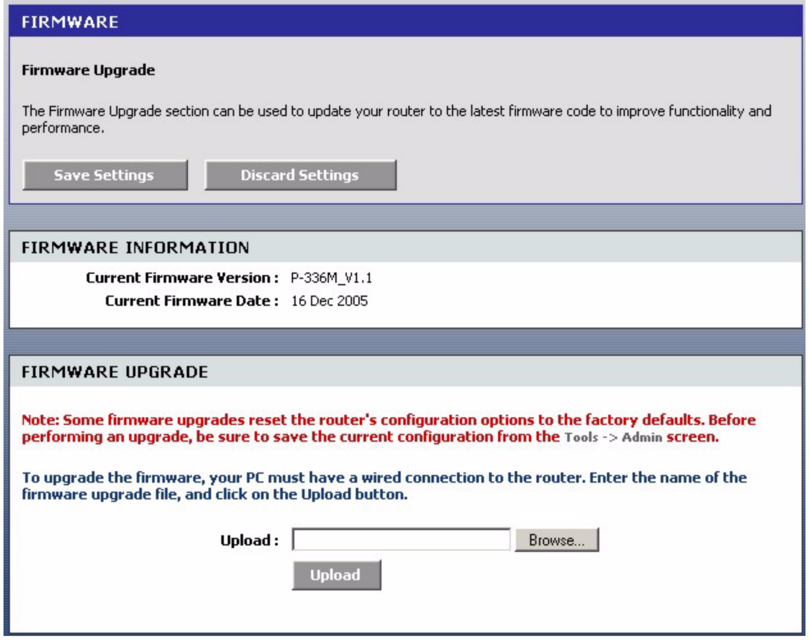
3 In the **Uplaod** field, enter the new firmware file name or click **Browse** to locate it.

4 Click **Upload** to start the file transfer process.

Note: Do not turn off the P-336M while the file transfer process is taking place.

5 Wait for the P-336M finishes rebooting before accessing the web configurator again. Check the firmware version and date in the Firmware screen.

Figure 41 Tools: Firmware



FIRMWARE

Firmware Upgrade

The Firmware Upgrade section can be used to update your router to the latest firmware code to improve functionality and performance.

FIRMWARE INFORMATION

Current Firmware Version : P-336M_V1.1
Current Firmware Date : 16 Dec 2005

FIRMWARE UPGRADE

Note: Some firmware upgrades reset the router's configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the Tools -> Admin screen.

To upgrade the firmware, your PC must have a wired connection to the router. Enter the name of the firmware upgrade file, and click on the Upload button.

Upload :

5.7 DDNS

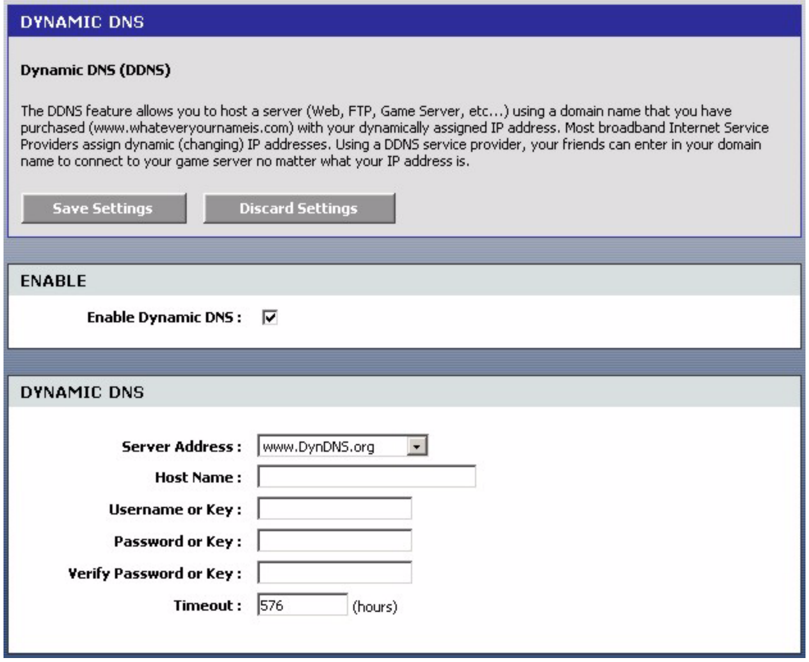
Dynamic DNS (DDNS) allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

Note: You must go to the Dynamic DNS service provider's website and register a user account and a domain name before you can use the Dynamic DNS service with your P-336M.

Click **Tools** > **DDNS** to display the configuration screen.

Figure 42 Tools: DDNS



DYNAMIC DNS

Dynamic DNS (DDNS)

The DDNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter in your domain name to connect to your game server no matter what your IP address is.

ENABLE

Enable Dynamic DNS : ☑

DYNAMIC DNS

Server Address : www.DynDNS.org
Host Name :
Username or Key :
Password or Key :
Verify Password or Key :
Timeout : 576 (hours)

The following table describes the labels in this screen.

Table 32 Tools: DDNS

LABEL	DESCRIPTION
Enable	Select Enable Dynamic DNS to active this feature.
Dynamic DNS	
Service Address	Select the web address of your Dynamic DNS service provider.

