Networking Gateway

System Manual

S/W Version 2.0
August 2005
P/N 214196

About This Manual

This manual contains the following chapters:

Â **Chapter 1 – Product Description**: Describes the Networking Gateway and its components.

Â **Chapter 2 – Installation**: Describes how to install the system and its components.

Â **Chapter 3 – Operation and Administration**: Describes how to use the web-based management application for configuring parameters and managing the Networking Gateway.

Â **Appendix A – Print Server**: Describes how to configure the printer server.

Â **Appendix B – 802.1x Setting.**

Contents

Figures

Tables

1

Chapter 1 - Product Description

In This Chapter:

1.1 Introducing the Networking Gateway IDU

The Networking Gateway Indoor Unit (IDU) enables operators and service providers using a Broadband Wireless Access system to provide subscribers with a number of broadband services transparently.

The Networking Gateway IDU together with the SU-ODU comprises a Subscriber Unit that provides data connections to the Base Station. The four 10/100Base-T Ethernet ports connect to the user's data equipment, providing comprehensive routing functionality and supporting various security features. User's data equipment equipped with either IEEE 802.11b (11M) or IEEE 802.11g (54M) compatible wireless adapters can connect to the unit via its built-in Wireless LAN port, functioning as an Access Point.

The Networking Gateway IDU is powered from the mains. The Networking Gateway IDU is connected to the ODU via a category 5E Ethernet cable. This cable carries the Ethernet data between the two units as well as power (54 VDC) and control signals to the ODU. It also carries status indications from the ODU.

The Networking Gateway is designed for remote management and supervision using either the built-in internal web server or SNMP.

The Networking Gateway is easily updated and upgraded as it supports remote software and configuration file download.

1.2 Functions and Features

1.2.1 Basic Functions

Â **Auto-sensing Ethernet Switch**
Equipped with a 4-port auto-sensing Ethernet switch.

Â **Printer sharing**
Embedded print server to allow all of the networked computers to share one printer through the USB host port.

Â **WAN Types**
Support of several WAN types: Static, Dynamic, PPPoE, PPTP, and Dynamic IP with Road Runner Session Management (e.g., Telstra, BigPond).

Â **Firewall**
All unwanted packets from outside intruders can be blocked to protect the Intranet.

Â **DHCP Server Support**
All of the networked computers can retrieve TCP/IP settings automatically from the Networking Gateway.

Â **Web-based configuring**
Configurable through any networked computer's web browser using Netscape or Internet Explorer.

Â **Virtual Server Support**
Enables to expose WWW, FTP and other services on your LAN to other Internet users.

Â **User-Definable Application Sensing Tunnel**
Users can define the attributes to support special applications requiring multiple connections, such as Internet gaming, video conferencing, Internet telephony and so on. The Networking Gateway can sense the application type port as a trigger and open a multi-port tunnel for it.

Â **DMZ Host Support**
Lets one specific networked computer be fully exposed to the Internet. This function is used when special application sensing tunnel feature is insufficient to allow an application to function correctly. Use with caution.

Â **Statistics of WAN Support**

Enables to monitor inbound and outbound packets.

1.2.2 Wireless Functions

Â **High speed for wireless LAN connection**

Up to 54 Mbps data rate by incorporating Orthogonal Frequency Division Multiplexing (OFDM).

Â **IEEE 802.11b compatible (11M)**

Allowing inter-operation among multiple vendors.

Â **IEEE 802.11g compatible (54M)**

Allowing inter-operation among multiple vendors.

Â **Auto fallback**

54M, 48M, 36M, 24M, 18M, 12M, 6M data rates with auto fallback in 802.11g mode.

11M, 5.5M, 2M, 1M data rates with auto fallback in 802.11b mode.

1.2.3 Security Functions

Â **Packet Filter**

Packet Filter allows controlling access to a network by analyzing the incoming and outgoing packets and letting them pass or blocking them based on the source and destination IP addresses and ports.

Â **Domain Filter Support**

Enables preventing users from accessing specific domains.

Â **URL Blocking Support**

URL Blocking uses keywords to block hundreds of applicable websites connections.

Â **VPN Pass-through**

The Networking Gateway can also support VPN pass-through.

Â **802.1X Support**

When the 802.1X function is enabled, the Wireless user must be authenticated by the Networking Gateway before being allowed to use the Network services.

Â **SPI Mode Support**

When SPI Mode is enabled, the Networking Gateway checks every incoming packet and detects if this packet has changed its IP address since initial negotiation.

Â **DoS Attack Detection Support**

When this feature is enabled, the Networking Gateway detects and logs Denial of Service (DoS) attack arriving from the Internet.

1.2.4 Advanced Functions

Â **System Time**

Allows synchronizing system time with a network time server, with the PC, or set the time manually.

Â **E-mail Alert**

The Networking Gateway can be configured to send its log file by mail.

Â **Dynamic DNS**

At present, the Networking Gateway supports 3 Dynamic DNSs: DynDNS.org, TZO.com and dhs.org.

Â **SNMP Support**

The Networking Gateway supports SNMP V1 and V2c.

Â **Routing Table**

The Networking Gateway supports static routing and two kinds of dynamic routing: RIP1 and RIP2.

Â **Schedule Rule**

Customers can control the schedule (when to allow and when to block) for several functions, such as virtual server and packet filters.

1.3 Specifications

1.3.1 Radio Specifications

Table 1: Radio Specifications

Item	Description
Frequency	2400-2483.5 MHz
Wireless LAN Standards	Compliant with IEEE 802.11b and IEEE 802.11g
Output Power (Average)	10, 12, 15, 17 dBm
Data Rates	Â IEEE 802.11g mode: 54M, 48M, 36M, 24M, 18M, 12M, 6M with auto fallback in. Â IEEE 802.11b mode: 11M, 5.5M, 2M, 1M with auto fallback in.

1.3.2 Regulatory Standards Compliance

Table 2: Regulatory Standards Compliance

Type	Standard
EMC	ETS EN 301 489-17
Safety	Â EN 60950 (CE) Â IEC 60 950 US/C UL
Radio	Â ETSI 300 328 Â FCC Part 15
Immunity	EN 55024:1998

1.3.3 Environmental

Table 3: Environmental Specifications

Item	Details
Operating temperature	0 °C to 40 °C
Operating humidity	5%-95% non condensing

1.3.4 Mechanical

Table 4: Mechanical Specifications

Item	Details
Dimensions (W x H x D)	190.5 x 26.2 x 111 mm
Weight	0.62 kg

1.3.5 Electrical

Table 5: Electrical Specifications

Item	Details
Power Transformer	100-240 VAC, 50-60 Hz, 2A max. Supplies 5 VDC (for the Networking Gateway IDU) and 55 VDC (for the ODU via the RADIO connector)
Power Consumption	Â Networking Gateway IDU (5 VDC): 10W max Â ODU (55 VDC): 50W max.

2

Chapter 2 - Installation

In This Chapter:

2.1 Installation Requirements

2.1.1 Packing List

Â Networking Gateway IDU

Â Antenna

Â Power Transformer

Â Mains power cord

2.1.2 Additional Installation Requirements

Â Ethernet cable(s) for connecting to the end-user's data equipment.

Â Mains plug adapter or termination plug (if the power plug on the supplied AC power cord does not fit local power outlets).

Â PC with an Ethernet card and an Ethernet cable for configuring the Networking Gateway IDU parameters using a web browser, and for configuring the SU-ODU parameters using Telnet.

Â Other installation tools and materials (e.g., means for securing cables to walls, etc.)

2.2 Panels Layout and Components

2.2.1 Front Panel

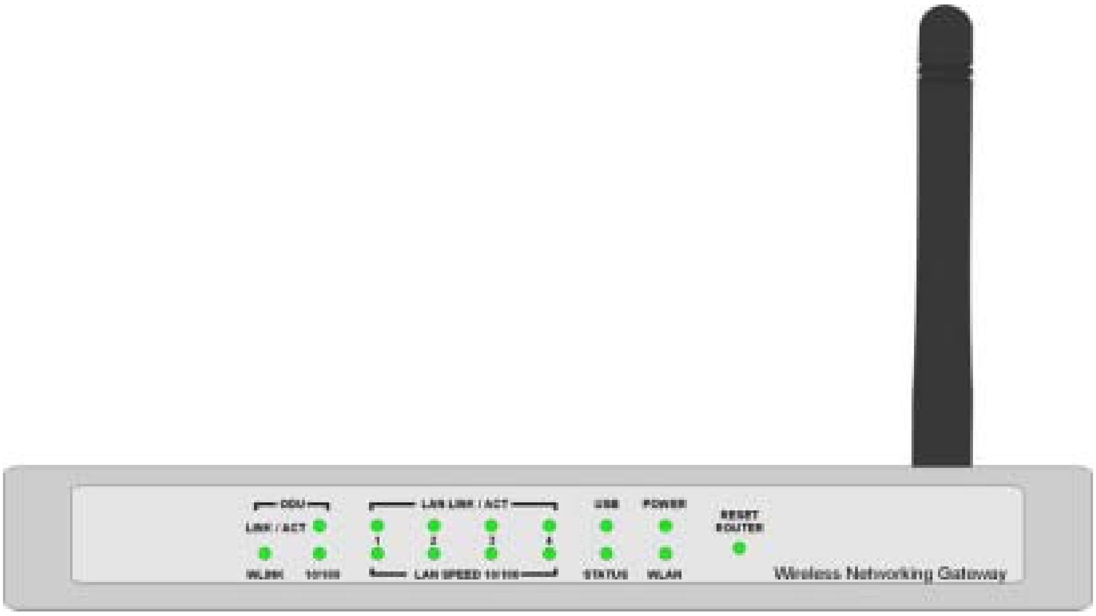


Figure 1: Front Panel

2.2.1.1 Front Panel LEDs

Table 6: Front Panel LEDs

LED	Function	Status	Description
POWER	Power Indication	On	Power is available.
WLAN	Wireless LAN Activity	Blinking	Sending or receiving data via wireless LAN.
USB	USB Port Activity	On	The USB port is linked.
		Blinking	The USB port is sending or receiving data.
STATUS	System Status	Blinking	The unit is functioning properly.
LAN LINK/ACT 1~4	LAN Status	On	An active station is connected to the corresponding LAN port.
		Blinking	The corresponding LAN port is sending or receiving data.
LAN SPEED 10/100 1~4	LAN Port Data Rate	On	Data rate is 100 Mbps on the corresponding LAN port.

LED	Function	Status	Description
		Off	Data rate is 10 Mbps on the corresponding LAN port.
ODU LINK/ACT	ODU Port Activity	On	The ODU port is connected to the ODU.
		Blinking	The ODU port is sending or receiving data.
ODU 10/100	ODU Port Data Rate	On	Data rate is 100 Mbps.
		Off	Data rate is 10 Mbps.
ODU WLINK	ODU Wireless Link Status	On	The ODU is connected with an AU.

2.2.1.2 RESET ROUTER Button

Press momentarily the recessed RESET ROUTER button to reset the Networking Gateway IDU.

2.2.1.3 Resetting the IDU to Factory Defaults

Press the RESET ROUTER button for at least 5 seconds, until the STATUS LED flashes 5 times. After releasing the button, the unit will resume operation with the factory default configuration.

2.2.2 Rear Panel Components

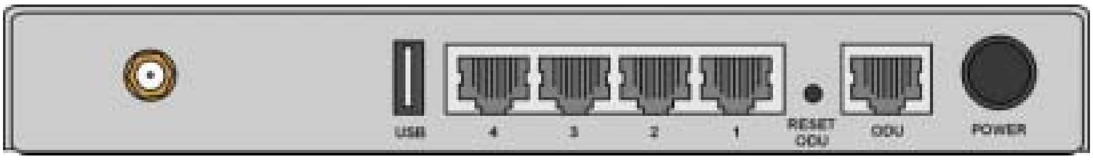


Figure 2: Rear Panel (without antenna)

2.2.2.1 Rear Panel Connectors

Table 7: Rear Panel Connectors

Connector	Description
POWER	DC Power Inlet from Power Transformer
ODU	Connection to the ODU. Carries Ethernet, Power (55 VDC) and signaling.
Port 1-4	LAN ports for networked computers and other devices.
USB	USB Host Port for a USB printer.
Antenna (not marked)	An SMA connector for the WLAN antenna

⚠ **CAUTION**

Do not connect data equipment to the ODU port. The ODU port supplies high DC power to the ODU, and this may harm other equipment connected to it.

2.2.2.2 RESET ODU Button

Press momentarily the recessed RESET ODU button to reset the ODU.

2.3 Installation

The unit can be placed on a desktop or a shelf. Alternatively, it may be wall-mounted.

For optimal performance, place the Networking Gateway in the center of your office (or your home), in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to a mains outlet and network connections.

To install the Networking Gateway IDU:

1. Assemble an RJ-45 connector with a protective cover on the indoor end of the IDU-ODU cable. The length of the IDU-ODU cable should not exceed 100m. Refer to the relevant System Manual for instructions on preparing the cable and for information on the cable type.
2. Connect the IDU-ODU cable to the ODU connector located on the rear panel.
3. Connect the power cord of the transformer to the unit's POWER socket, located on the rear panel. Connect the Mains power cord to the power transformer and to the AC mains.

NOTE

The color codes of the power cable are as follows:

Brown	Phase	~
Blue	Neutral	0
Yellow/Green	Ground	⏚

4. When power is connected, the unit will automatically enter the self-test phase. When it is in the self-test phase, the STATUS LED will be lit ON for about 10 seconds, and will then blink 3 times, indicating that the self-test operation has ended. Finally, the STATUS LED will blink continuously one blink per second, indicating that the unit is functioning properly.
5. Connect a PC to one of the LAN ports using an Ethernet cable and configure the basic parameters of the SU-ODU. Align the antenna of the ODU. For more information refer to the applicable sections of the relevant System Manual.
6. Use a web browser to configure the parameters of the Networking Gateway IDU. For details refer to Chapter 3.

7 If a printer is to be used, connect it to the USB port using a standard USB cable. To configure the Print Server on your computer(s), refer to Appendix A - Print Server.

8 Configure the network settings of the computers for proper operation with the Networking Gateway. The default IP address of the Networking Gateway LAN is 192.168.254.253, and the default subnet mask is 255.255.255.0.

9 To verify data connectivity, from the end-user's PC or from a portable PC connected to the unit, try to connect to the Internet.

10 Verify proper operation using the LED indicators (see Table 6).

3

Chapter 3 - Using the Web Configuration Server

In This Chapter:

3.1 Introduction

The Networking Gateway IDU can be configured using the following methods:

Â The Web Configuration Server

Â A .cfg-file loaded into the unit from the web configuration server or TFTP.

Â SNMP

This document describes the configuration using the Web Configuration Server.

3.2 Accessing the Web Configuration Server

Follow the steps below to access the Web Configuration Server:

1 Connect the unit to the AC mains.

2 Connect PC to LAN port 1.

NOTE

When connecting from WAN, make sure that a remote administrator is enabled (see section 3.7.6), and enter the WAN IP address specified in the *System Status* window (see section 3.4) using TCP port 88.

IMPORTANT

When managing the NG via bwaNMS (using the cut through option), the Remote Administrator Port must be set to 8080.

3 Open a web browser (Internet Explorer or Netscape Communicator).

NOTE

Be sure to disable the proxy on your Web browser or add the IP address of the product into the proxy exceptions.

4 Type http://192.168.254.253 in the Address (IE) or Location (Netscape) field and click **Enter**.

5 If the Web Configuration Server is password protected, you will be prompted to enter your password in order to login to the system (see section 3.3).

6 The Web Configuration Server main view appears on the screen.

3.3 Log in and Log out

After connection is established, the networking gateway web user interface appears. There are two entry levels: for general users and for system administrators. The menus and screens vary depending on entry level. The menus and parameters specified hereinafter, refer to both entry levels, unless otherwise specified.

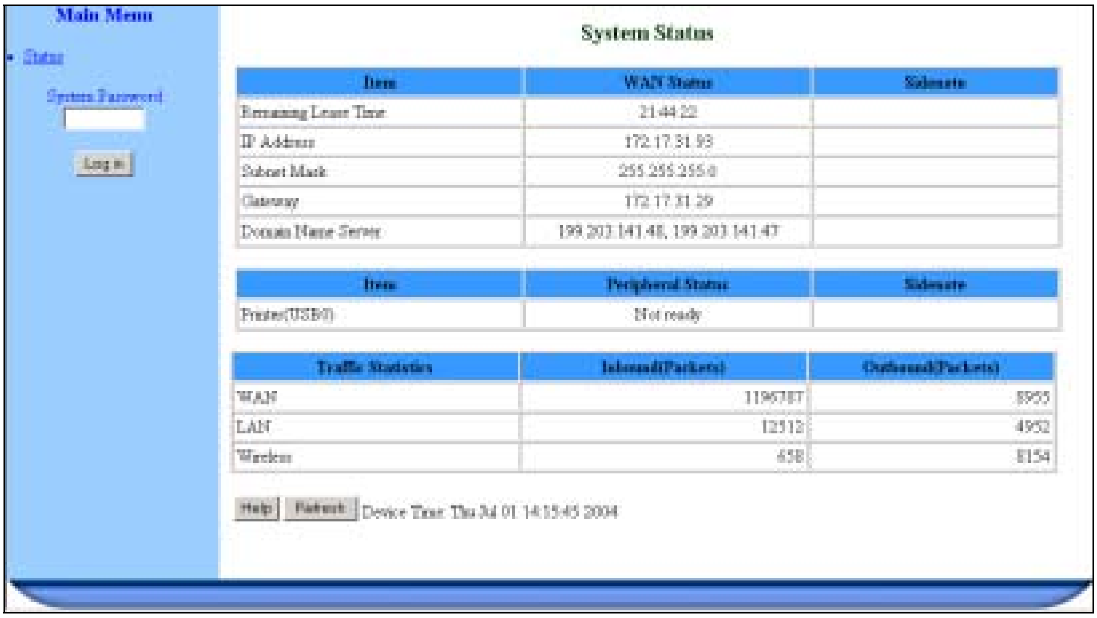
To log in, enter the system password in the **System Password** field and click the **Log in** button.

NOTE

The default passwords for the two access levels are:

Â For Administrators: **private**

Â For Users: **public**



System Status

Item	WAN Status	Sidenote
Remaining Lease Time	21:44:22	
IP Address	172.17.31.93	
Subnet Mask	255.255.255.0	
Gateway	172.17.31.29	
Domain Name Server	199.203.141.48, 199.203.141.47	

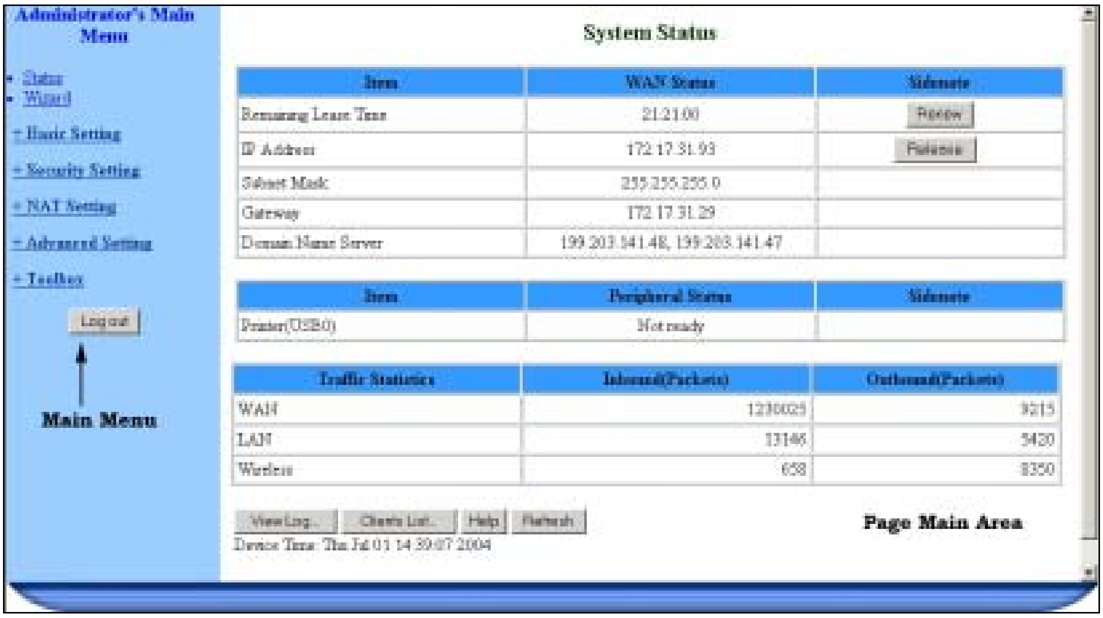
Item	Peripheral Status	Sidenote
Printer(USB0)	Not ready	

Traffic Statistics	Inbound(Packets)	Outbound(Packets)
WAN	1196787	8955
LAN	12512	4952
Wireless	658	8154

Device Time: Thu Jul 01 14:15:45 2004

Figure 3: Log In Window

Upon successful Log in, the *Networking Gateway Main Window* appears.