Table 32 Tools: DDNS

LABEL	DESCRIPTION
Host Name	Enter the system name.
Username or Key	Enter your user name. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed.
Password or Key	Enter the password associated with the user name above. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed.
Verify Password or Key	Enter the password again for confirmation.
Timeout	Specify the time (in hours) the P-336M waits before time out.

CHAPTER 6
Status

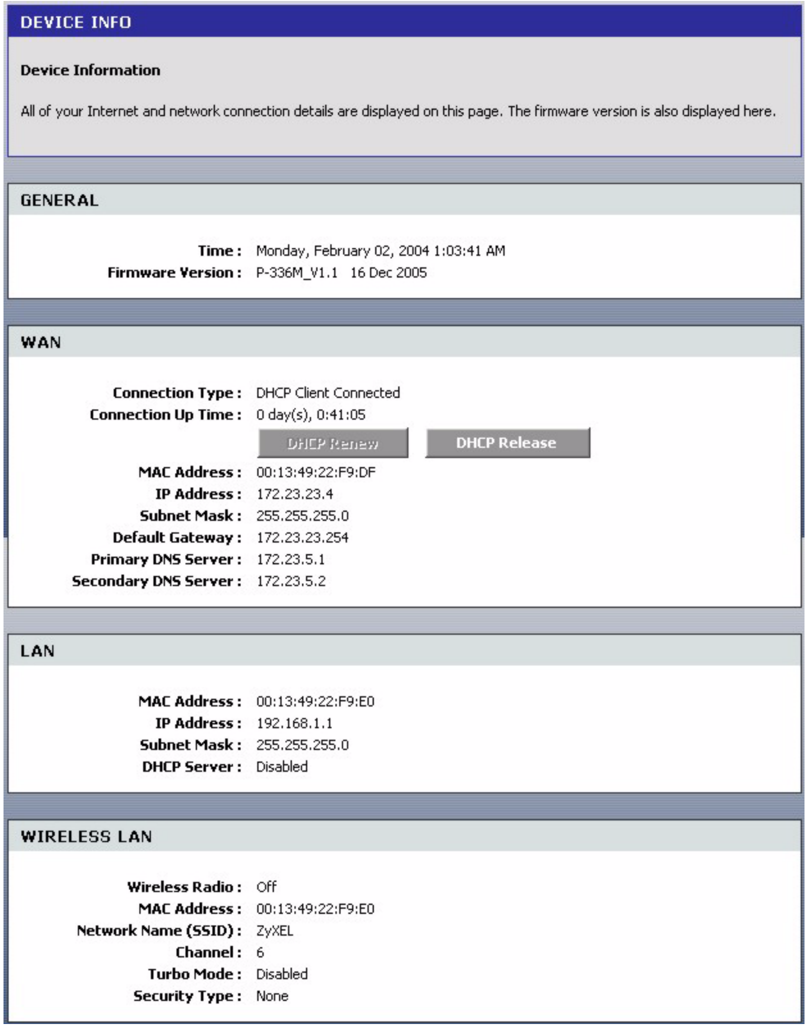
This chapter describes the **Status** screens you use to view the system status and logs.

6.1 Device Info

Display the **Device Status** screen to view device information such as the system time and interface settings.

Click **Status** > **Device Status** to display the screen.

Figure 43 Status: Device Info



DEVICE INFO

Device Information

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

GENERAL

Time : Monday, February 02, 2004 1:03:41 AM
Firmware Version : P-336M_V1.1 16 Dec 2005

WAN

Connection Type : DHCP Client Connected
Connection Up Time : 0 day(s), 0:41:05
MAC Address : 00:13:49:22:F9:DF
IP Address : 172.23.23.4
Subnet Mask : 255.255.255.0
Default Gateway : 172.23.23.254
Primary DNS Server : 172.23.5.1
Secondary DNS Server : 172.23.5.2

LAN

MAC Address : 00:13:49:22:F9:E0
IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0
DHCP Server : Disabled

WIRELESS LAN

Wireless Radio : Off
MAC Address : 00:13:49:22:F9:E0
Network Name (SSID) : ZyXEL
Channel : 6
Turbo Mode : Disabled
Security Type : None

The following table describes the labels in this screen.

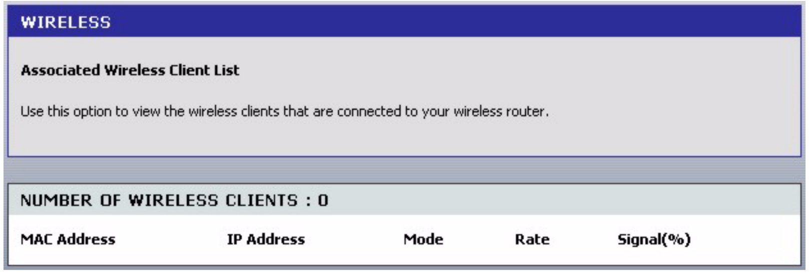
Table 33 Tools: Admin

LABEL	DESCRIPTION
General	
Time	This field displays the current system date and time.
Firmware Version	This field displays the firmware version and the date created.
WAN	
Connection Type	This field displays the connection status.
Connection Up Time	This field displays the time since the connection was up.
DHCP Renew	This button is applicable when the P-336M uses a dynamic IP address. Click **DHCP Renew** to get a new dynamic IP address.
DHCP Release	This button is applicable when the P-336M uses a dynamic IP address. Click **DHCP Release** to release the current IP address. You must then click **DHCP Renew** to get a new IP address.
Connect	This button is available when the P-336M is set to use PPPoE connection type. Click **Connect** to establish an Internet connection using PPPoE.
Disconnect	This button is available when the P-336M is set to use PPPoE connection type. Click **Disconnect** to disconnect the Internet connection.
MAC Address	This field displays the MAC address of the WAN port on the P-336M.
IP Address	This field displays the WAN IP address.
Subnet Mask	This field displays the WAN subnet mask.
Default Gateway	This field displays the IP address of the gateway on the WAN.
Primary/ Secondary DNS Server	This field displays the IP address(es) of the DNS server(s).
LAN	
MAC Address	This field displays the MAC address of the LAN port on the P-336M.
IP Address	This field displays the LAN IP address.
Subnet Mask	This field displays the LAN subnet mask.
DHCP Server	This field displays whether the DHCP server is active or not on the LAN.
Wireless LAN	
Wireless Radio	This field displays whether the wireless LAN feature is active or not.
MAC Address	This field displays the MAC address of the WLAN interface on the P-336M.
Network Name (SSID)	This field displays the name of the wireless network.
Channel	This field displays the wireless channel number the P-336M is using.
Turbo Mode	This field displays whether the turbo mode is active or not.
Security Type	This field displays the wireless LAN security type.

6.2 Wireless

To view a list of wireless clients currently connected to the P-336M, click **Status > Wireless**.

Figure 44 Status: Wireless



WIRELESS

Associated Wireless Client List

Use this option to view the wireless clients that are connected to your wireless router.

NUMBER OF WIRELESS CLIENTS : 0

MAC Address	IP Address	Mode	Rate	Signal(%)

The following table describes the fields in this screen.

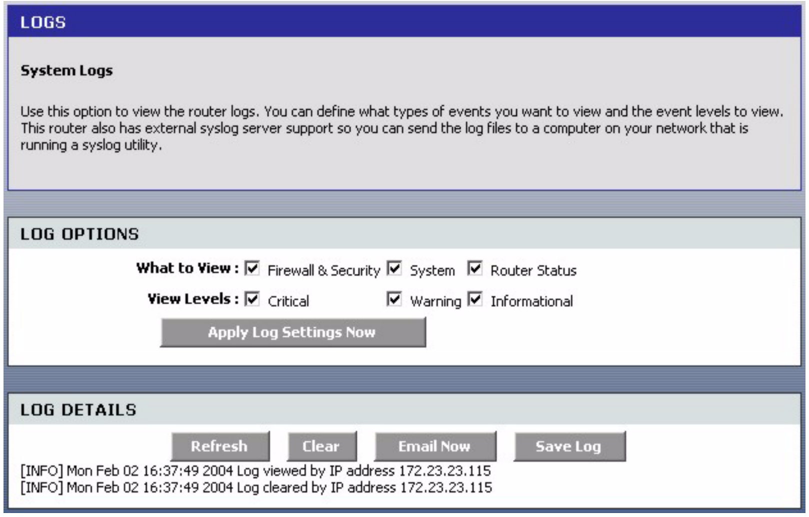
Table 34 Association List

LABEL	DESCRIPTION
Number of Wireless Clients	This field displays the number of wireless clients currently connected to the P-336M.
MAC Address	This field displays the MAC (Media Access Control) address of an associated wireless station. Every Ethernet device has a unique MAC 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.
IP Address	This field displays the LAN IP address of the wireless client.
Mode	This field displays the wireless standard the wireless client is using.
Rate	This field displays the transmission rate (in megabits per second) of the wireless client.
Signal (%)	This field displays the relative measurement of the signal strength (in percentage).

6.3 Logs

To view system logs, click Status > Logs.

Figure 45 Status: Logs



LOGS

System Logs

Use this option to view the router logs. You can define what types of events you want to view and the event levels to view. This router also has external syslog server support so you can send the log files to a computer on your network that is running a syslog utility.

LOG OPTIONS

What to View : ☑ Firewall & Security ☑ System ☑ Router Status

View Levels : ☑ Critical ☑ Warning ☑ Informational

LOG DETAILS

```
[INFO] Mon Feb 02 16:37:49 2004 Log viewed by IP address 172.23.23.115
[INFO] Mon Feb 02 16:37:49 2004 Log cleared by IP address 172.23.23.115
```

The following table describes the labels in this screen.