System Status

Item	WAN Status	Sidenote
Remaining Lease Time	21:21:00	Renew
IP Address	172.17.31.93	Release
Subnet Mask	255.255.255.0	
Gateway	172.17.31.29	
Domain Name Server	199.203.141.48, 199.203.141.47	

Item	Peripheral Status	Sidenote
Printer(USB0)	Not ready	

Traffic Statistics	Inbound(Packets)	Outbound(Packets)
WAN	1230025	9215
LAN	13146	5420
Wireless	658	8350

Device Time: Thu Jul 01 14:39:07 2004

Figure 4: Networking Gateway Main Window

3.3.1 The Main Menu

The Web Configuration Server view consists of a number of menu links (to the left). Clicking on each of them expands the menu node and displays the selected page with the applicable content (configurable parameters/options or status information) in the main area.

IMPORTANT

Many pages include a "Save" button. Click on the Save button before selecting another page/menu item, or before quitting the application. The Save functionality in many cases is per page. If you leave the page without clicking the Save button, all the changes in the page will be discarded.

Changes to most of the settings are applied only after restarting the unit (refer to section 3.10.5).

3.3.2 Control Buttons

A control button causes an immediate action. To activate a control button, click on it. Certain control buttons only appear in selected windows. Others are common to most windows.

NOTE

Some control buttons may be disabled for user entry level (***public*** password).

Â Save – Saves any changes made to the configuration. Most changes require rebooting the system for them to take effect.

Â Undo – Recovers the original settings.

Â Help – Displays a help screen for the specific window.

Â Refresh – Refreshes the displayed information.

Â Back – Reverts to a previous step/screen.

Â <<Previous – In windows that are divided into several pages, use the **<<Previous** button to jump to the previous page.

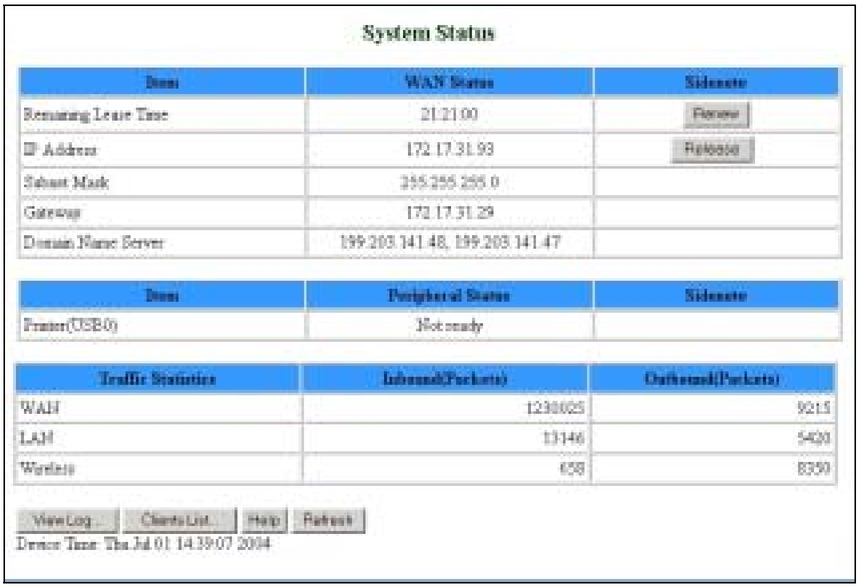
Â Next>> **-** In windows that are divided into several pages, use the **Next>>** button to jump to the next page.

Â Cancel – Clears unsaved changes to the configuration.

Â Reboot – Reboots the Networking Gateway.

3.4 Status

The Status window appears in the main window upon successful log in. The window can be accessed at any time by clicking on the Status menu on the menu list.



System Status

Item	WAN Status	Sidenote
Remaining Lease Time	21:21:00	Renew
IP Address	172.17.31.93	Release
Subnet Mask	255.255.255.0	
Gateway	172.17.31.29	
Domain Name Server	199.203.141.48, 199.203.141.47	

Item	Peripheral Status	Sidenote
Printer(USB0)	Not ready	

Traffic Statistics	Inbound(Packets)	Outbound(Packets)
WAN	1230025	9215
LAN	13146	5420
Wireless	658	8350

Device Time: Thu Jul 01 14:39:07 2004

Figure 5: System Status

The *Status* window provides information for observing the product's working status, as follows:

Table 8: Status Window Parameters

Parameter	Description
Remaining Lease Time	A counter displaying the remaining time (in hh:mm:ss) in which unit will request a new IP. When the lease time expires, a new IP address will be automatically allocated, or the lease will be automatically renewed, depending on the settings (see sections 3.6.1.2 and 3.6.1.3. This field is relevant only for Dynamic IP Address mode and will not appear in any of the other modes. Â Renew (Administrator only) – In Dynamic IP Address mode, click to reset the Lease Time. The gateway will request an IP address from the DHCP server. Â In Static IP Address, PPPoE and PPTP modes, the WAN type is specified in the sidenote (Static IP, PPPoE, or PPTP, respectively).

Parameter	**Description**
IP Address	The WAN IP address. Â Release (Administrator only) – In Dynamic IP Address mode only, Click to release the WAN IP address.
Subnet Mask	The Subnet mask of the device. (The default is 255.255.255.0)
Gateway	The default Gateway IP address.
Domain Name Server	The DNS Server IP address(es).
Connection Time (PPPoE and PPTP modes only)	Connect/ Disconnect – When in PPPoE or PPTP mode, click **Connect** to initiate a session, or **Disconnect** to terminate a session.
Peripheral Status	The USB Printer status: Â Not ready - no printer is available Â Off-line or No Paper – the printer is off-line or the paper tray is empty Â Printing – the printer is currently printing Â Ready - a printer is connected and ready to print. Â Device error – a general error occurred.
Traffic Statistics	Enables to monitor inbound and outbound packets for WAN, LAN and wireless beginning from last reset.

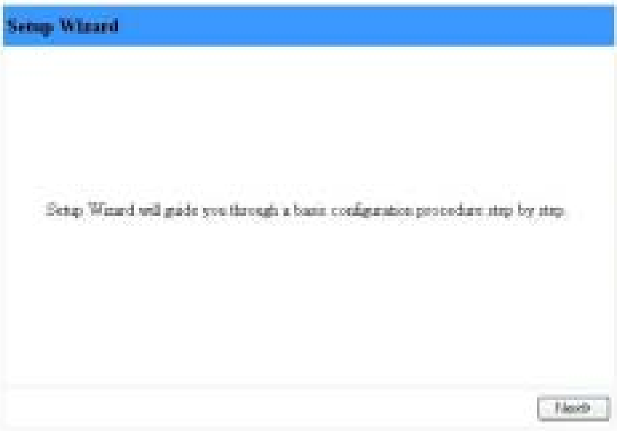
In addition, the *Status* window includes the following buttons:

Â View Log – opens the log file for viewing. See section 3.10.1.

Â Clients List – opens the list of DHCP assigned clients. See section 3.6.2.1.

3.5 Wizard (Administrator only)

The Setup Wizard will guide you through the basic configuration procedure (recommended for most users).



Setup Wizard

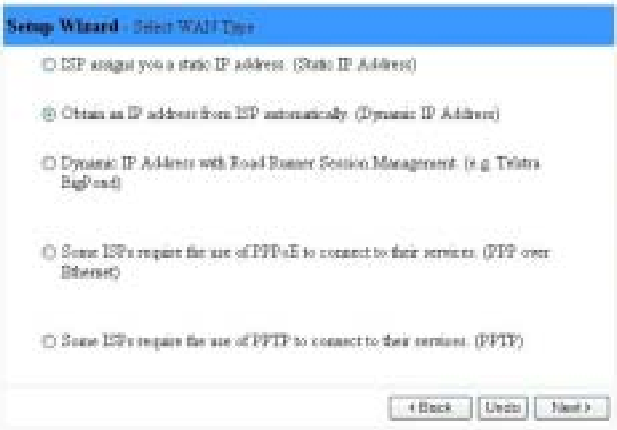
Setup Wizard will guide you through a basic configuration procedure step by step.

Figure 6: Setup Wizard

1 Click on **Next**. The *Select WAN Type* window appears.

NOTE

You can click **Back** at any time to return to previous screens and change your settings.



Setup Wizard - Select WAN Type

○ ISP assigns you a static IP address. (Static IP Address)

● Obtain an IP address from ISP automatically. (Dynamic IP Address)

○ Dynamic IP Address with Road Runner Session Management. (e.g. Telstra BigPond)

○ Some ISPs require the use of PPPoE to connect to their services. (PPP over Ethernet)

○ Some ISPs require the use of PPTP to connect to their services. (PPTP)

Figure 7: Setup Wizard - Select WAN Type

2 Select the WAN Type from the list:

Ï Static IP Address – a static IP Address provided by the ISP

Ï Dynamic IP Address – an IP Address automatically obtained from the ISP (default)

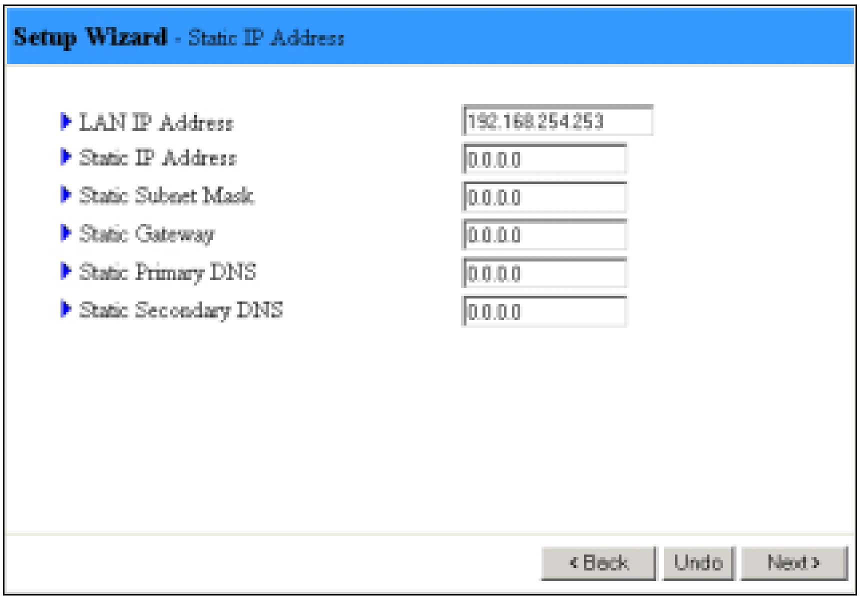
Ï Dynamic IP Address with Road Runner Session Management (e.g. Telstra, BigPond)

Ï PPP over Ethernet – some ISPs require the use of PPPoE to connect to their services

Ï PPTP – Some ISPs require the use of PPTP to connect to their services.

3 Click **Next**. For each WAN type selected, a different WAN Type-specific window appears:

Ï Static IP Address



Setup Wizard - Static IP Address

LAN IP Address	192.168.254.253
Static IP Address	0.0.0.0
Static Subnet Mask	0.0.0.0
Static Gateway	0.0.0.0
Static Primary DNS	0.0.0.0
Static Secondary DNS	0.0.0.0

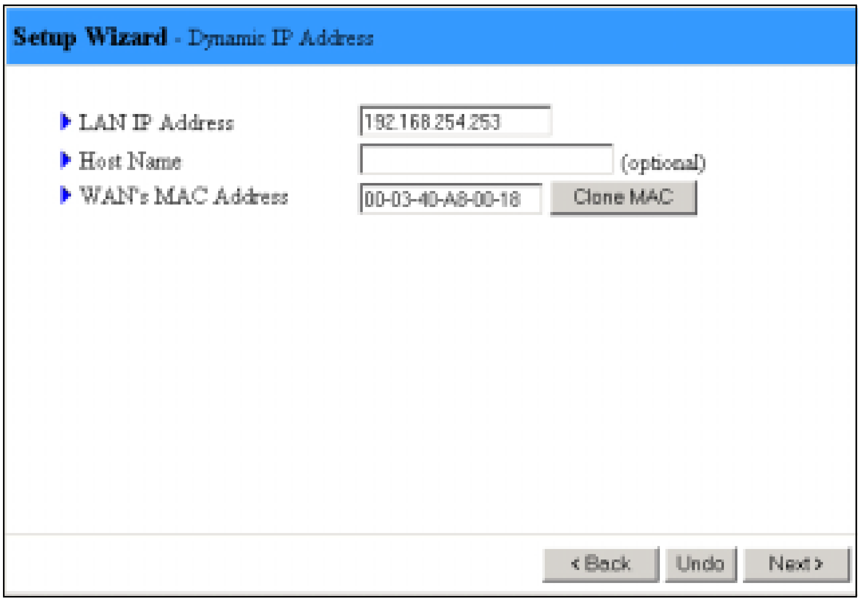
Figure 8: Setup Wizard – WAN Type - Static IP Address

Set the following parameters provided by your ISP:

Table 9: Setup Wizard – Static IP Address Parameters

Parameter	Description
LAN IP Address	Sets the local IP address of the device.
Static IP Address	The IP address of the WAN port. The default is 0.0.0.0.
Static Subnet Mask	The subnet mask of the WAN port. The default is 0.0.0.0.
Static Gateway	The Default Gateway IP address of the unit. The default is 0.0.0.0.
Static Primary DNS	The IP address of the primary Domain Name Server. The default is 0.0.0.0.
Static Secondary DNS	The IP address of the secondary Domain Name Server. The default is 0.0.0.0.

Ï Dynamic IP Address



Setup Wizard - Dynamic IP Address

LAN IP Address	192.168.254.253
Host Name	(optional)
WAN's MAC Address	00-03-40-A8-00-18

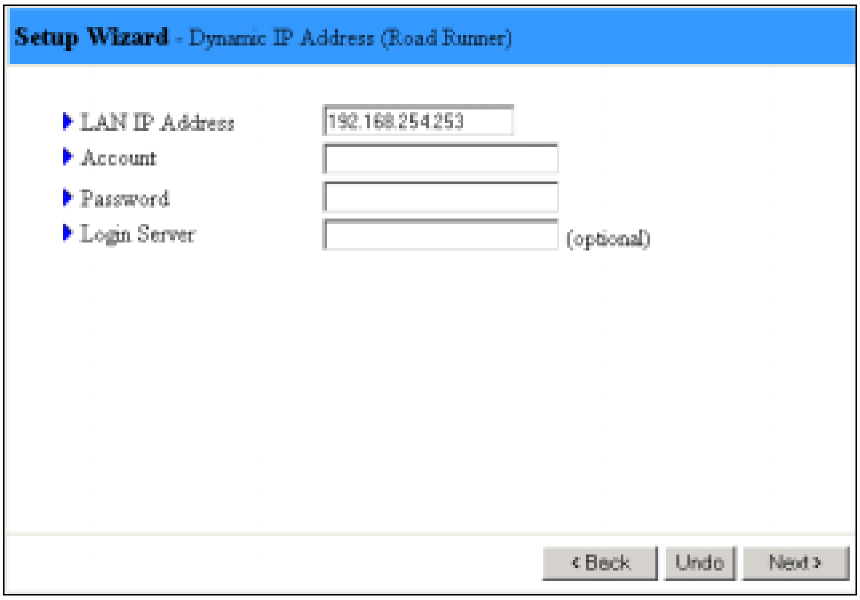
Figure 9: Setup Wizard - Dynamic IP Address

Set the following parameters:

Table 10: Setup Wizard – Dynamic IP Address Parameters

Parameter	Description
LAN IP Address	The local IP address of the device. The default IP address is 192.168.254.253. To change the IP address enter a new value.
Host Name: Optional	Some ISPs require a host name, for example, Home. A string of maximum 39 characters. The default is an empty field.
WAN's MAC Address	The gateway's pre-configured MAC Address. Â Clone MAC - Click to replace the Gateway's WAN MAC Address with the PC's MAC Address. Â Restore MAC - When Clone MAC is activated, the button changes to Restore MAC, to enable to restore the unit's default MAC Address.

Ï Dynamic IP Address with Road Runner Session Management



Setup Wizard - Dynamic IP Address (Road Runner)

- LAN IP Address: 192.168.254.253
- Account:
- Password:
- Login Server: (optional)

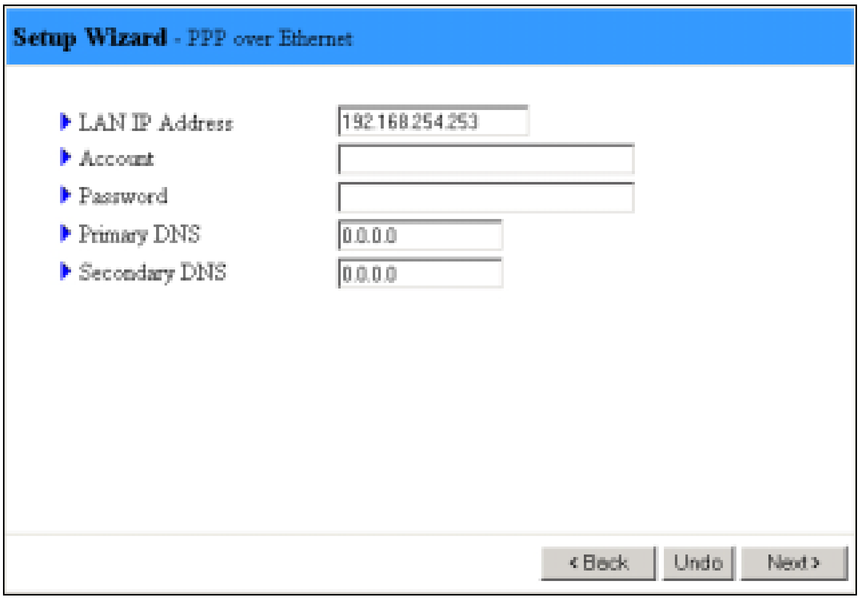
Figure 10: Setup Wizard - Dynamic IP Address with Road Runner Session Management

Set the following parameters:

Table 11: Setup Wizard – Dynamic IP Address with Road Runner Session Management Parameters

Parameter	Description
LAN IP Address	The local IP address of the device. The default IP address is 192.168.254.253. To change the IP address enter a new value.
Account	The account provided by the service provider. If you do not want to change the account, leave empty. At initial entry, you are required to enter an account. A string of up to 53 printable characters. The default is an empty field.
Password	The password provided by the service provider. If you do not want to change the password, leave empty. At initial entry, you are required to enter a password. A string of up to 53 printable characters.
Login Server	The Login Server (optional). Leave empty if you want the default server.