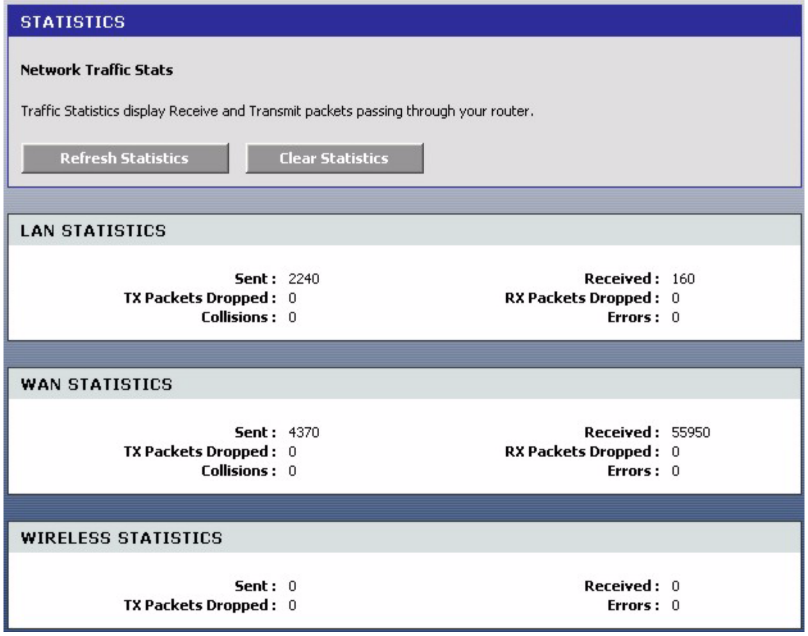
Table 35 Status: Logs

LABEL	DESCRIPTION
Log Options	
What to View	Select the type of logs to display in this screen.
View Levels	Select the log severity level to display in this screen.
Apply Log Settings Now	Click this button to save the changes in this screen.
Log Details	
Refresh	Click **Refresh** to update this screen.
Clear	Click **Clear** to delete all the logs. Once deleted, you cannot view the logs again.
Email Now	Click **Email Now** to send the logs to the e-mail you specified in the **Tools > E-mail** screen.
Save Log	Click **Save Log** to store the logs to a file on your computer.

6.4 Statistics

To view the LAN, WAN and WLAN statistics, click Status > Statistics.

Figure 46 Status: Statistics



STATISTICS

Network Traffic Stats

Traffic Statistics display Receive and Transmit packets passing through your router.

LAN STATISTICS

Sent : 2240
TX Packets Dropped : 0
Collisions : 0
Received : 160
RX Packets Dropped : 0
Errors : 0

WAN STATISTICS

Sent : 4370
TX Packets Dropped : 0
Collisions : 0
Received : 55950
RX Packets Dropped : 0
Errors : 0

WIRELESS STATISTICS

Sent : 0
TX Packets Dropped : 0
Received : 0
Errors : 0

The following table describes the labels in this screen.

Table 36 Status: Statistics

LABEL	DESCRIPTION
LAN Statistics	
Sent	This field displays the number of packets sent on the LAN.
Tx Packets Dropped	This field displays the number of transmitted packets that were dropped on the LAN.
Collisions	This field displays the number of packets sent with collision errors on the LAN.
Received	This field displays the number of packets received on the LAN.
Rx Packets Dropped	This field displays the number of packets received that were dropped on the LAN.
Errors	This field displays the number of packets received with errors on the LAN.
WAN Statistics	
Sent	This field displays the number of packets sent on the WAN.
Tx Packets Dropped	This field displays the number of transmitted packets that were dropped on the WAN.
Collisions	This field displays the number of packets sent with collision errors on the WAN.
Received	This field displays the number of packets received on the WAN.
Rx Packets Dropped	This field displays the number of packets received that were dropped on the WAN.
Errors	This field displays the number of packets received with errors on the WAN.
WLAN Statistics	
Sent	This field displays the number of packets sent on the WLAN.
Tx Packets Dropped	This field displays the number of transmitted packets that were dropped on the WLAN.

Table 36 Status: Statistics (continued)

LABEL	DESCRIPTION
Received	This field displays the number of packets received on the WLAN.
Errors	This field displays the number of packets received with errors on the WLAN.

Appendix A
Types of EAP Authentication

This appendix discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP.

The type of authentication you use depends on the RADIUS server or the AP (consult your network administrator for more information). Your wireless LAN device may not support all authentication types.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station '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 stations 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 screen. You may still configure and store keys here, 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

User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless stations using an external RADIUS database.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES), Message Integrity Check (MIC) and IEEE 802.1x.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates 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 stations. This all happens in the background automatically.

AES (Advanced Encryption Standard) also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data.

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), TKIP makes it much more difficult to decrypt data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it’s still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ 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	ENCRYPTION METHOD	ENTER MANUAL KEY	ENABLE IEEE 802.1X
Open	None	No	No
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	WEP	No	Yes
WPA	TKIP	No	Yes
WPA-PSK	WEP	Yes	Yes
WPA-PSK	TKIP	Yes	Yes

Appendix B
Setting up Your Computer’s IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

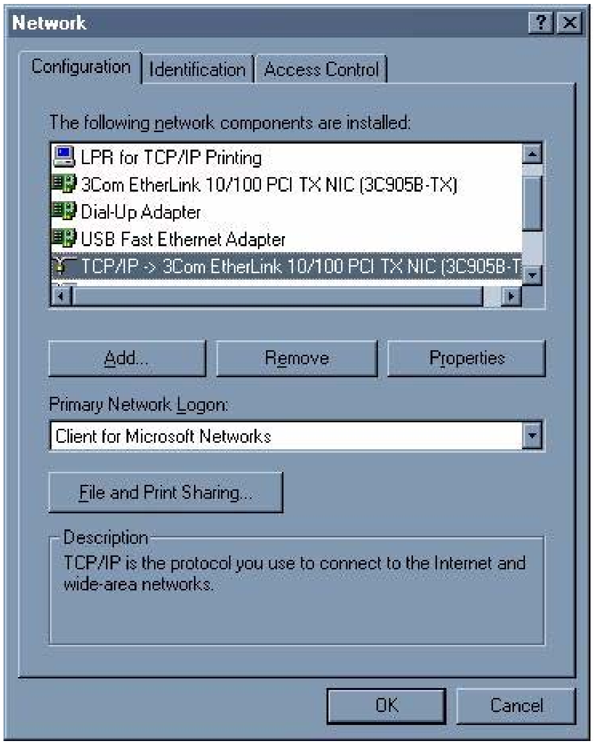
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the P-336M’s LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window

Figure 47 WIndows 95/98/Me: Network: Configuration



The following network components are installed:

LPR for TCP/IP Printing
3Com EtherLink 10/100 PCI TX NIC (3C905B-TX)
Dial-Up Adapter
USB Fast Ethernet Adapter
TCP/IP -> 3Com EtherLink 10/100 PCI TX NIC (3C905B-T

Primary Network Logon:
Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1 In the **Network** window, click **Add**.
2 Select **Adapter** and then click **Add**.
3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1 In the **Network** window, click **Add**.
2 Select **Protocol** and then click **Add**.
3 Select **Microsoft** from the list of **manufacturers**.
4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1 Click **Add**.
2 Select **Client** and then click **Add**.

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

5 Restart your computer so the changes you made take effect.

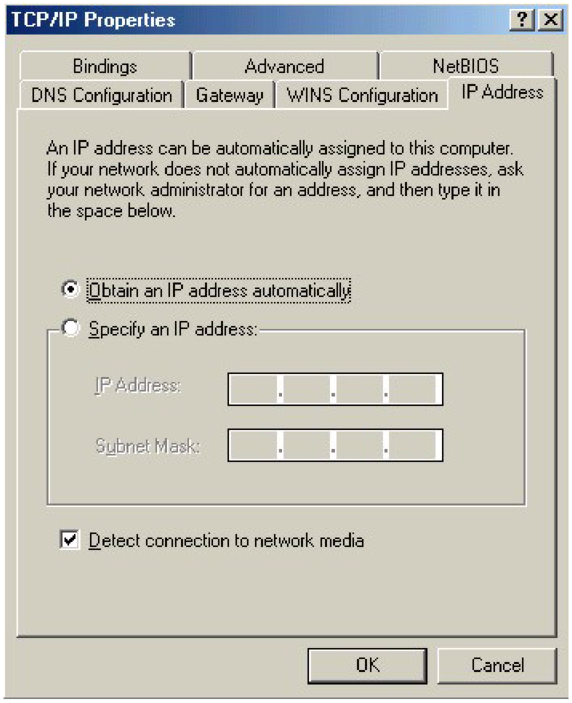
Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 48 Windows 95/98/Me: TCP/IP Properties: IP Address



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

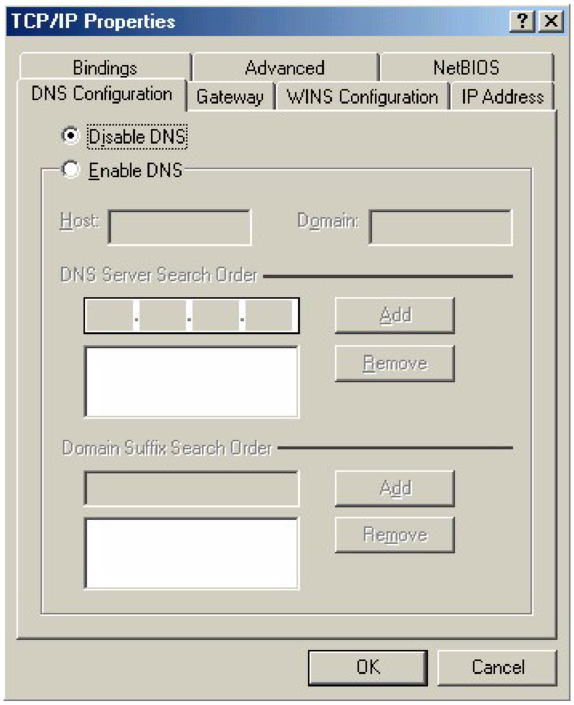
○ Specify an IP address:

☑ Detect connection to network media

3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 49 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



● Disable DNS

○ Enable DNS

4 Click the **Gateway** tab.

- If you do not know your gateway’s IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your P-336M and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