Ï PPP over Ethernet



Setup Wizard - PPP over Ethernet

LAN IP Address	192.168.254.253
Account	
Password	
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

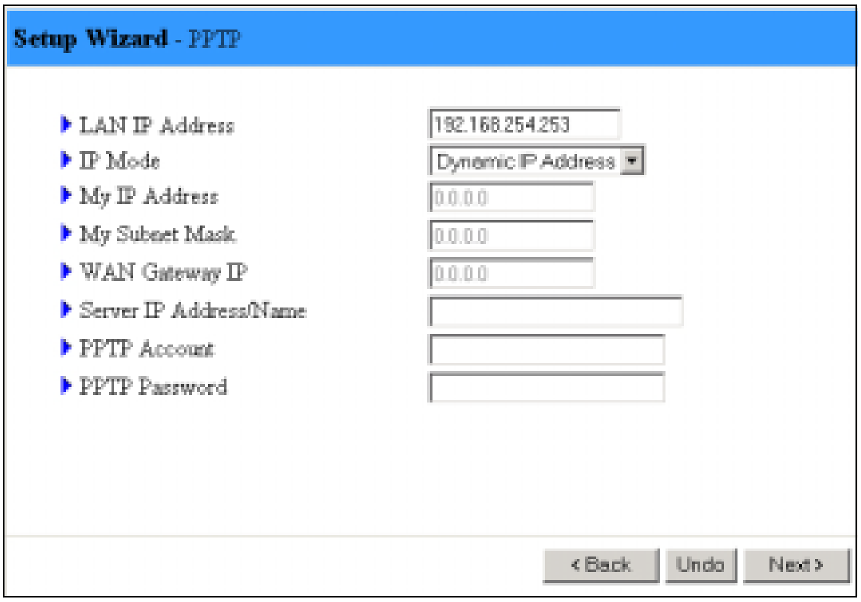
Figure 11: Setup Wizard – PPP over Ethernet

Set the following parameters:

Table 12: Setup Wizard – PPPoE Parameters

Parameter	Description
LAN IP Address	The local IP address of the device. The default IP address is 192.168.254.253. To change the IP address enter a new value.
Account	The account provided by the service provider. A string of up to 53 printable characters. The default is an empty field.
Password	The password provided by the service provider. If you do not want to change the password, leave empty. At initial entry, you are required to enter a password. A string of up to 53 printable characters.
Primary DNS	The DNS provided by your ISP. To use a specific DNS, enter a specific address. Leave the default 0.0.0.0 setting to automatically assign the parameter.
Secondary DNS	The backup DNS provided by the service provider. (optional)

Ï PPTP



Setup Wizard - PPTP

LAN IP Address: 192.168.254.253
IP Mode: Dynamic IP Address
My IP Address: 0.0.0.0
My Subnet Mask: 0.0.0.0
WAN Gateway IP: 0.0.0.0
Server IP Address/Name:
PPTP Account:
PPTP Password:

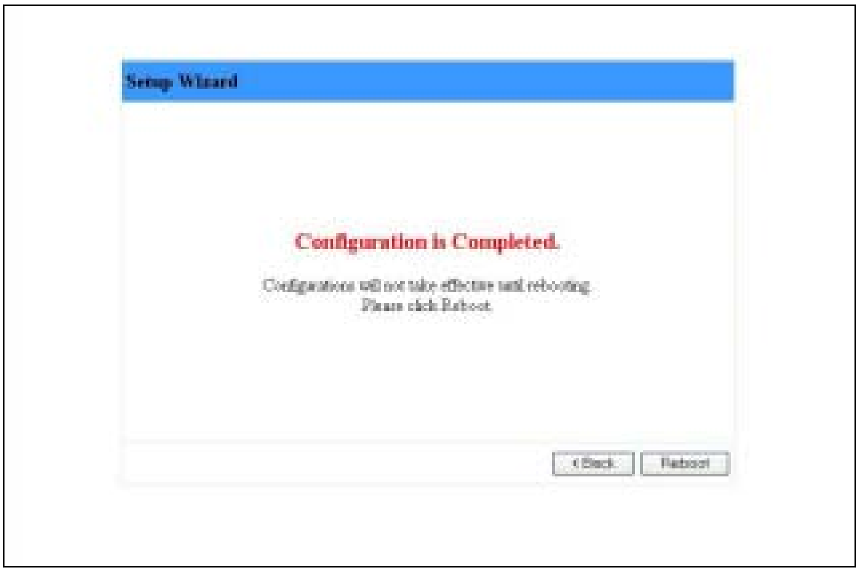
Figure 12: Setup Wizard – PPTP

Set the following parameters:

Table 13: Setup Wizard – PPTP Parameters

Parameter	Description
LAN IP Address	The local IP address of the device. The default IP address is 192.168.254.253. . To change the IP address enter a new value.
IP Mode	select one of the following options: Â Dynamic IP Address (this is the default setting) Â Static IP Address
My IP Address	The private IP address assigned by the service provider after connection. When in Static Mode, the IP address must be configured manually.
My Subnet Mask	The private subnet mask assigned by the service provider after connection. When in Static Mode, the subnet mask must be configured manually.
WAN Gateway IP	The WAN Gateway IP address after connection. When in Static Mode, the IP address must be configured manually.
Server IP Address/Name	The IP address/Name of the PPTP server.
PPTP Account	The user account assigned by the service provider. A string of up to 53 characters
PPTP Password	The password assigned by the service provider. If you do not want to change the password, leave this field empty. At initial entry, you are required to enter a password. A string of up to 53 characters

4 After setting the appropriate parameters, the following window appears:



Configuration is Completed.

Configurations will not take effective until rebooting.
Please click Reboot.

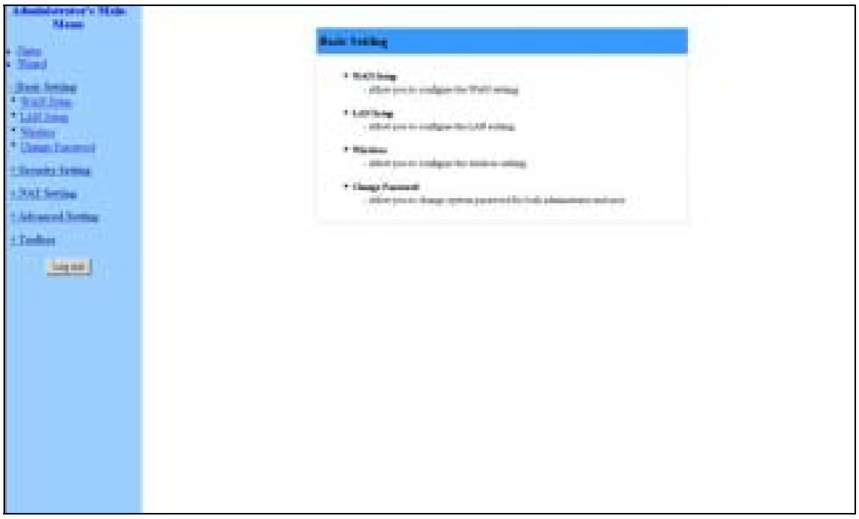
Figure 13: Setup Wizard - Configuration Completed

5 The configurations will take effect only after rebooting your computer. Click on **Reboot** to restart your computer.

For more advance configurations, see details on the specific windows, below.

3.6 Basic Setting

The *Basic Setting* window allows to configure the settings for WAN, LAN, and Wireless and to change the password.



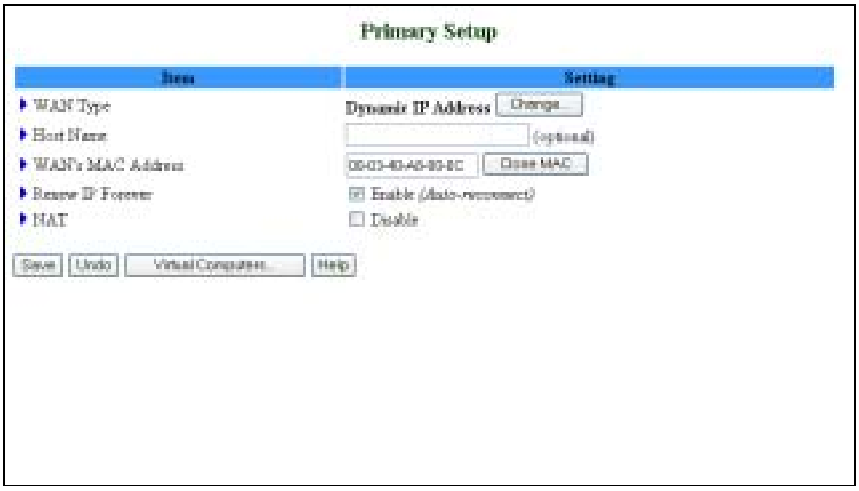
Basic Setting

- WAN Setup
  - allow you to configure the WAN setting
- LAN Setup
  - allow you to configure the LAN setting
- Wireless
  - allow you to configure the wireless setting
- Change Password
  - allow you to change system password for both administrator and user

Figure 14: Basic Setting

3.6.1 WAN Setup

Click on *WAN Setup* from the *Basic Setting* menu on the menu list. The *Primary Setup* window appears. The parameters displayed may vary depending on the WAN Type selected. The default WAN Type is Dynamic IP Address.


Primary Setup

Item	Setting
WAN Type	Dynamic IP Address [Change...]
Host Name	(optional)
WAN's MAC Address	00-03-40-A8-80-8C [Clone MAC]
Renew IP Forever	☒ Enable (Auto-reconnect)
NAT	□ Disable

Figure 15: WAN Setup/Primary Setup

NOTE

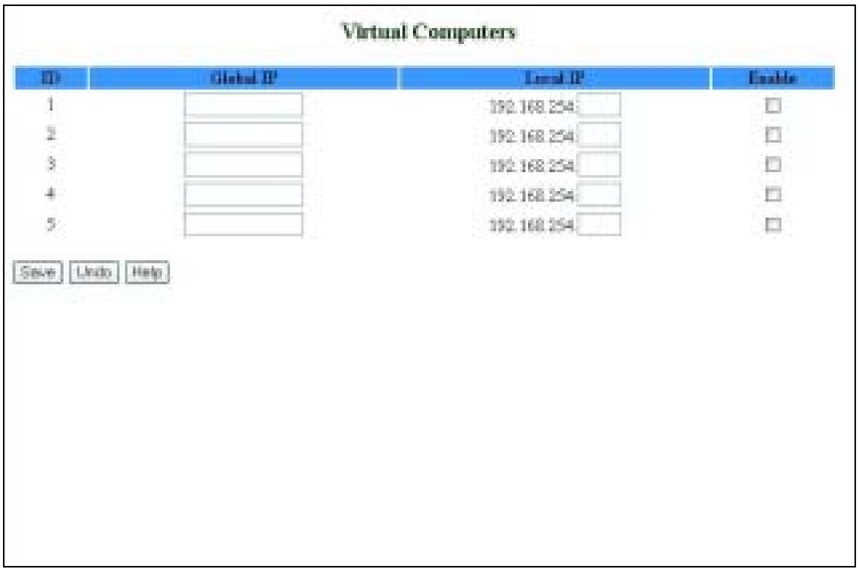
The WAN setup window is read only for user level entry.

From the *WAN Setup* window you can:

Â Set the WAN type – allows to select the WAN connection type of your ISP.

Â NAT – Enable/Disable - When disabled, the gateway functions as a regular router as opposed to a NAT router. This option is available in the *Primary Setup* window for all WAN types.

Â Set Virtual Computers (Administrators only) – Enabled when using NAT. In addition to the primary WAN address, enables to set up one-to-one mapping of up to five global IP address and local IP address (see Figure 16 below).



Virtual Computers

ID	Global IP	Local IP	Enable
1		192.168.254.	□
2		192.168.254.	□
3		192.168.254.	□
4		192.168.254.	□
5		192.168.254.	□

Figure 16: Virtual Computers

The Virtual Computers window includes the following parameters:

Table 14: Virtual Computers Parameters

Parameter	Description
Global IP	Enter the global IP address assigned by the service provider.
Local IP	Enter the local IP address of your LAN PC corresponding to the global IP address.
Enable	Check/Uncheck this item to enable/disable the Virtual Computer feature.

NOTE

Â The Reboot button is not available at first entry to the Primary Setup window and appears only after saving your changes.

Â For user entry level (***public*** password), the parameter fields in all WAN type screens are disabled (for display only).

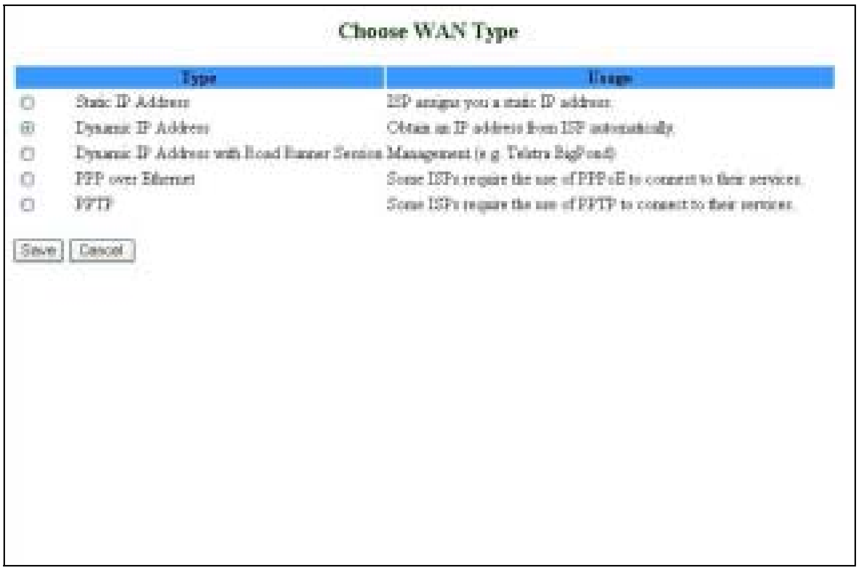
IMPORTANT

Changes to the *Primary Setup* window will take effect only after rebooting the system.

The default WAN type is **Dynamic IP Address**. However, you can change the WAN type as follows:

To select a different WAN type:

1 Click **Change**. The Choose *WAN Type* window opens.



Choose WAN Type

	Type	Usage
○	Static IP Address	ISP assigns you a static IP address.
●	Dynamic IP Address	Obtain an IP address from ISP automatically.
○	Dynamic IP Address with Road Runner Session Management (e.g. Telstra BigPond)	
○	PPP over Ethernet	Some ISPs require the use of PPPoE to connect to their services.
○	PPTP	Some ISPs require the use of PPTP to connect to their services.

Figure 17: Choose WAN Type

2 Select one of the following types:

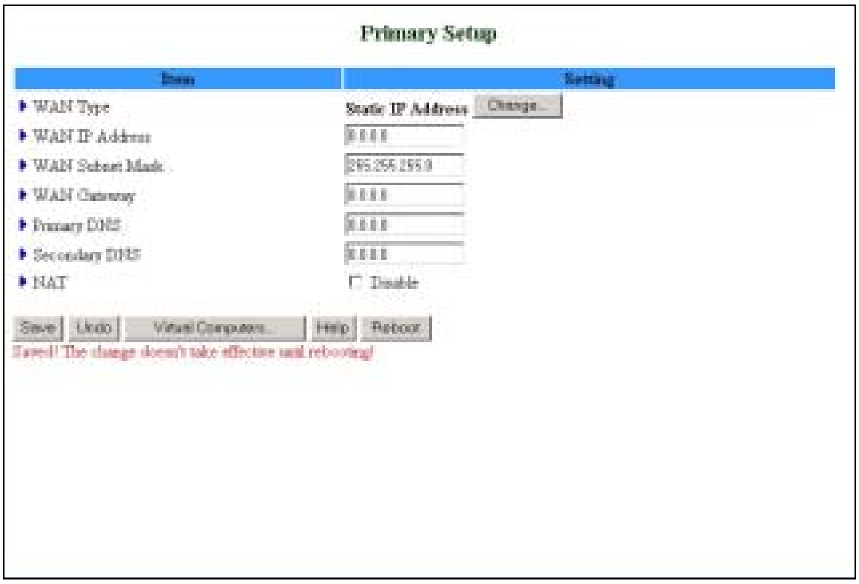
Ï Static IP Address: The ISP provides you with a static IP address. See section 3.6.1.1.

Ï Dynamic IP Address: Automatically obtain an IP address from the ISP. See section 3.6.1.2. This is the default setting.

- Ï Dynamic IP Address with Road Runner Session Management (e.g. Telstra BigPond). See section 3.6.1.3.
- Ï PPP over Ethernet: Some ISPs require the use of PPPoE to connect to their services. See section 3.6.1.4.
- Ï PPTP: Some ISPs require the use of PPTP to connect to their services. See section 3.6.1.5.

For each WAN type selected, a different *Primary Setup* window appears, as follows. You can change the WAN type by clicking on **Change** and selecting a different WAN type.

3.6.1.1 Static IP Address



Primary Setup

Item	Setting
WAN Type	Static IP Address
WAN IP Address	0.0.0.0
WAN Subnet Mask	255.255.255.0
WAN Gateway	0.0.0.0
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
NAT	□ Disable

Saved! The change doesn't take effective until rebooting!

Figure 18: Primary Setup - Static IP Address

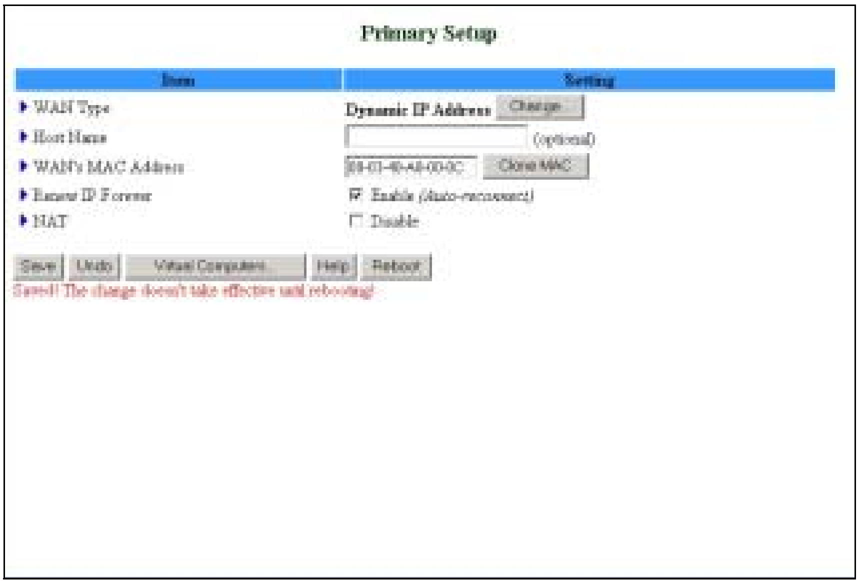
The *Setup* page for Static IP Address includes the following parameters provided by the service provider:

Table 15: Static IP Address Parameters

Parameter	Description
WAN IP Address	The IP address of the WAN port. The default is 0.0.0.0.
WAN Subnet Mask	The IP subnet mask of the WAN port. The default is 255.255.255.0
WAN Gateway	The Default Gateway IP address of the unit.

Parameter	**Description**
	The default is 0.0.0.0.
Primary DNS	The IP address of the primary Domain Name Server. The default is 0.0.0.0.
Secondary DNS	The IP address of the secondary Domain Name Server. The default is 0.0.0.0.
NAT	Enable/Disable. When disabled, the gateway functions as a regular router as opposed to a NAT router. This option is available in the Primary Setup window for all WAN types. The default is: Enable

3.6.1.2 Dynamic IP Address



Primary Setup

Item	Setting
WAN Type	Dynamic IP Address
Host Name	(optional)
WAN's MAC Address	00-01-40-A8-00-0C
Renew IP Forever	☑ Enable (Auto-reconnect)
NAT	□ Disable

Saved! The change doesn't take effective until rebooting!