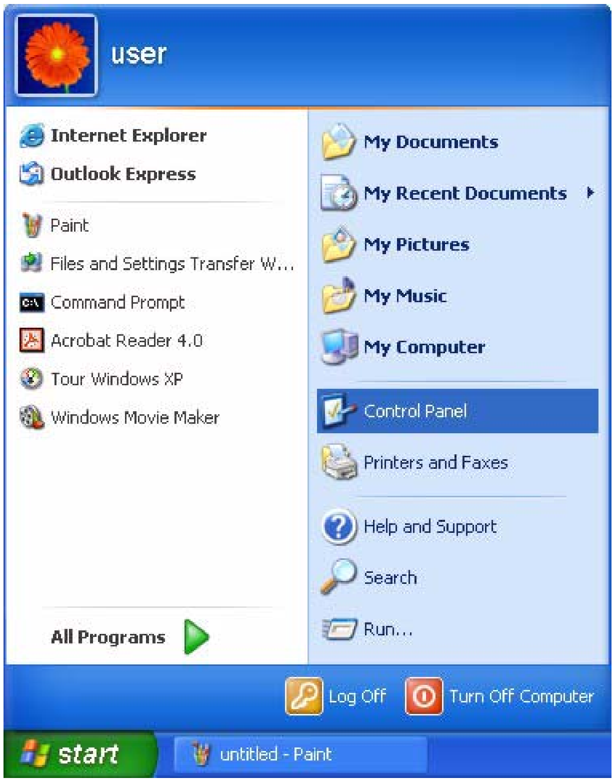
2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

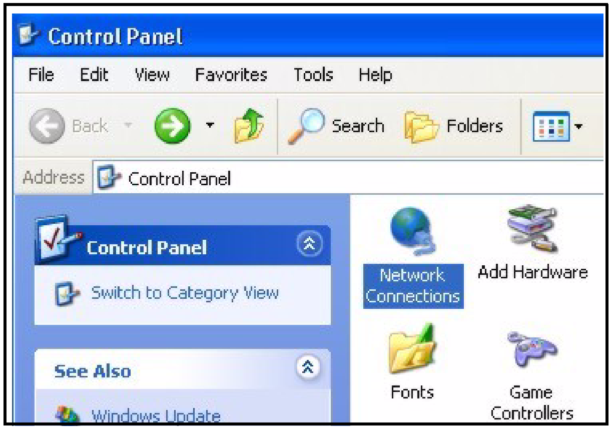
1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

Figure 50 Windows XP: Start Menu



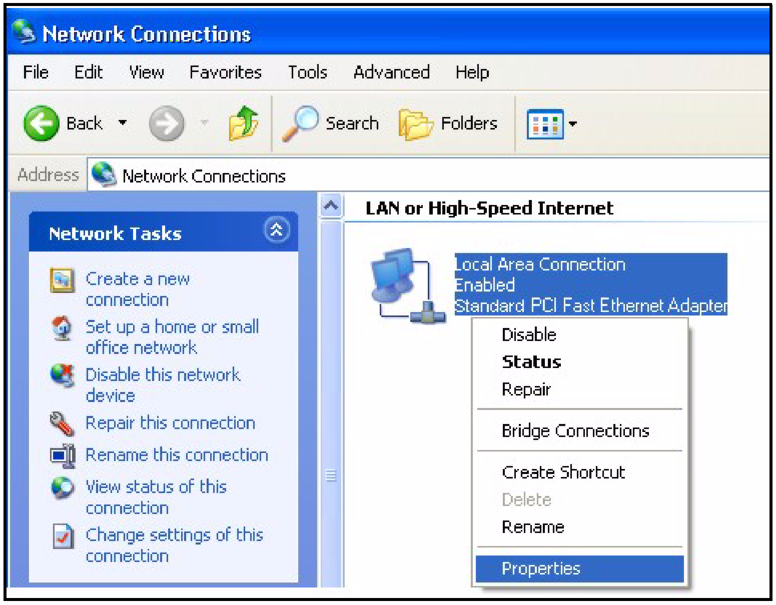
2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 51 Windows XP: Control Panel



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

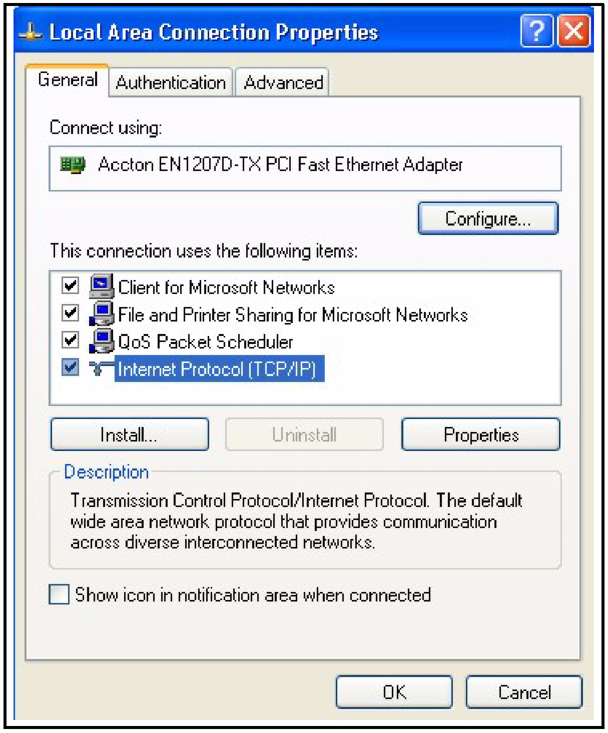
Figure 52 Windows XP: Control Panel: Network Connections: Properties