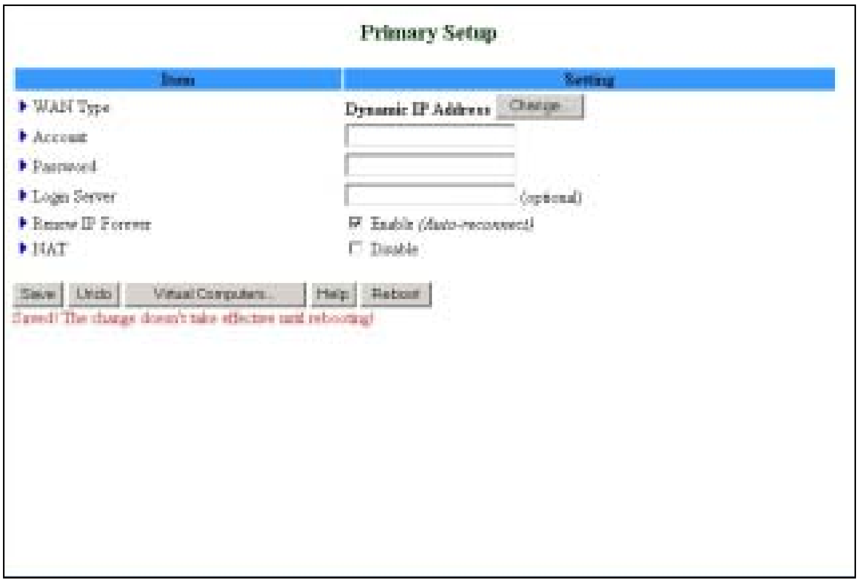
Figure 19: Primary Setup - Dynamic IP Address

The *Setup* page for Dynamic IP Address includes the following parameters:

Table 16: Dynamic IP Address Parameters

Parameter	Description
Host Name	Optional - Some ISPs require a host name, for example, Home. A string of maximum 39 characters.
WAN's MAC Address	The gateway's pre-configured MAC Address. Â Clone MAC - Click to replace the Gateway's WAN MAC Address with the PC's MAC Address. Â Restore MAC - When Clone MAC is activated, the button changes to Restore MAC, to enable to restore the unit's pre-configured MAC Address.
Renew IP Forever	When enabled, this feature will automatically renew your IP address when the lease time expires, even if the system is idle.
NAT	Enable/Disable - When disabled, the gateway functions as a regular router as opposed to a NAT router.

3.6.1.3 Dynamic IP Address with Road Runner Session Management



Primary Setup

Item	Setting
WAN Type	Dynamic IP Address
Account	
Password	
Login Server	(optional)
Renew IP Forever	☑ Enable (Auto-reconnect)
NAT	□ Disable

Saved! The change doesn't take effect until rebooting!

Figure 20: Primary Setup - Dynamic IP Address with Road Runner Session Management

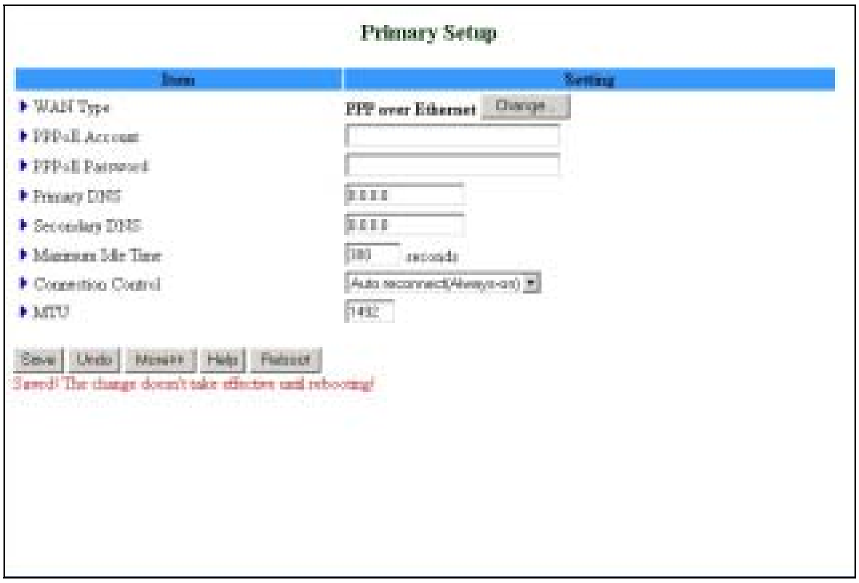
The Setup page for Dynamic IP Address with Road Runner Session Management provides authentication using dedicated DHCP server and includes the following parameters:

Table 17: Dynamic IP Address with Road Runner Session Management Parameters

Parameter	Description
Account	The account provided by your ISP A string of maximum 53 characters.
Password	The password provided by your ISP. If you do not want to change the password, leave empty. A string of maximum 53 characters.
Login Server	The Login Server (optional). Leave empty if you want the default server. A string of maximum 31 characters.
Renew IP Forever	Enable/Disable – when enabled, your IP address will automatically be renewed when the lease time expires, even if the system is idle.
NAT	Enable/Disable - When disabled, the gateway functions as a regular router as opposed to a NAT router.

3.6.1.4 PPP over Ethernet

Some ISPs require the use of PPPoE to connect to their services. If this is the case, click **Change** to select PPPoE as your WAN type. The *Primary Setup* window display changes to reflect the parameters for PPPoE.



Primary Setup

Item	Setting
WAN Type	PPP over Ethernet Change
PPPoE Account	
PPPoE Password	
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Maximum Idle Time	180 seconds
Connection Control	Auto reconnect(Always-on)
MTU	1492

Saved! The change doesn't take effective until rebooting!

Figure 21: Primary Setup - PPPoE

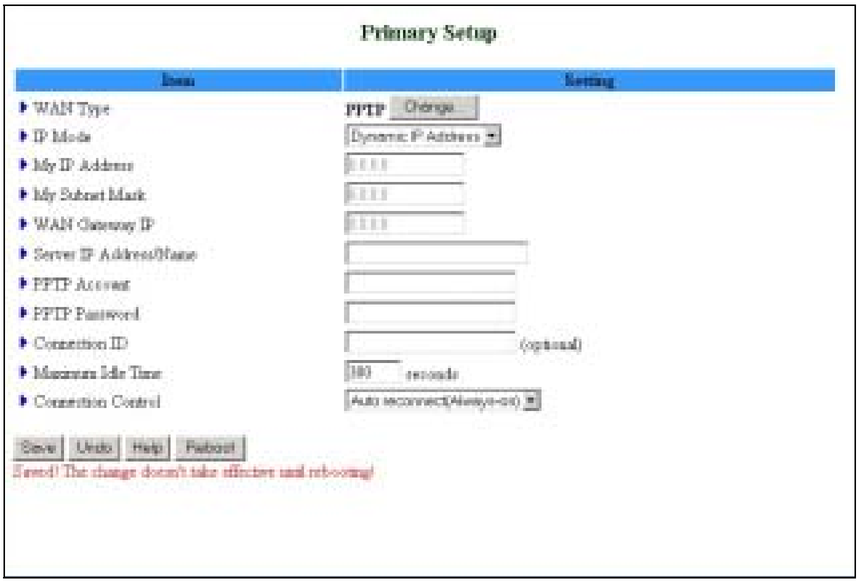
The Setup page for PPPoE includes the following parameters:

Table 18: PPP over Ethernet Parameters

Parameter	Description
PPPoE Account	The account assigned to you by your ISP.
PPPoE Password	The password assigned to you by your ISP. This field always appears blank. If you don't want to change the password, leave it empty.
Primary DNS	The DNS provided by your ISP. To use a specific DNS, enter a specific address. Leave the default 0.0.0.0 setting to automatically assign the parameter.
Secondary DNS	The backup DNS provided by your ISP. (optional)
Maximum Idle Time	The amount of time of inactivity before disconnecting your PPPoE session. To disable this feature, set this parameter to 0 seconds, or enable Auto-reconnect. The Maximum Idle Time is applicable only when Connection Control is set to Connect-on-demand or to Manually.
Connection Control	Authentication for IP allocation. Select one of the following options: Â Connect-on-demand – An IP address is automatically allocated whenever the user attempts to make a connection. Â Auto reconnect(Always-on) – The system automatically connects to the ISP after restart or after connection is dropped. Â Manually – The user manually performs the connection.
Maximum Transmission Unit (MTU)	Most ISPs provide an MTU value to users. The maximum MTU value allowed is 1492 bytes.
More >>	Click to display the following parameters: Â PPPoE Service Name (optional) - Directs to a PPPoE server. Â Assigned IP Address (optional) – The fixed IP assigned by the ISP.

3.6.1.5 PPTP

Some ISPs require the use of PPTP to connect to their services.



Primary Setup

Item	Setting
WAN Type	PPTP Change
IP Mode	Dynamic IP Address
My IP Address	[illegible]
My Subnet Mask	[illegible]
WAN Gateway IP	[illegible]
Server IP Address/Name	
PPTP Account	
PPTP Password	
Connection ID	(optional)
Maximum Idle Time	180 seconds
Connection Control	Auto reconnect(Always-on)

Saved! The change doesn't take effective until rebooting!

Figure 22: Primary Setup - PPTP

The *Setup* page for PPTP includes the following parameters:

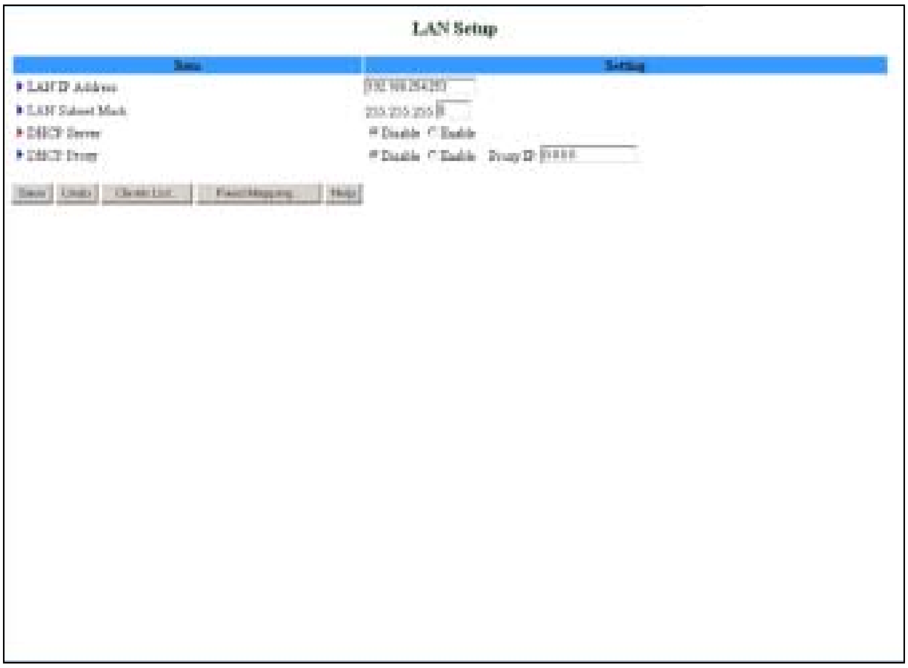
Table 19: PPTP Parameters

Parameter	Description
IP Mode	Select one of the following options: Â Dynamic IP Address (this is the default setting) Â Static IP Address
My IP Address	The private IP address assigned by your ISP. This parameter is enabled only for Static IP Address mode.
My Subnet Mask	The private subnet mask assigned by your ISP. This parameter is enabled only for Static IP Address mode.
WAN Gateway IP	The WAN Gateway IP address. This parameter is enabled only for Static IP Address mode.
Address/Name	The IP address/Name of the PPTP server.
PPTP Account	The user account assigned by your ISP. A string of maximum 53 characters.
Connection ID	Enter the connection ID if your ISP requires it (optional).

Parameter	Description
Maximum Idle Time	The amount of time of inactivity before disconnecting your PPTP session. To disable this feature, set this parameter to 0 seconds, or enable Auto-reconnect.
Connection Control	Authentication for IP allocation. Select one of the following options: Â Connect-on-demand – An IP address is automatically allocated whenever the user attempts to make a connection. Â Auto reconnect(Always-on) – The system automatically connects to the ISP after restart or after connection is dropped. Â Manually – The user manually performs the connection.

3.6.2 LAN Setup

Select *Basic Setting* > *LAN Setup* submenu on the menu list. The *LAN Setup* window opens.



LAN Setup

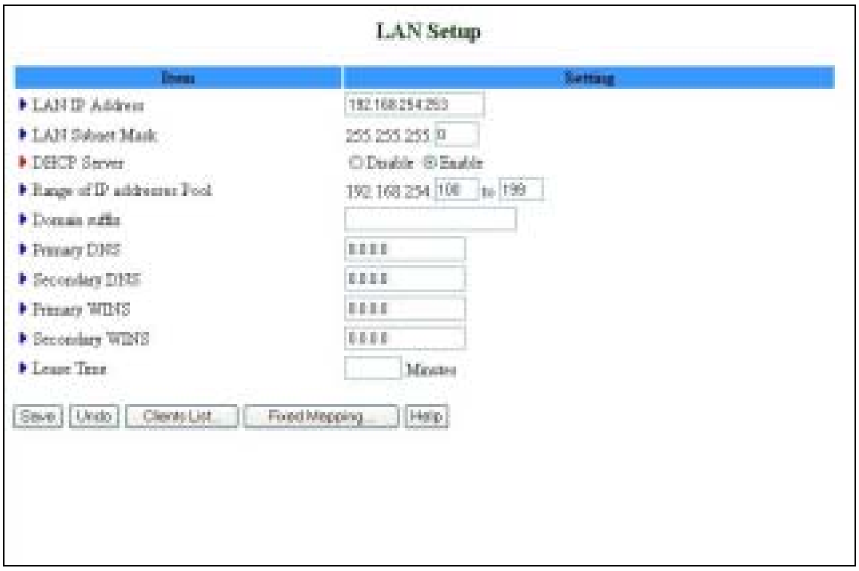
Item	Setting
LAN IP Address	192.168.254.253
LAN Subnet Mask	255.255.255.0
DHCP Server	● Disable ○ Enable
DHCP Proxy	● Disable ○ Enable Proxy IP: 0.0.0.0

Figure 23: LAN Setup

The LAN Setup page includes the following parameters:

Table 20: LAN Setup Parameters

Parameter	Description
LAN IP Address	Sets the local IP address of the device. The users on your network must use this LAN IP address as their default gateway. You can change it as necessary.
LAN Subnet Mask	Sets the subnet mask to the LAN IP address.
DHCP Server	Enable/Disable to turn off this service. When enabled, the LAN Setup window display changes (indicated by the red icon), and the following parameters are displayed (see Figure 24): Â Range of IP addresses Pool – Specify the starting and ending address for DHCP clients. The IP addresses are allocated from this pool according to calculations based on the client's MAC address. Â Domain suffix – Specify the domain suffix for DHCP clients. Â Primary DNS – Specify the primary DNS for DHCP clients. Â Secondary DNS – Specify the secondary DNS for DHCP clients. Â Primary WINS – Specify the primary WINS address for DHCP clients. Â Secondary WINS – Specify the secondary WINS address for DHCP clients. Â Lease Time – The time set (in minutes) for IP allocation.
DHCP Proxy	This parameter is available only when DHCP Server is disabled.



LAN Setup

Item	Setting
LAN IP Address	192.168.254.253
LAN Subnet Mask	255.255.255. 0
DHCP Server	○ Disable ● Enable
Range of IP addresses Pool	192.168.254. 100 to 199
Domain suffix	
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Primary WINS	0.0.0.0
Secondary WINS	0.0.0.0
Lease Time	Minutes

Figure 24: LAN Setup - DHCP Server Enabled

The LAN PC receives a DHCP IP address from the Networking Gateway. To receive the DHCP IP address from the DHCP server, perform the following procedure:

3 Set the **DHCP Server** parameter to **Disable**.

4 Set the **DHCP Proxy** parameter to **Enable**.

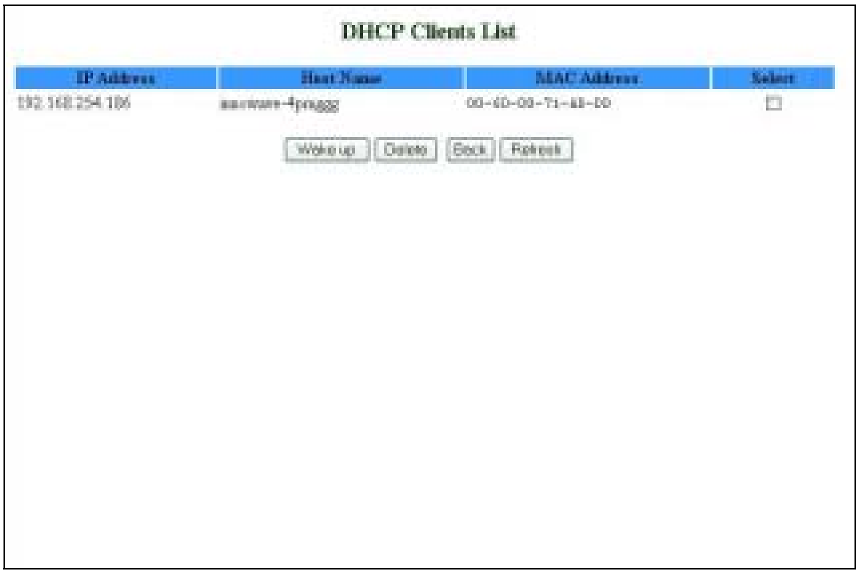
5 In the **Proxy IP** field, enter the IP of the DHCP server.

In addition, the LAN Setup window includes the following control buttons:

Â Clients List – Opens a list of the current mapping of the IP and MAC address for each DHCP client (see section 3.6.2.1)

Â Fixed Mapping – Opens the *MAC Address Control* window for assigning a specific IP address to the specified MAC address for DHCP clients (see MAC Address Control on page 52 for further details).

3.6.2.1 DHCP Clients List



DHCP Clients List

IP Address	Host Name	MAC Address	Select
192.168.254.106	[illegible]-4pnggg	00-60-00-71-[illegible]-D0	□

Figure 25: DHCP Clients List

The *DHCP Clients List* displays the following parameters for each DHCP client:

Table 21: DHCP Clients List Parameters

Parameter	Description
IP Address	The IP address of the DHCP client.
Host Name	The host name of the DHCP client.
MAC Address	The MAC address of the DHCP client.

From the *DHCP Clients List* window you can do the following for the selected clients:

Â Wake up – Sends Ethernet packets to turn on the PC, relevant hardware and configuration is required on NIC and PC

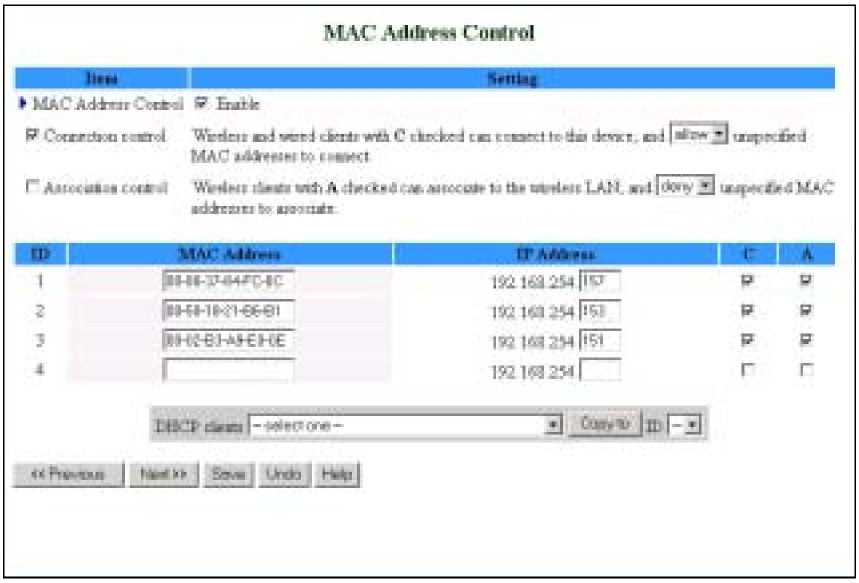
Â Delete – Delete the selected clients from the list.

3.6.2.2 Fixed Mapping

Opens the *MAC Address Control* window. MAC Address Control allows to assign different access rights for different users and to assign a fixed IP address to a specific MAC address.

NOTE

All the settings in this page will take effect only when MAC Address Control is set to "Enable".



MAC Address Control

Item	Setting
MAC Address Control	☑ Enable
☑ Connection control	Wireless and wired clients with C checked can connect to this device, and [allow] unspecified MAC addresses to connect.
□ Association control	Wireless clients with A checked can associate to the wireless LAN, and [deny] unspecified MAC addresses to associate.

ID	MAC Address	IP Address	C	A
1	00-08-37-84-FC-8C	192.168.254.157	☑	☑
2	00-50-18-21-86-B1	192.168.254.153	☑	☑
3	00-02-B3-A9-E3-0E	192.168.254.151	☑	☑
4		192.168.254.	□	□

Figure 26: MAC Address Control

The *MAC Address Control* window includes the following parameters:

Table 22: DHCP Clients List Parameters

Parameter	Description
MAC Address Control	Check "Enable" to enable the MAC Address Control feature.
Connection control	Check the "Connection control" check box to enable controlling which wired and wireless clients can connect to this device. If a client is denied the connection to this device, he will not be able to access the Internet either. Select **allow**/**deny** to allow or deny clients whose MAC addresses are not in the "Control table" (see below) to connect to this device. ("deny" is the default setting.) A wired client who is allowed to connect to the device has full access to the Internet and to network resources. When denied the connection to the device, he can communicate with other clients on the wired LAN, but cannot connect to the Internet, use the Print Server function, communicate with

Parameter	Description
	clients on the wireless LAN, or use the Web configuration.
Association control	"Association" refers to the exchanging of information between wireless clients and the device to establish a link between them. A wireless client is able to transmit and receive data to the device only after successful association. Check "Association control" check box to control which wireless clients can associate to the wireless LAN. If a client is denied the association to the wireless LAN, he will not be able to send or receive any data via this device. Select **allow**/**deny** to allow or deny clients whose MAC addresses are not in the "Control table" to associate to the wireless LAN. A wireless client who is allowed both to associate to the wireless LAN and to connect to the device has full access to the Internet and to network resources. When allowed to associate to the wireless LAN, but denied to connect to the device, he can communicate with other clients on the LAN (wired and wireless), but cannot connect to the Internet, use the Print Server function, or use the Web configuration. When denied to associate to the wireless LAN, the client cannot communicate with other clients on the LAN (wired or wireless), connect to the internet, use the Print Server function, or use the Web configuration. NOTE: Association control does not affect wired clients.
Control Table: Each row in the control table indicates the MAC address and the mapped IP address of a single client.	
MAC Address	The MAC address of a specific client.
IP Address	The expected IP address of the corresponding client. Leave empty if you do not want to specify an IP address for the corresponding client.
C	When "**Connection control**" is checked, checking "**C**" will allow/deny (depending on the connection control setting) the corresponding client to connect to this device.
A	When "**Association control**" is checked, checking "**A**" will allow/deny (depending on the association control setting) the corresponding client to associate to the wireless LAN.

To enter the MAC address:

Use the DHCP clients combo box.

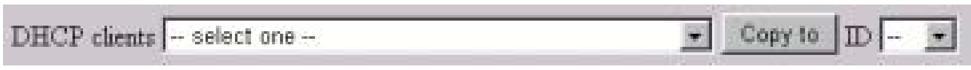


Figure 27: DHCP Clients Combo Box

1. Select a specific client in the "DHCP clients" Combo box and click on **Copy to** to copy the MAC address of the selected client to the selected ID in the "ID" Combo box

NOTE

When the unit has a list of clients connected through DHCP, and the unit is reset, the list will show empty. In this case renew the PC IP address from DHCP on LAN.

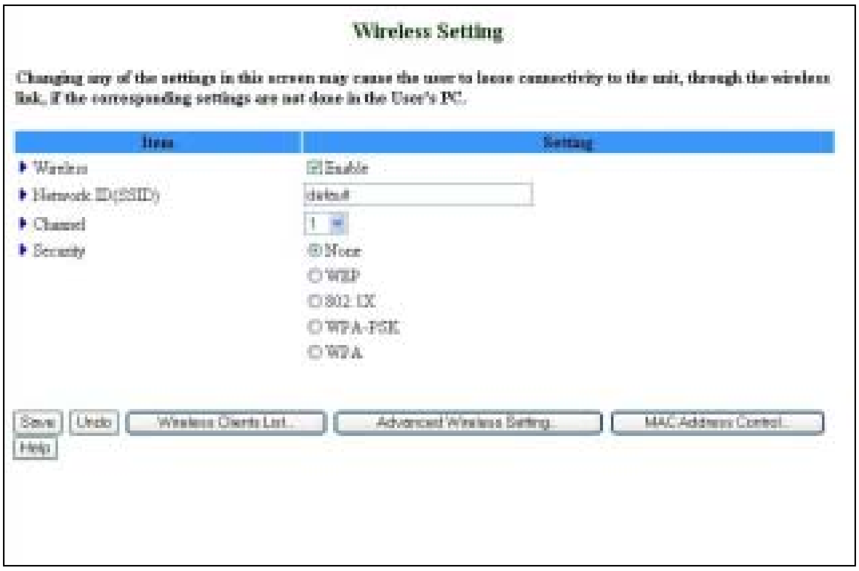
2. The control table is divided into several pages. Use the << **Previous page** and **Next Page** >> buttons to jump to a different page.

3.6.3 Wireless Setting

Wireless settings allow you to set the wireless configuration items.

CAUTION

Changing any of the parameters may cause loss of wireless link connectivity to the unit if the settings do not match the settings on the WLL subscriber in the User's PC.



Wireless Setting

Changing any of the settings in this screen may cause the user to loose connectivity to the unit, through the wireless link, if the corresponding settings are not done in the User's PC.

Item	Setting
Wireless	☑ Enable
Network ID(SSID)	default
Channel	1
Security	● None ○ WEP ○ 802.1X ○ WPA-PSK ○ WPA

Figure 28: Wireless Setting

The *Wireless Setting* window includes the following parameters:

Table 23: Wireless Setting Parameters

Parameter	Description
Wireless	Enable/Disable – Check the Enable box to enable this service. The default setting is "Enable".
Network ID (SSID)	Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this product and other Access Points that have the same Network ID. The factory setting is "default".
Channel	The radio channel number. The permissible channels depend on the Regulatory Domain.
Security	Select the data privacy algorithm you want to protect your data when being transferred from one station to another. The available security protocols are:
	Â None – No encryption is applied. (default) Â WEP (Wired Equivalent Privacy) – Encrypts frames transmitted through a wireless module using a pre-entered WEP key. You can configure 4 key sets and select one to apply as follows: 4# WEP 64 bit - 10 hexadecimal digits 4# WEP 128 bit – 26 hexadecimal digits 4# WEP 256 bit – 58 hexadecimal digits Â 802.1x – When enabled, the wireless user must be authenticated before it is allowed to use the network services. One implementation of 802.1x (the most common one) is through a RADIUS server on your LAN, containing an authentication database. 4# Encryption Key Length – Select either 64 or 128 bits for the encryption key. 4# RADIUS Server IP – The 802.1x server's IP address. 4# RADIUS Port – The 802.1x server's service port. Â WPA-PSK - Accepts WPA clients only. Manually enter a pre-share key (encryption key) as follows:

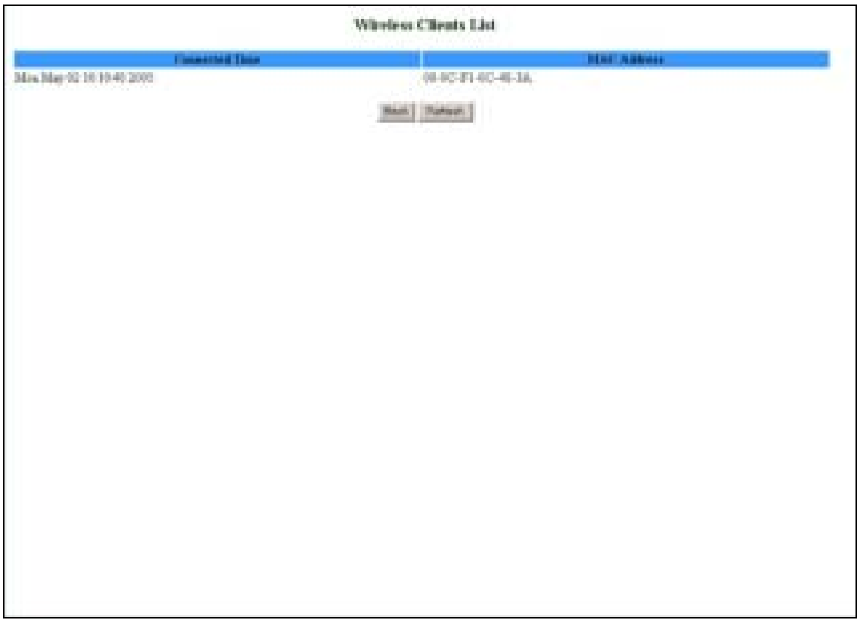
Parameter	Description
	4# Pre-share key mode: ASCII or HEX can be selected. 4# Pre share key: 32 ASCII characters or 64 hexadecimal digits pre-share key (encryption key).
	Â WPA (Wi-Fi Protected Access) – improves data protection and implements access control to Wireless LAN systems. Frames transmitted through a wireless module are encrypted using a Pre-share key (PSK) or a key received from the RADIUS server. 4# RADIUS Server IP – The 802.1x server's IP address. 4# RADIUS Port – The 802.1x server's service port. 4# RADIUS Shared Key – Key value shared by the RADIUS server and the networking gateway. The key value is consistent with the one in the RADIUS server.

IMPORTANT

If you enable the 802.1x or WPA feature, you must have a RADIUS server available.

3.6.3.1 Wireless Clients List

Clicking on the **Wireless Clients List** button that appears in the Wireless Setting window opens the *Wireless Clients List* window.



Wireless Clients List

Connected Time	MAC Address
Mon May 02 16:19:40 2005	00-0C-F1-0C-4E-3A

Figure 29: Wireless Clients List

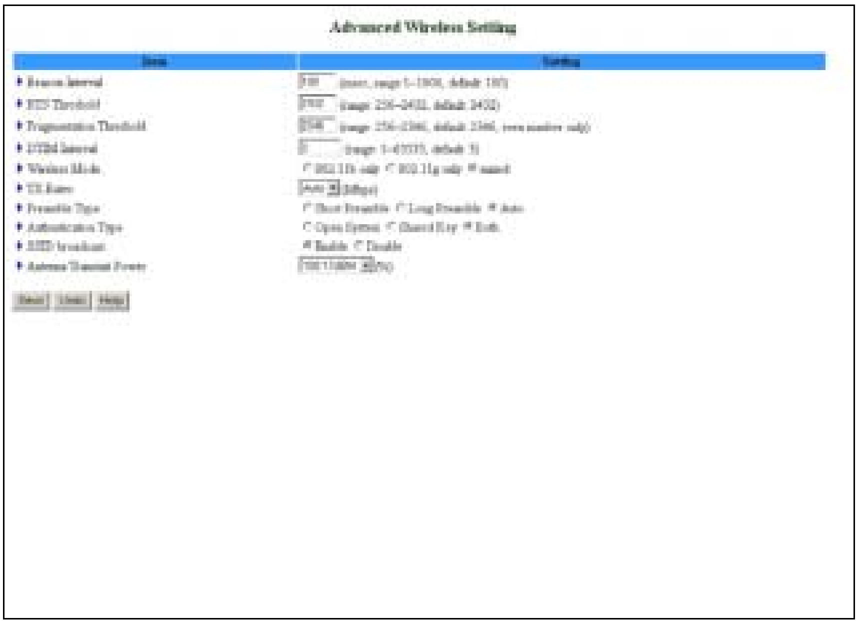
The *Wireless Clients List* displays the following parameters for each wireless client:

Table 24: Wireless Clients List Parameters

Parameter	Description
Connected Time	The connection time.
MAC Address	The MAC address of the wireless client.

3.6.3.2 Advanced Wireless Setting

Clicking the **Advanced Wireless Setting** button that appears in the *Wireless Setting* window opens the *Advanced Wireless Setting* window.



Advanced Wireless Setting

Item	Setting
Beacon Interval	100 (msec, range 1~1000, default 100)
RTS Threshold	2432 (range 256~2432, default 2432)
Fragmentation Threshold	2346 (range 256~2346, default 2346, even number only)
DTIM Interval	3 (range 1~65535, default 3)
Wireless Mode	○ 802.11b only ○ 802.11g only ● mixed
TX Rates	Auto (Mbps)
Preamble Type	○ Short Preamble ○ Long Preamble ● Auto
Authentication Type	○ Open System ○ Shared Key ● Both
SSID broadcast	● Enable ○ Disable
Antenna Transmit Power	100(100mW) (%)

Figure 30: Advanced Wireless Setting

The *Advanced Wireless Setting* window includes the following parameters:

Table 25: Advanced Wireless Setting Parameters

Parameter	Description
Beacon Interval	Specify the intervals (in milliseconds) between the packets sent by the access point to synchronize the wireless network (beacons). The range is 1~1000 milliseconds The default is 100 milliseconds.
RTS Threshold	Specify the packet size above which a Request To Send will be performed. Used to determine whether CSMA/CD or CSMA/CA will be used. The range is 256~2432 bytes The default is 2432 bytes.
Fragmentation Threshold	Specify the packet size above which fragmentation will be performed. The range is 256~2346 bytes, even numbers only The default is 2346 bytes.

Parameter	Description
DTIM Interval	Delivery Traffic Indication Message (DTIM) is a countdown informing clients of the next window for listening to broadcast and multicast messages. The range is: 1~65535 seconds. The default value is 3 seconds.
Wireless Mode	The wireless mode supported: 802.11b, 802.11g, or both. The default is both.
TX Rates	Select the wireless transfer rate from the dropdown list, based on the speed of wireless adapters on the WLAN. The default is auto rate.
Preamble Type	Defines the length of the Cyclic Redundancy Check (CRC) block for communication between the Access Point and roaming wireless adapters. A long transmit preamble may provide a more reliable connection or slightly longer range. A short transmit preamble provides better performance. Select short/long or automatic preamble to be assigned to each packet. The default is auto mode.
Authentication Type	Used for wireless authentication when associated with an AP router. Â Open System Â Shared Key Â Both The default is auto mode.
SSID Broadcast	Enable/Disable broadcasting the network's ID. The default is Enable.
Antenna Transmit Power	Select the antenna's transmission power from the dropdown list. The default is 100% TX power (17 dBm).

3.6.3.3 MAC Address Control

MAC Address Control allows to assign different access rights for different users and to assign a fixed IP address to a specific MAC address. For further details, see section 3.6.2.2.

3.6.4 Change Password

The *Change Password* window allows to change the system password. For security reasons, it is strongly recommended that you do so.

To access change password:

1 Select *Basic Setting* > *Change Password* submenu on the menu list. The *Change Password* window opens.

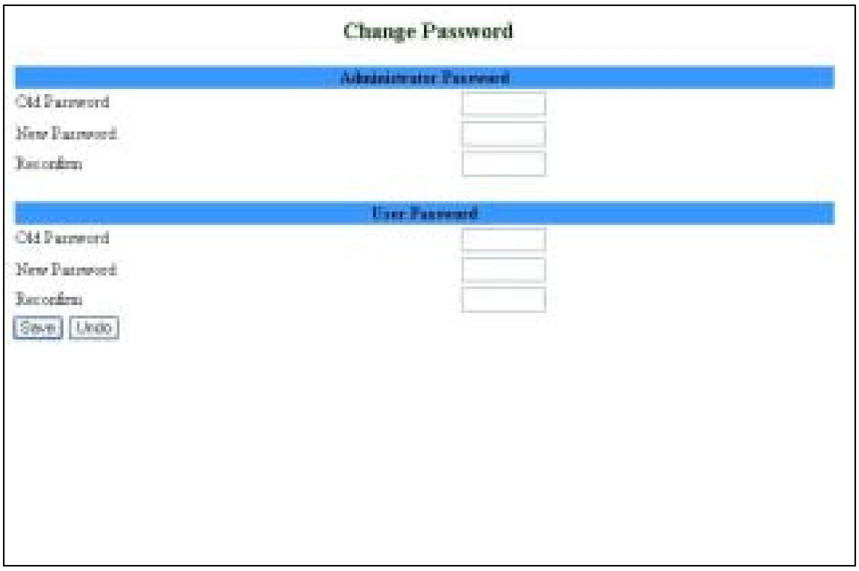


Figure 31: Change Password

2 Type in the old password in the Old Password box.

3 Type in the new password in the New Password box.

4 Re-type the new password in the Reconfirm box. The password should be identical to the one entered in the New Password field.

5 Click **Save** to save the new password(s).

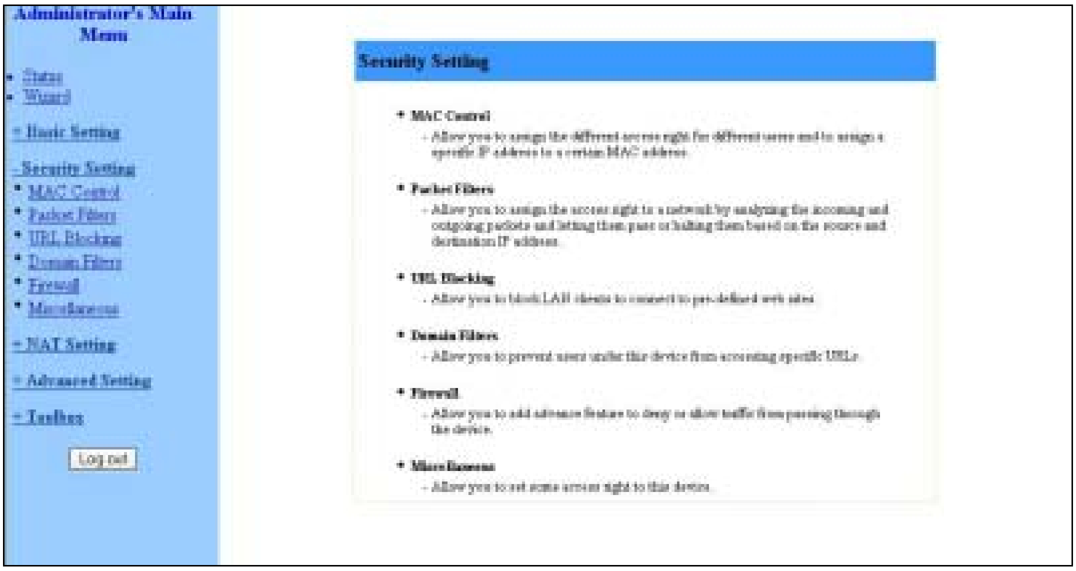
Follow this procedure for the Administrator Password level, for the User Password level, or for both password levels.

NOTE

The Administrator Password is visible to the Administrator entry level only.

3.7 Security Setting

Click on the *Security Setting* menu on the menu list to display the submenus and the *Security Setting* window.



Security Setting

- MAC Control
  - Allow you to assign the different access right for different users and to assign a specific IP address to a certain MAC address.
- Packet Filters
  - Allow you to assign the access right to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the source and destination IP address.
- URL Blocking
  - Allow you to block LAN clients to connect to pre-defined web sites.
- Domain Filters
  - Allow you to prevent users under this device from accessing specific URLs.
- Firewall
  - Allow you to add advance feature to deny or allow traffic from passing through the device.
- Miscellaneous
  - Allow you to set some access right to this device.