Local Area Connection
Enabled
Standard PCI Fast Ethernet Adapter

4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

Figure 53 Windows XP: Local Area Connection Properties



Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

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

Description

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

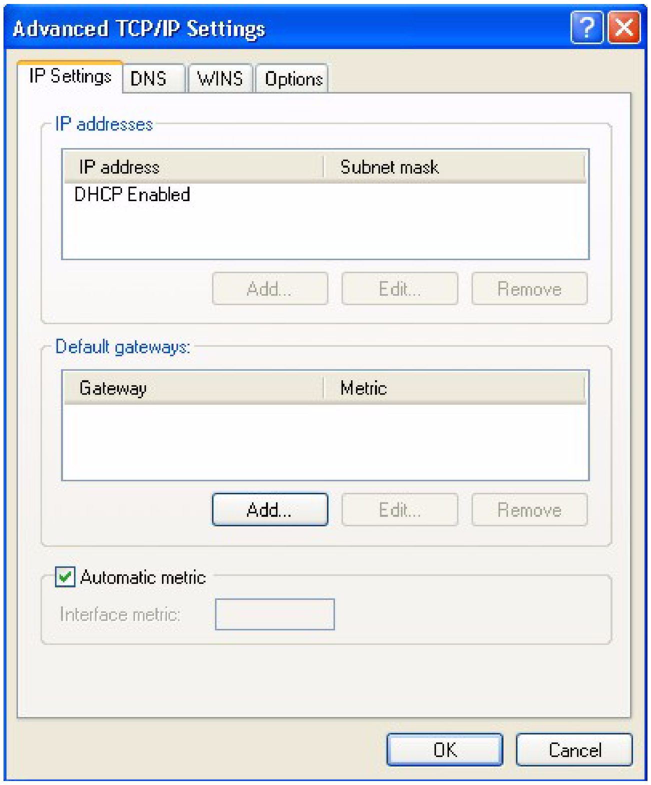
☐ Show icon in notification area when connected

5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.

- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields. Click **Advanced**.

Figure 54 Windows XP: Advanced TCP/IP Settings



IP address	Subnet mask
DHCP Enabled	

Gateway	Metric

☑ Automatic metric

6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settin**gs tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

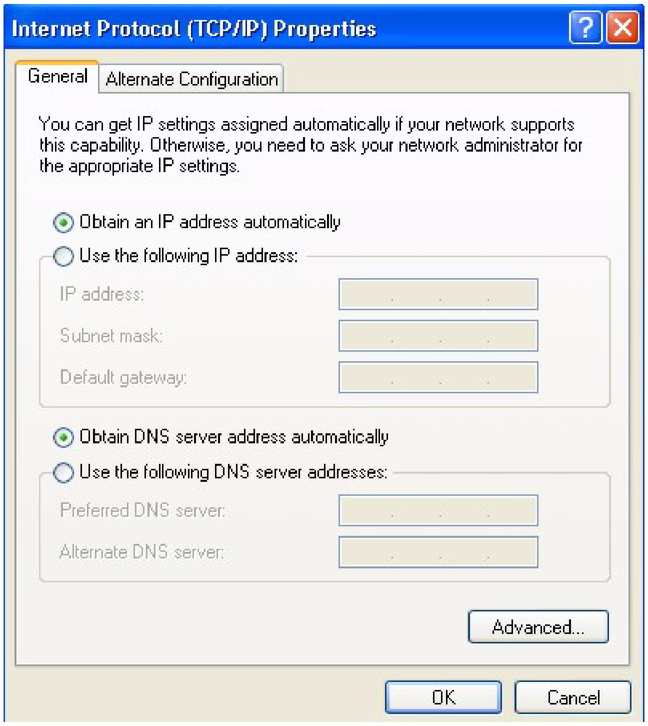
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 55 Windows XP: Internet Protocol (TCP/IP) Properties



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

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

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

10Turn on your P-336M and restart your computer (if prompted).

Verifying Settings

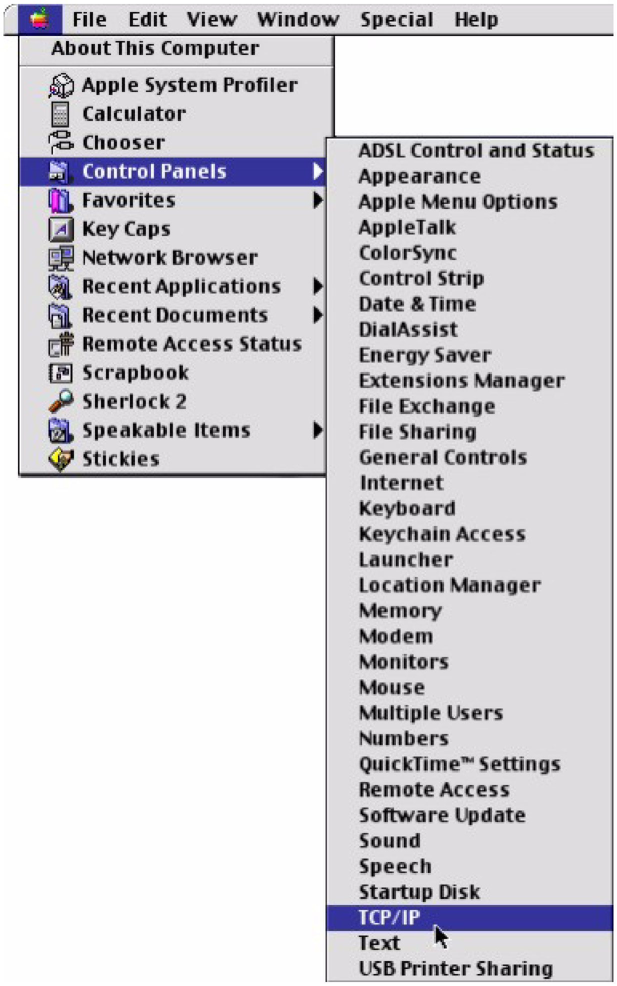
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