Figure 32: Security Setting Window

3.7.1 MAC Control

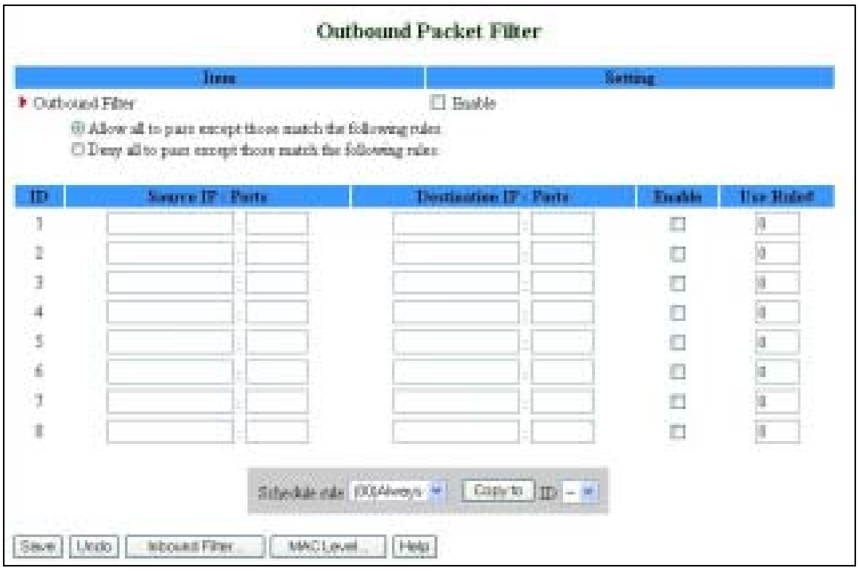
MAC Address Control allows to assign different access rights for different users and to assign a fixed IP address to a specific MAC address. For further details, see section 3.6.2.2.

3.7.2 Packet Filters (Administrator only)

Packet Filter enables to control which packets are allowed to pass through the networking gateway. When selecting the *Packet Filters* submenu on the menu list, the *Outbound Packet Filter* window opens.

NOTE

The **Inbound Filter…** button at the bottom of the window toggles between the *Outbound* and *Inbound Packet Filter* windows. The button's text will change from **Inbound Filter…** to **Outbound Filter…** accordingly.



Outbound Packet Filter

Item	Setting
Outbound Filter	□ Enable

● Allow all to pass except those match the following rules

○ Deny all to pass except those match the following rules

ID	Source IP : Ports		Destination IP : Ports		Enable	Use Rule#
1					□	0
2					□	0
3					□	0
4					□	0
5					□	0
6					□	0
7					□	0
8					□	0

Schedule rule (00)Always

Figure 33: Packet Filter Initial Window

The Outbound filter applies on all outbound packets. The Inbound filter applies only on packets that are destined to Virtual Servers or DMZ host. You can select one of the following filtering policies:

Â Allow all to pass except those match the specified rules

Â Deny all to pass except those match the specified rules

Up to 8 rules can be specified for each direction, inbound and outbound. For each rule, you can define the following:

Table 26: Advanced Wireless Setting Parameters

Parameter	Description
Source IP address	You can define a single IP address (for example, 4.3.2.1) or a range of IP addresses (for example, 4.3.2.1-4.3.2.254). An empty field denotes all IP addresses.
Source Ports address	You can define a single port (for example, 80) or a range of ports (for example, 1000-1999). Add a prefix "T" or "U" to specify a TCP or UDP protocol. For example, T80, U53, U2000-2999. No prefix indicates both TCP and UDP protocols. An empty field denotes all port addresses.

Parameter	Description
Destination IP address	You can define a single IP address (for example, 4.3.2.1) or a range of IP addresses (for example, 4.3.2.1-4.3.2.254). An empty field denotes all IP addresses.
Destination port address	You can define a single port (for example, 80) or a range of ports (for example, 1000-1999). Add prefix "T" or "U" to specify a TCP or UDP protocol. For example, T80, U53, U2000-2999. No prefix indicates both TCP and UDP protocols. An empty field denotes all port addresses.
Enable	Check to enable the rule. Each rule can be enabled or disabled individually.
Use Rule#	*Packet Filter* can work with *Scheduling Rules*. For details, please refer to *Schedule Rule* on page 80.

The Schedule Rule option facilitates the process of selecting a scheduling rule for each Filter ID. Select a specific Schedule Rule from the Schedule Rule Combo box. Select the Filter ID to which the schedule rule will apply from the ID Combo box and click **Copy to** to copy the Schedule Rule number to the selected Filter ID.

Click **Save** to save your Inbound/Outbound Packet Filter settings.

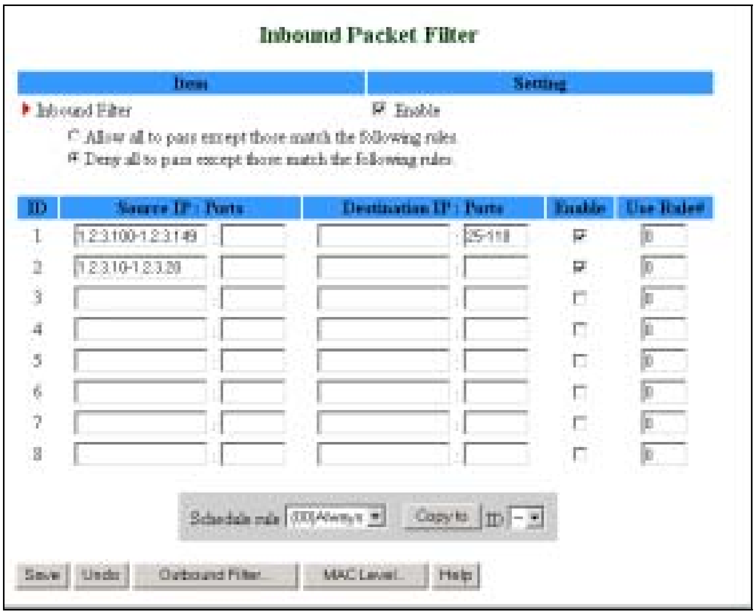
The following paragraphs provide examples for using the Inbound/Outbound Packet Filter option.

3.7.2.1 Inbound Filter

To enable *Inbound Packet Filter* click on the **Inbound Filter** button and check the *Enable* box in the *Inbound Packet Filter* window.

In the following examples, the SMTP Server (port 25), POP Server (port 110), Web Server (port 80), FTP Server (port 21), and News Server (port 119) are defined in the Virtual Server or DMZ Host.

Example 1:



Inbound Packet Filter

Item	Setting
Inbound Filter	☑ Enable

○ Allow all to pass except those match the following rules
● Deny all to pass except those match the following rules

ID	Source IP : Ports		Destination IP : Ports		Enable	Use Rule#
1	1.2.3.100-1.2.3.149			25-110	☑	0
2	1.2.3.10-1.2.3.20				☑	0
3					☐	0
4					☐	0
5					☐	0
6					☐	0
7					☐	0
8					☐	0

Schedule rule (00)Always ▾ Copy to ID - ▾

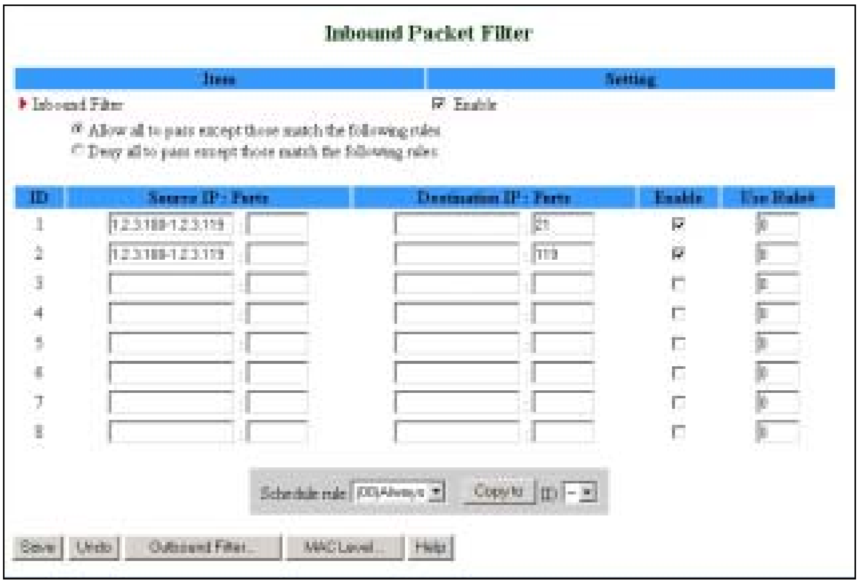
Figure 34: Inbound Packet Filter – Example 1

In this example, IPs (1.2.3.100-1.2.3.149) are allowed to send mail (port 25), receive mail (port 110), and browse the Internet (port 80).

IPs (1.2.3.10-1.2.3.20) are allowed to perform all operations.

All other IPs are all blocked from performing any operation.

Example 2:



Inbound Packet Filter

Item	Setting
Inbound Filter	☑ Enable

● Allow all to pass except those match the following rules
○ Deny all to pass except those match the following rules

ID	Source IP : Ports		Destination IP : Ports		Enable	Use Rule#
1	1.2.3.100-1.2.3.119			21	☑	0
2	1.2.3.100-1.2.3.119			119	☑	0
3					☐	0
4					☐	0
5					☐	0
6					☐	0
7					☐	0
8					☐	0

Schedule rule (00)Always ▾ Copy to ID - ▾

Figure 35: Inbound Packet Filter - Example 2

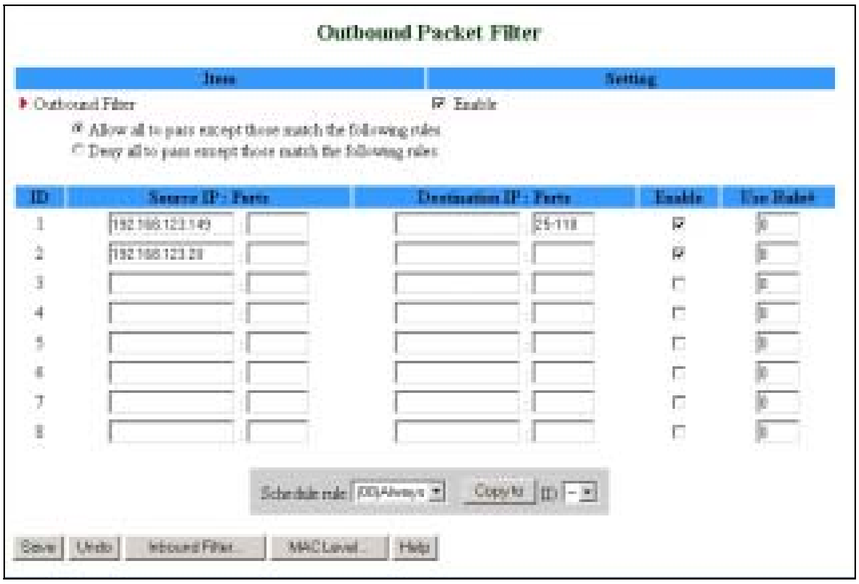
In this example, IPs (1.2.3.100-1.2.3.119) are allowed to do everything except read net news (port 119) and transfer files via FTP (port 21).

All other IPs are all allowed to perform all operations.

3.7.2.2 Outbound Filter

To enable *Outbound Packet Filter*, click on the **Outbound Filter** button and check the *Enable* box in the *Outbound Packet Filter* window.

Example 1:



Outbound Packet Filter

Item	Setting
Outbound Filter	☑ Enable

● Allow all to pass except those match the following rules
○ Deny all to pass except those match the following rules

ID	Source IP : Ports		Destination IP : Ports		Enable	Use Rule#
1	192.168.123.149			25-110	☑	0
2	192.168.123.20				☑	0
3					☐	0
4					☐	0
5					☐	0
6					☐	0
7					☐	0
8					☐	0

Schedule rule (00)Always

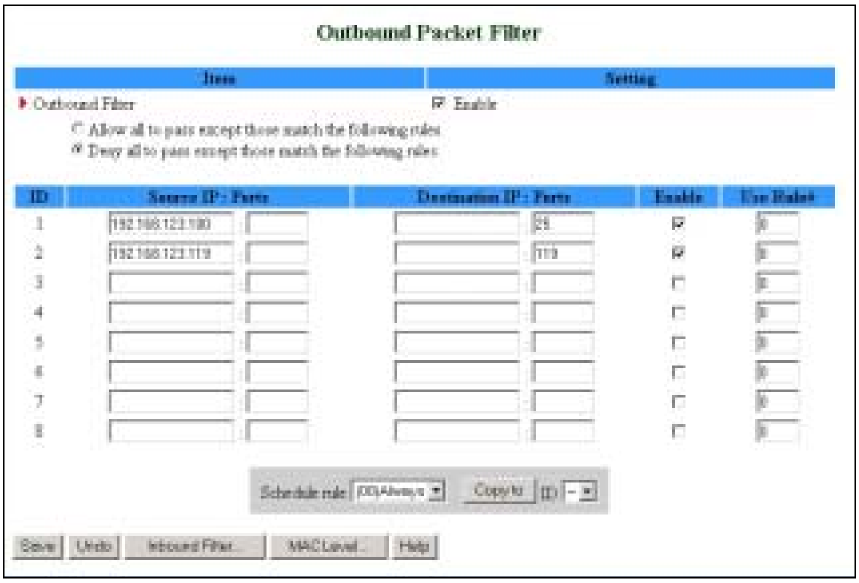
Figure 36: Outbound Packet Filter - Example 1

In this example, IP (192.168.123.149) is restricted from sending mail (port 25), receiving mail (port 110), and browsing the Internet (port 80). It is allowed to perform all other operations.

IP (192.168.123.20) is blocked from performing any operation.

All other IPs are allowed to perform all operations.

Example 2:



Outbound Packet Filter

Item	Setting
Outbound Filter	☑ Enable

○ Allow all to pass except those match the following rules
● Deny all to pass except those match the following rules

ID	Source IP : Ports		Destination IP : Ports		Enable	Use Rule#
1	192.168.123.100			25	☑	0
2	192.168.123.119			119	☑	0
3					☐	0
4					☐	0
5					☐	0
6					☐	0
7					☐	0
8					☐	0

Schedule rule (00)Always

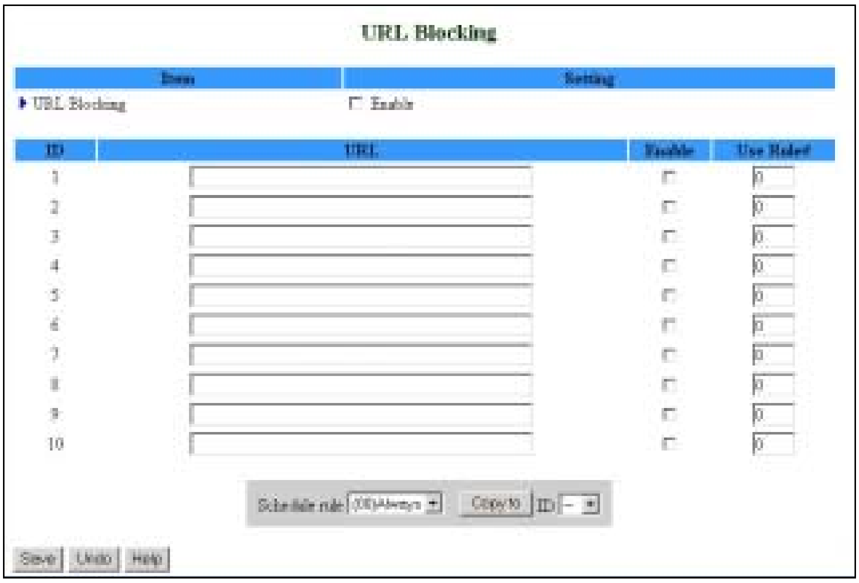
Figure 37: Outbound Packet Filter - Example 2

In this example, IPs (192.168.123.100) and (192.168.123.119) can only read net news (port 119) and send mail (port 25). They are blocked from performing any other operation.

All other IPs are blocked from performing any operation.

3.7.3 URL Blocking (Administrator only)

When enabled, this feature blocks LAN computers from connecting to predefined Web sites.



URL Blocking

Item	Setting
URL Blocking	☐ Enable

ID	URL	Enable	Use Rule#
1		☐	0
2		☐	0
3		☐	0
4		☐	0
5		☐	0
6		☐	0
7		☐	0
8		☐	0
9		☐	0
10		☐	0

Schedule rule (00)Always

Figure 38: URL Blocking

The *URL Blocking* window includes the following parameters:

Table 27: URL Blocking Parameters

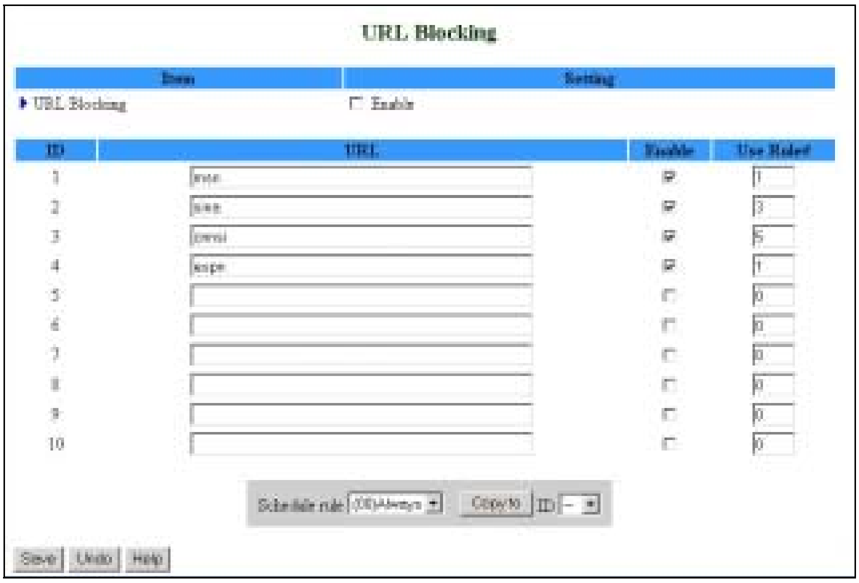
Parameter	Description
URL Blocking	Enable/Disable - Check to enable the URL Blocking feature.
URL	If any part of the Web site's URL matches the pre-defined word specified in this field, the connection will be blocked. For example, you can use a pre-defined word "sex" to block all Web sites whose URLs contain the word "sex".
Enable	Check to enable the rule. Each rule can be enabled or disabled individually.
Use Rule#	URL Blocking can work with Scheduling Rules. For details, please refer to *Schedule Rule* on page 80.

The Schedule Rule option facilitates the process of selecting a scheduling rule for each Filter ID. Select a specific Schedule Rule from the Schedule Rule Combo box. Select the Filter ID to which the schedule rule will apply from the ID Combo box and click **Copy to** to copy the Schedule Rule number to the selected Filter ID.

Click **Save** to save your settings.

The following section provides an example for using the URL Blocking option.

3.7.3.1 URL Blocking - Example



URL Blocking

Item	Setting
URL Blocking	□ Enable

ID	URL	Enable	Use Rule#
1	msn	☑	1
2	sina	☑	3
3	pensi	☑	5
4	espn	☑	1
5		□	0
6		□	0
7		□	0
8		□	0
9		□	0
10		□	0

Schedule rule (00)Always Copy to ID -

Figure 39: URL Blocking Example

In this example:

1 All URLs which include the string "msn" will be blocked, and the action will be recorded in the log file.

2 All URLs which include the string "sina" will be blocked, and the action will be recorded in the log file.

3 All URLs which include the string "cnnsi" will be blocked, and the action will be recorded in the log file.

4 All URLs which include the string "espn" will be blocked, and the action will be recorded in the log file.

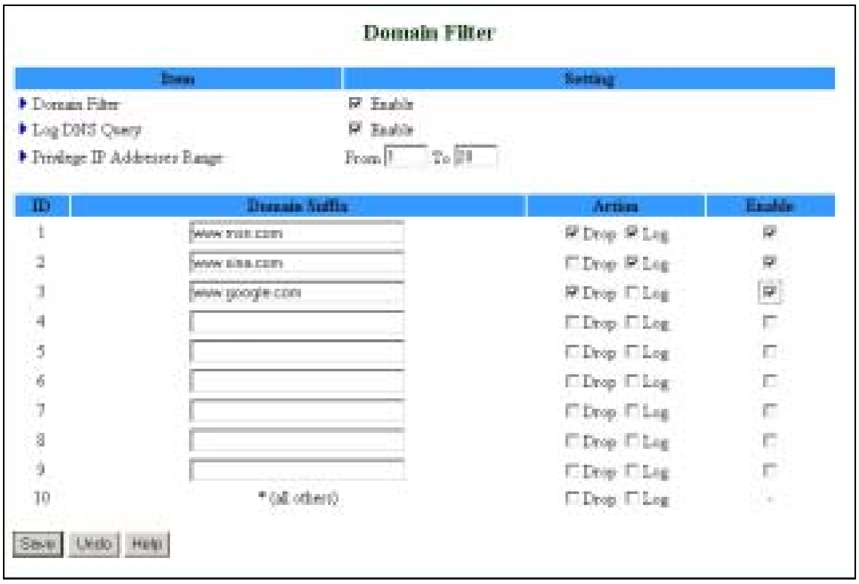
If the Enable box is not checked for a specific rule, the rule will not be applied and the matching URLs will not be blocked.

3.7.4 Domain Filter (Administrator only)

When enabled, the Domain Filter feature blocks LAN computers from connecting to pre-defined Web sites.

NOTE

While URL Blocking uses keywords to block all Web sites whose URL includes the pre-specified keyword, Domain Filter blocks a single or multiple domains by specifying the suffix (such as xxx.com, .org, etc.).



Domain Filter

Item	Setting
Domain Filter	☑ Enable
Log DNS Query	☑ Enable
Privilege IP Addresses Range	From 1 To [illegible]

ID	Domain Suffix	Action	Enable
1	www.msn.com	☑ Drop ☑ Log	☑
2	www.sina.com	☐ Drop ☑ Log	☑
3	www.google.com	☑ Drop ☐ Log	☑
4		☐ Drop ☐ Log	☐
5		☐ Drop ☐ Log	☐
6		☐ Drop ☐ Log	☐
7		☐ Drop ☐ Log	☐
8		☐ Drop ☐ Log	☐
9		☐ Drop ☐ Log	☐
10	* (all others)	☐ Drop ☐ Log	-

Figure 40: Domain Filter

Up to 9 Domain Suffixes can be defined, and for each rule you can specify the desired action to be taken when a user attempts to access that domain. For each rule you can define the following:

Table 28: Domain Filter Parameters

Parameter	Description
Domain Filter	Check to enable the Domain Filter feature to prevent users from accessing specific URLs.
Log DNS Query	Check to enable logging users' attempts to enter the specified URLs.
Privilege IP Addresses Range	Sets a group of hosts and allows them to access the network without restriction. The range is: From: 1~254, To: 1~254
Domain Suffix	A suffix of URL to be restricted. For example, ".com", "xxx.com".
Action	You can specify the type of action you want performed when someone attempts to access the specific URL that meets the domain-suffix: Â **Drop** – Check to block access. Â **Log** – Check to log the access attempt.
Enable	Check to enable the rule. Each rule can be enabled/disabled individually.

In the example above (Figure 40):

1 The URL "www.msn.com" will be blocked, and the action will be recorded in the log file.

2 The URL "www.sina.com" will not be blocked, but any attempt to enter the Web site will be recorded in the log file.

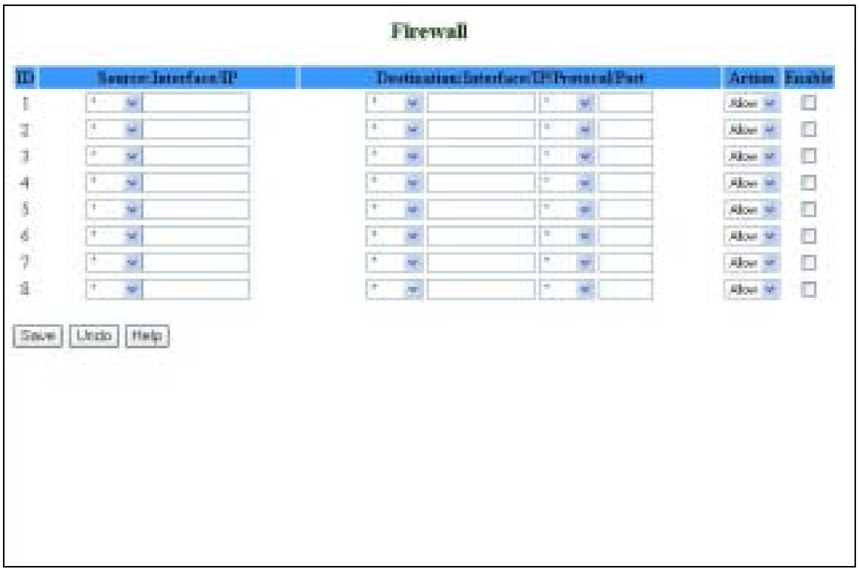
3 The URL "www.google.com" will be blocked, but the action will not be recorded in the log file.

4 IP address X.X.X.1~ X.X.X.20 can access network without restriction.

Click **Save** to save your settings.

3.7.5 Firewall (Administrator only)

Firewall rules deny/allow traffic from passing through the device.



Firewall

ID	Source:Interface/IP	Destination:Interface/IP/Protocol/Port	Action	Enable
1	*	* *	Allow	□
2	*	* *	Allow	□
3	*	* *	Allow	□
4	*	* *	Allow	□
5	*	* *	Allow	□
6	*	* *	Allow	□
7	*	* *	Allow	□
8	*	* *	Allow	□

Figure 41: Firewall

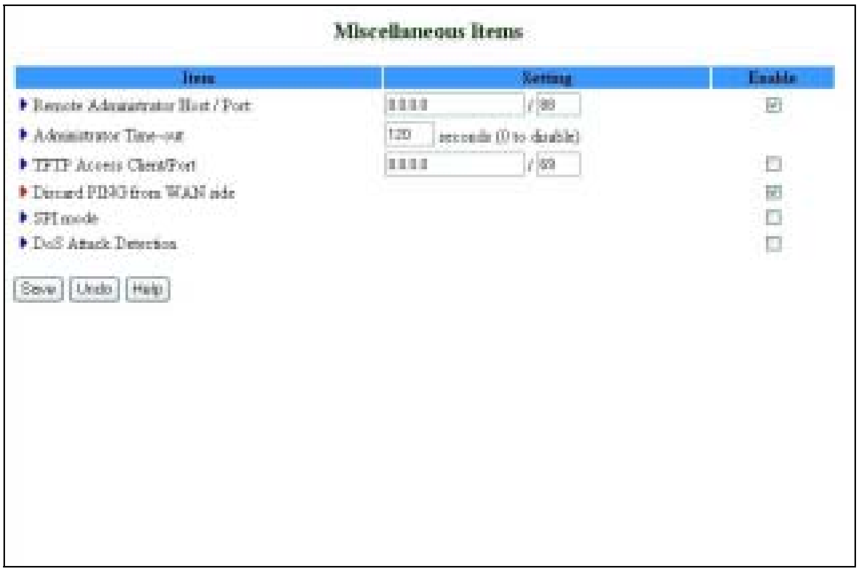
Up to 8 rules can be specified for each direction of traffic: inbound and outbound. For each rule, you can define the following:

Table 29: Firewall Parameters

Parameter	Description
Source IP address	From LAN or WAN
Destination IP address	From LAN or WAN
Destination Protocol	TCP, UDP or ICMP
Destination	Destination port number
Action	Allow/Deny The default is Allow
Enable	Check to enable the rule. Each rule can be enabled/disabled individually

Click **Save** to save your settings.

3.7.6 Miscellaneous Items (Administrator only)



Miscellaneous Items

Item	Setting	Enable
Remote Administrator Host / Port	0.0.0.0 / 88	☑
Administrator Time-out	120 seconds (0 to disable)	
TFTP Access Client/Port	0.0.0.0 / 69	☐
Discard PING from WAN side		☑
SPI mode		☐
DoS Attack Detection		☐

Figure 42: Miscellaneous Items

From the *Miscellaneous Items* window you can set the following parameters:

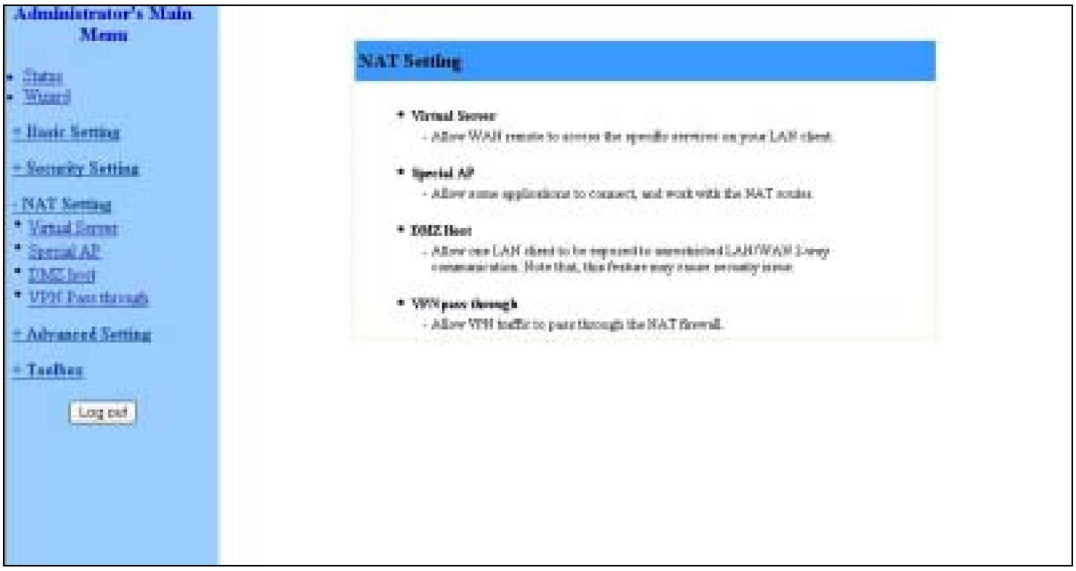
Table 30: Miscellaneous Items Parameters

Parameter	Description
Remote Administrator Host/Port	Enables the user to perform administration tasks from a remote host. When enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect to this device in order to perform administration tasks. You can use subnet mask bits "/nn" notation to specify a group of trusted IP addresses. For example, "10.1.2.0/24". **NOTE** - When Remote Administration is enabled, the web server port will automatically change to 88. You can change the web server port to another port. **IMPORTANT** – When managing the NG via bwaNMS (using the cut through option), the Remote Administrator Port must be set to 8080.
Administrator Time-out	The time of no activity to logout automatically. Set it to zero to disable automatic time-out
TFTP Access Client/Port	When enabled, the specified IP address can access the device through the TFTP client utility.
Discard PING from WAN	When enabled, any ping packet from WAN will be discarded.

Parameter	Description
side	
SPI Mode	When enabled, the router records the information, such as IP address, port address, ACK, SEQ number and so on, of the packets that pass through the WAN, and the Networking Gateway checks every incoming packet to detect whether it is valid.
DoS Attack Detection	When enabled, the router detects and logs the Denial of Service (DoS) attack that comes from the Internet. Currently, the Networking Gateway can detect the following DoS attack: SYN Attack, WinNuke, Port Scan, Ping of Death, and Land Attack etc.

3.8 NAT Setting (Administrator only)

The NAT Setting page provides access to configuring the virtual server, special AP, DMZ host and VPN pass through.



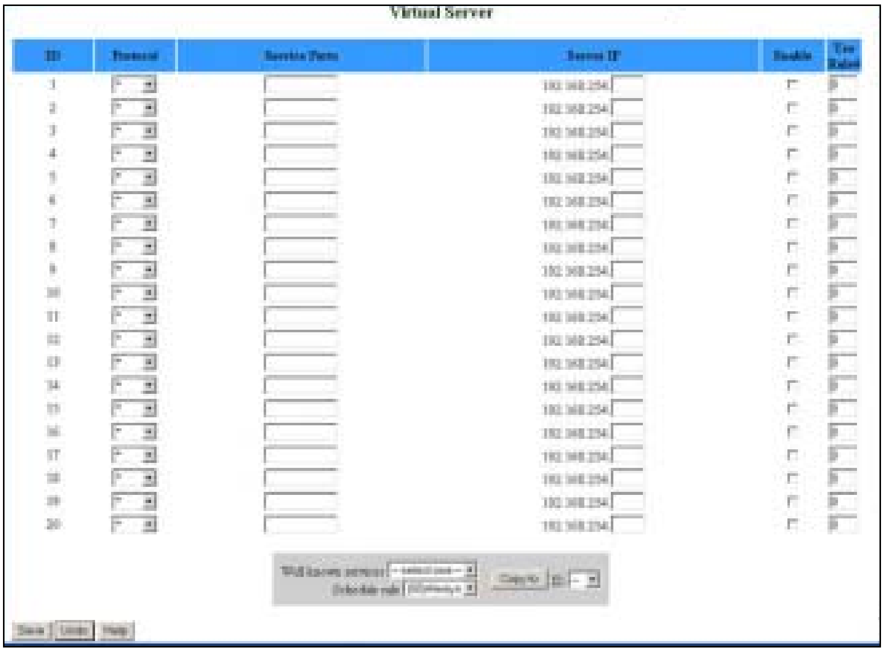
NAT Setting

- **Virtual Server**
  - Allow WAN remote to access the specific services on your LAN client.
- **Special AP**
  - Allow some applications to connect, and work with the NAT router.
- **DMZ Host**
  - Allow one LAN client to be exposed to unrestricted LAN/WAN 2-way communication. Note that, this feature may cause security issue.
- **VPN pass through**
  - Allow VPN traffic to pass through the NAT firewall.

Figure 43: NAT Setting

3.8.1 Virtual Server

Virtual Server enables WWW, FTP and other services on your LAN to be accessible to Internet users.



Virtual Server

ID	Protocol	Service Ports	Server IP	Enable	Use Rule#
1	T		192.168.254.	□	0
2	T		192.168.254.	□	0
3	T		192.168.254.	□	0
4	T		192.168.254.	□	0
5	T		192.168.254.	□	0
6	T		192.168.254.	□	0
7	T		192.168.254.	□	0
8	T		192.168.254.	□	0
9	T		192.168.254.	□	0
10	T		192.168.254.	□	0
11	T		192.168.254.	□	0
12	T		192.168.254.	□	0
13	T		192.168.254.	□	0
14	T		192.168.254.	□	0
15	T		192.168.254.	□	0
16	T		192.168.254.	□	0
17	T		192.168.254.	□	0
18	T		192.168.254.	□	0
19	T		192.168.254.	□	0
20	T		192.168.254.	□	0

Well known services: -- select one --
Schedule rule: (0)Always

Figure 44: Virtual Server

Specify the following parameters for each ID:

Table 31: Virtual Server Parameters

Parameter	Description
Protocol	Select from TCP, UDP, * (all). The default setting is *.
Service Ports	Enter a port number, or a range of ports.
Server IP	Enter the server IP on the LAN interface. The range is 1~254.
Enable	Check to enable the rule. Each rule can be enabled/disabled individually.
Use Rule#	*Virtual Server* can work with *Scheduling Rules*. For details, please refer to *Schedule Rule* on page 80.

In addition, the Virtual Server page allows to easily select services from a pre-defined list, and to assign to them a pre-defined rule.

Â Well known services – Select a service from the list of pre-defined services.

Â The Schedule Rule option facilitates the process of selecting a scheduling rule for each Virtual Server ID. Select a specific Schedule Rule from the Schedule Rule Combo box. Select the Virtual Server ID to which the schedule rule will apply from the ID Combo box and click **Copy to** to copy the Schedule Rule number to the selected Virtual Server ID.

3.8.2 Special AP

Some applications, such as Internet games, Video conferencing, Internet telephony etc., require multiple connections. Because of the firewall function, these applications cannot work with a pure NAT router. The *Special Applications* window makes some of these applications work with NAT router.

NOTE

Only one PC at a time can use each *Special Application*.

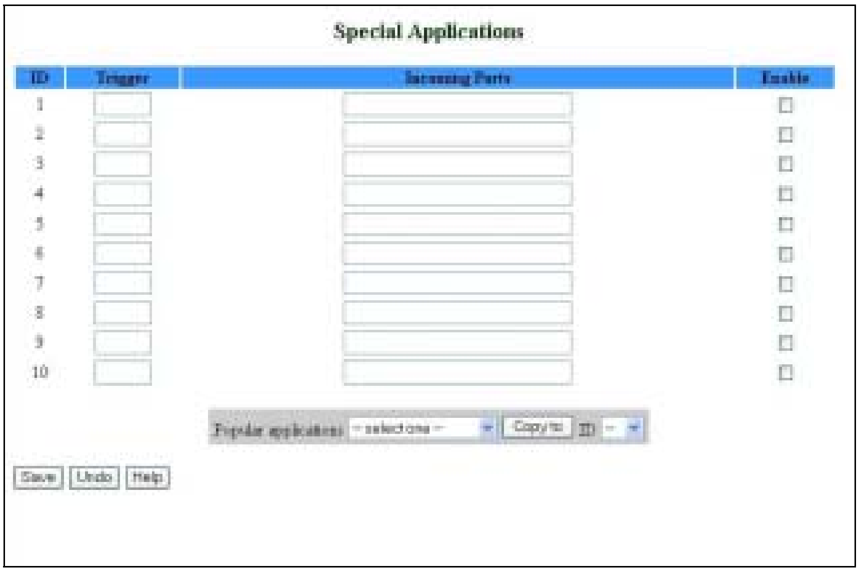


Figure 45: Special Applications

The *Special Applications* window includes the following parameters:

Table 32: Special Applications Parameters

Parameter	Description
Trigger	The outbound destination port number issued by the application.
Incoming Ports	When the trigger packet is detected using the destination port, the inbound packets to the specified port numbers are allowed to pass through the networking gateway.
Enable	Check to enable the rule. Each rule can be enabled/disabled individually.

Some predefined settings are provided. Select an application from the pre-defined list, select the ID number (1-10) and click **Copy to**, to add the predefined setting to your list.

NOTE

If *Special Applications* fails to make an application work, try DMZ host instead.

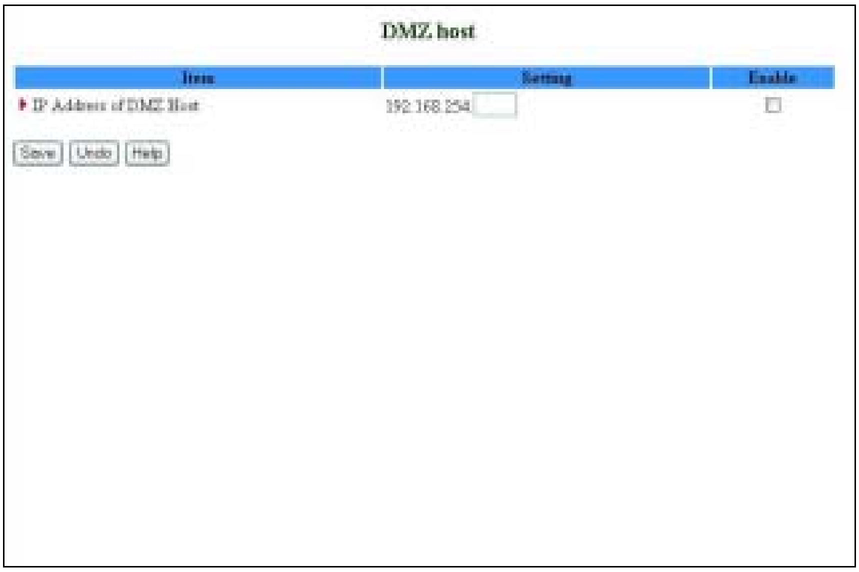
3.8.3 DMZ Host

Demilitarized Zone (DMZ) Host is a host without the firewall protection. It allows a computer to be exposed to unrestricted 2-way communication for

Internet games, Video conferencing, Internet telephony (H.323 or SIP), and other special applications.