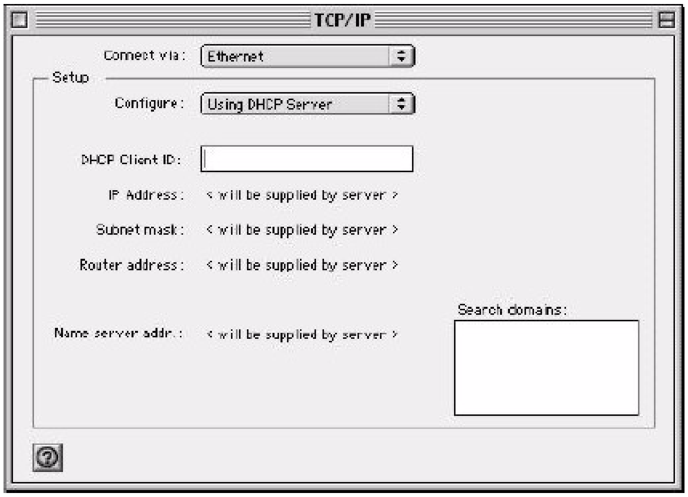
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 56 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 57 Macintosh OS 8/9: TCP/IP



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Name server addr.: < will be supplied by server >

Search domains:

3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your P-336M in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your P-336M and restart your computer (if prompted).

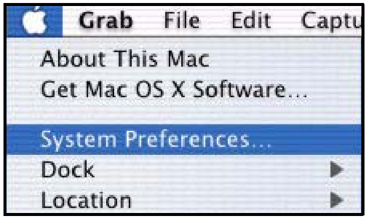
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 58 Macintosh OS X: Apple Menu

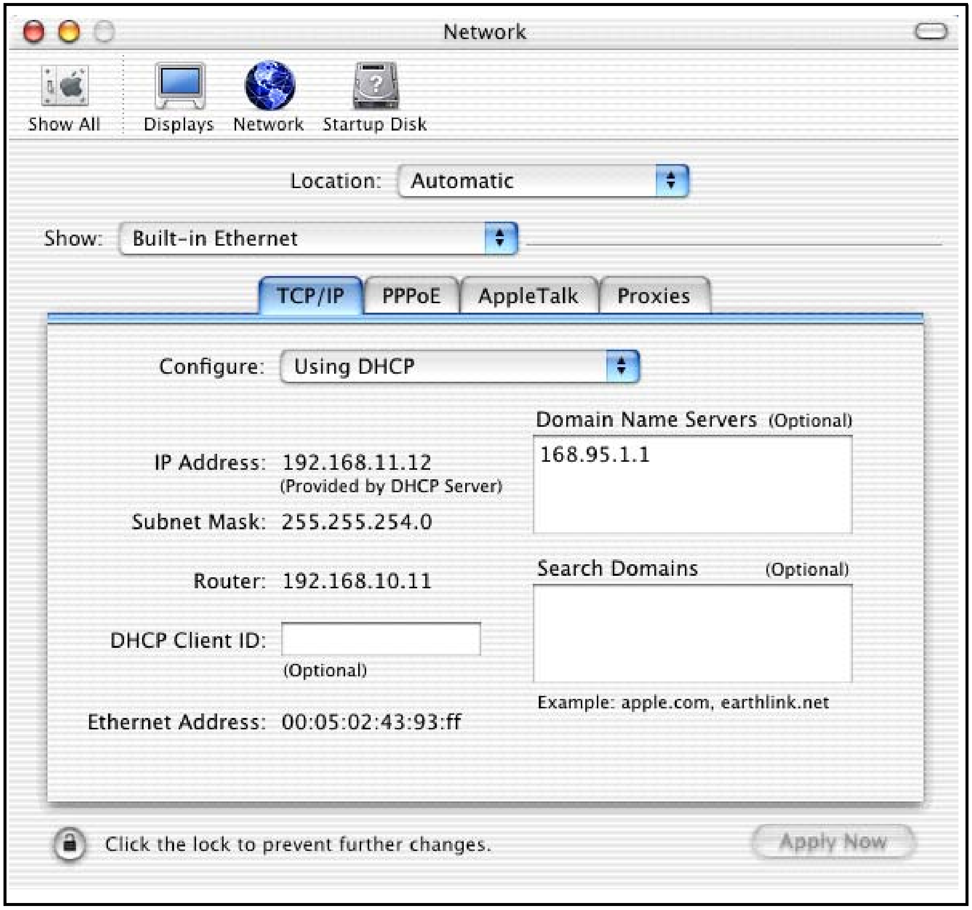


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 59 Macintosh OS X: Network



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

Ethernet Address: 00:05:02:43:93:ff

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

Click the lock to prevent further changes.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your P-336M in the **Router address** box.

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

6 Turn on your P-336M and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Index