CAUTION

This feature exposes your computer and may cause security issues. Make sure your PC is updated with the last security updates.



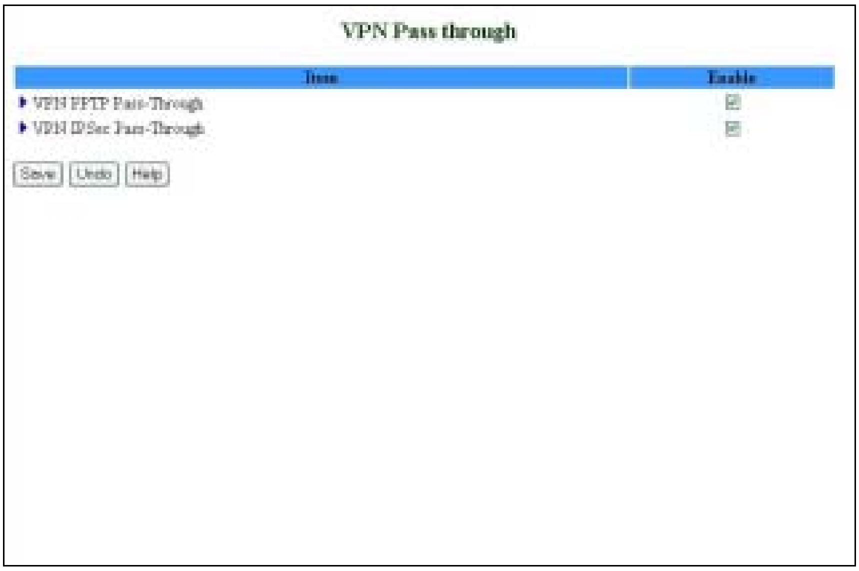
DMZ host

Item	Setting	Enable
IP Address of DMZ Host	192.168.254.	□

Figure 46: DMZ Host

Check the Enable box to enable this feature. One IP address should be set on the subnet of LAN.

3.8.4 VPN Pass Through



VPN Pass through

Item	Enable
VPN PPTP Pass-Through	☑
VPN IPSec Pass-Through	☑

Figure 47: VPN Pass Through

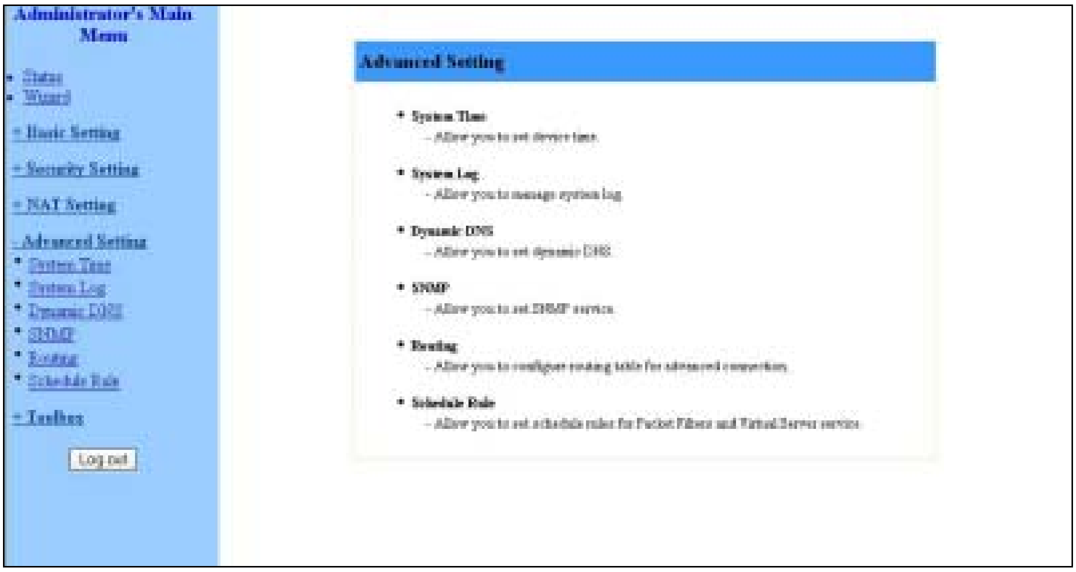
The *VPN Pass Through* window includes the following parameters:

Table 33: VPN Pass Through Parameters

Parameter	Description
VPN PPTP Pass-Through	Check to enable PPTP connection to pass through the device. The device can handle up to 8 concurrent sessions.
VPN IPSec Pass-Through	Check to enable IPSec connection to pass through the device. The device can handle up to 16 concurrent sessions.

3.9 Advanced Settings (Administrator only)

The *Advanced Settings* menu provides access to configuring additional features, such as System Time, Log, Dynamic DNS, SNMP, Routing, Scheduling Rules and enabling Universal Plug and Play protocol.



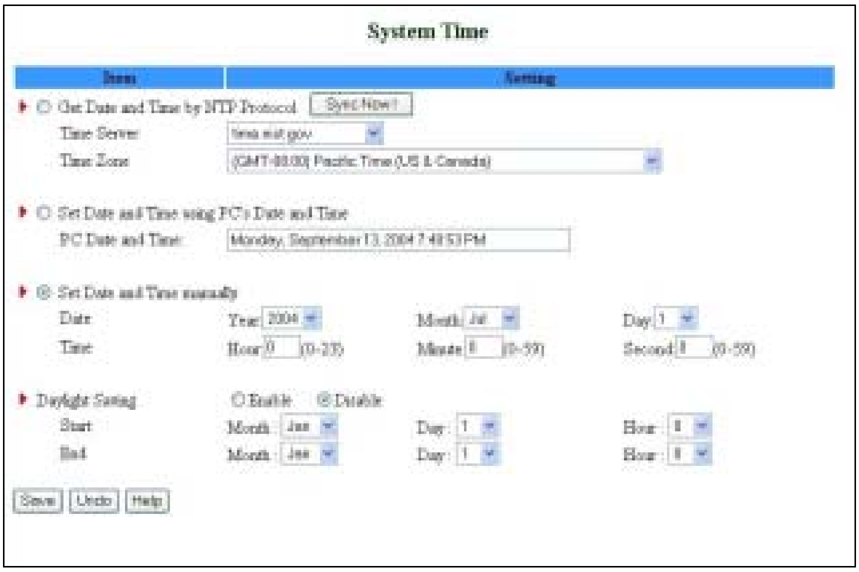
Advanced Setting

- System Time
  - Allow you to set device time.
- System Log
  - Allow you to manage system log.
- Dynamic DNS
  - Allow you to set dynamic DNS.
- SNMP
  - Allow you to set SNMP service.
- Routing
  - Allow you to configure routing table for advanced connection.
- Schedule Rule
  - Allow you to set schedule rules for Packet Filters and Virtual Server service.

Figure 48: Advanced Setting

3.9.1 System Time

The *System Time* window enables to set the device time.



System Time

Item	Setting
○ Get Date and Time by NTP Protocol	Sync Now!
Time Server	time.nist.gov
Time Zone	(GMT-08:00) Pacific Time (US & Canada)
○ Set Date and Time using PC's Date and Time	
PC Date and Time	Monday, September 13, 2004 7:48:53 PM
● Set Date and Time manually	
Date	Year 2004 Month Jul Day 1
Time	Hour 0 (0-23) Minute 0 (0-59) Second 0 (0-59)
Daylight Saving	○ Enable ● Disable
Start	Month Jan Day 1 Hour 0
End	Month Jan Day 1 Hour 0

Figure 49: System Time

From the *System Time* window, you can select one of the following ways to set the date and time of the device:

Table 34: System Time Parameters

Parameter	Description
Get Date and Time by NTP Protocol	Select if you want to set the device's internal clock using the Network Time Protocol (NTP) from a specific server located on the internet. Â Time Server - Select an NTP time server to consult UTC time. Â Time Zone - Select a time zone where this device is located. Â Sync Now! - Synchronize system time with network time server (alternatively, synchronization will be performed automatically from every 10 hours).
Set Date and Time using PC's Date and Time	Select if you want the device's internal clock to synchronize with the PC's clock.
Set Date and Time manually	Select if you want to manually set the device's internal clock. You need to specify: Â Date: Year, Month, Day Â Time: Hours (0-23), Minutes (0-59), Seconds (0-59).

The clock is set upon clicking **Save**.

NOTE

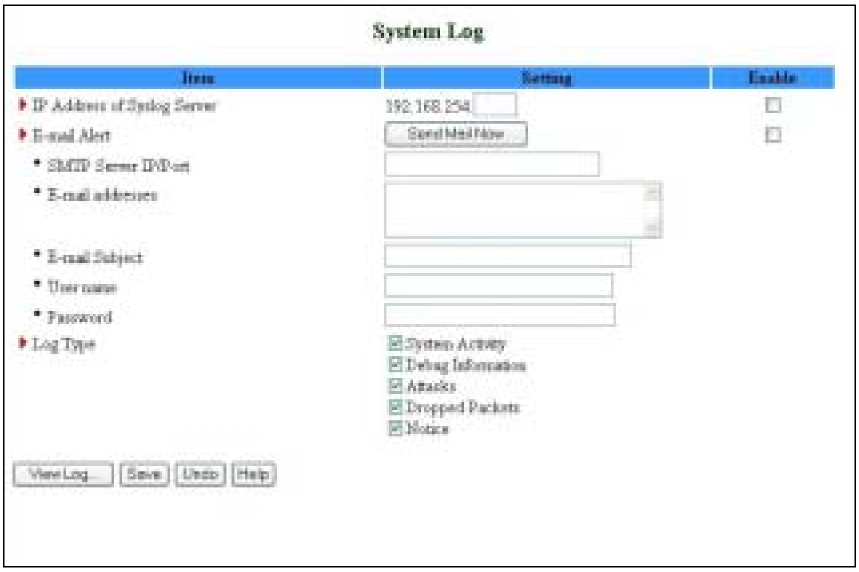
The device time is displayed at the bottom of the *Status* window.

In addition, you can specify daylight saving time as follows:

Â Daylight Saving - Enable/disable Daylight Saving and set start and end time of daylight saving time range.

3.9.2 System Log

System Log enables to set parameters for exporting system logs to a specified destination. Two exporting methods are supported: syslog (UDP) and SMTP (TCP).



System Log

Item	Setting	Enable
IP Address of Syslog Server	192.168.254.	□
E-mail Alert	Send Mail Now	□
• SMTP Server IP:Port		
• E-mail addresses		
• E-mail Subject		
• User name		
• Password		
Log Type	☑ System Activity ☑ Debug Information ☑ Attacks ☑ Dropped Packets ☑ Notice	

Figure 50: System Log

The *System Log* window includes the following parameters:

Table 35: System Log Parameters

Parameter	Description
IP Address for Syslog Server	Enter the IP address of the syslog server. It is valid only on your subnet LAN. Check to **Enable** this function.
E-mail Alert Enable	Check if you want to enable Email alert (send syslog via email). Â SMTP Server IP and Port - Enter the SMTP server IP and port, which are concatenate with ':'.For example, "mail.your_url.com" or "192.168.1.100:26". If you do not specify port number, the default value is 25. Â E-mail addresses - The listed recipients will receive these logs. You can assign more than 1 recipient, using a semi-colon (;) or a comma (,) to separate the addresses. Â E-mail Subject - The subject of email alert. This setting is optional. Â Username and Password - To fill some SMTP server's authentication requirement, you may need to enter the Username and Password provided by your ISP.
Log Type	Select the activities to be logged.

NOTE

The changes made in the System Log page become effective upon clicking **Save**. Rebooting the system is not required.

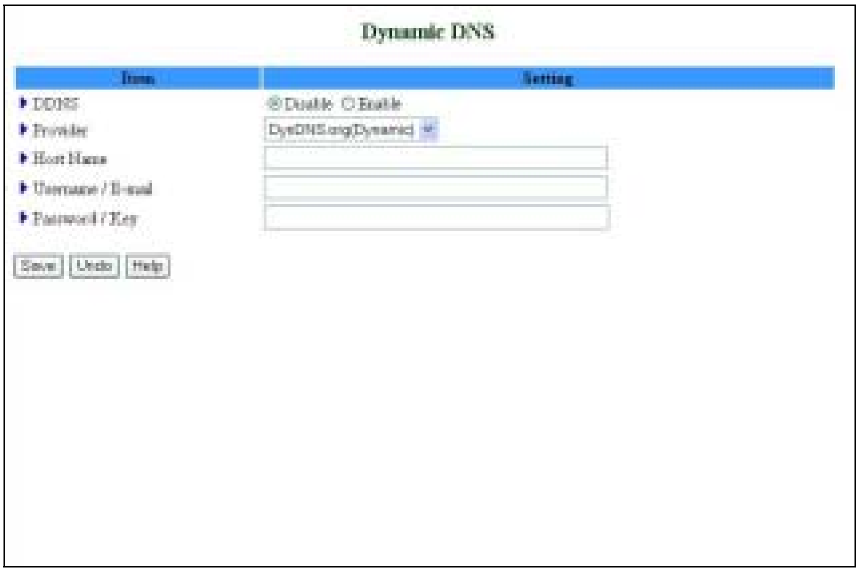
To view the system log:

Click on the **View Log...** button at the bottom of the screen. The *System Log* opens (see View Log on page 84, Figure 62)

3.9.3 Dynamic DNS

To host your server on a changing IP address, you need to use a Dynamic Domain Name Service (DDNS).

To reach your host, one needs to know its name. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect to your Internet service provider.



Dynamic DNS

Item	Setting
DDNS	● Disable ○ Enable
Provider	DynDNS.org(Dynamic)
Host Name	
Username / E-mail	
Password / Key	

Figure 51: Dynamic DNS

Before enabling Dynamic DNS, you need to register an account on of the Dynamic DNS servers listed here under Provider: DnyDNS.org(Dynamic), DnyDNS.org(Custom), TZO.com and dhs.org. Upon registration, you will receive your account details.

The *Dynamic DNS* window includes the following parameters:

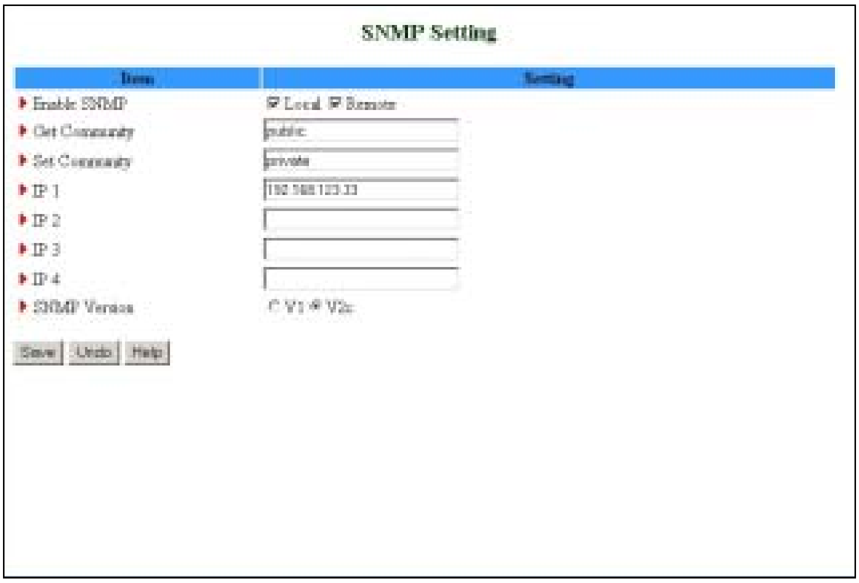
Table 36: Dynamic DNS Parameters

Parameter	Description
DDNS	Click **Enable** or **Disable** to enable/disable **Dynamic DNS**.
Provider	Select from the list of Dynamic DNS servers on which you have an account.
Host Name	Enter to register a domain name to the DDNS provider. The full domain name is concatenated with the specified Host Name and a suffix, specified by the DDNS provider.
Username/E-mail	Enter your Username or E-mail address according to the DDNS provider you selected.
Password/Key	Enter your password or key according to the DDNS provider you selected.

After Dynamic DNS setting is configured, click **Save**.

3.9.4 SNMP Setting

The Simple Network Management Protocol (SNMP) provides the user with the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.



SNMP Setting

Item	Setting
Enable SNMP	☑ Local ☑ Remote
Get Community	public
Set Community	private
IP 1	192.168.123.33
IP 2	
IP 3	
IP 4	
SNMP Version	○ V1 ● V2c

Figure 52: SNMP Setting

The *SNMP Setting* window includes the following parameters:

Table 37: SNMP Parameters

Parameter	Description
Enable SNMP	You must check either Local or Remote or both to enable the SNMP function. Â Local - The device will respond to requests from LAN. Â Remote – The device will respond to requests from WAN.
Get Community	Set the password for GetRequest access rights to your device.
Set Community	Setting the password for SetRequest access rights to your device.
IP 1,IP 2,IP 3,IP 4	Enter your IP addresses for allowed managers. SNMP Trap messages will be sent to this IP address as well. If no IP is defined, the unit cannot be managed by any PC, from either LAN or WAN.
SNMP Version	Select the proper SNMP Version supported by your SNMP Management software.

In the above figure:

Â The device will respond to requests from both LAN and WAN.

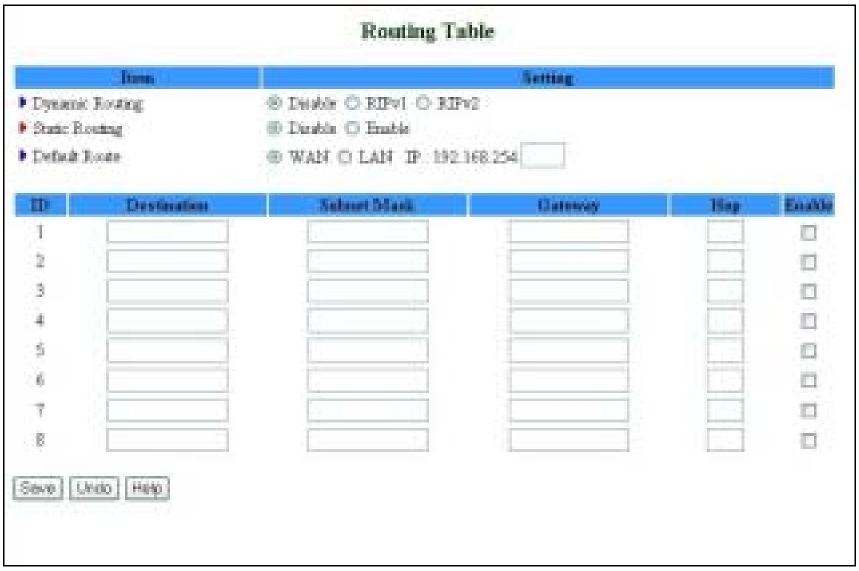
Â The device will respond to SNMP clients whose **get community** is set as "public" and coming from IP 192.168.123.33.

Â The device will respond to SNMP clients whose **set community** is set as "private" and coming from IP 192.168.123.33.

Â This device will send SNMP Trap messages to 192.168.123.33 (Using SNMP Version V2c).

3.9.5 Routing Table

Routing allows to determine which physical interface address to use for outgoing IP data grams. If you have more than one gateway and subnet, you will need to enable Routing Table to allow packets to find the proper routing path and allow different subnets to communicate with each other.



Routing Table

Item	Setting
Dynamic Routing	● Disable ○ RIPv1 ○ RIPv2
Static Routing	● Disable ○ Enable
Default Route	● WAN ○ LAN IP: 192.168.254.

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1					□
2					□
3					□
4					□
5					□
6					□
7					□
8					□

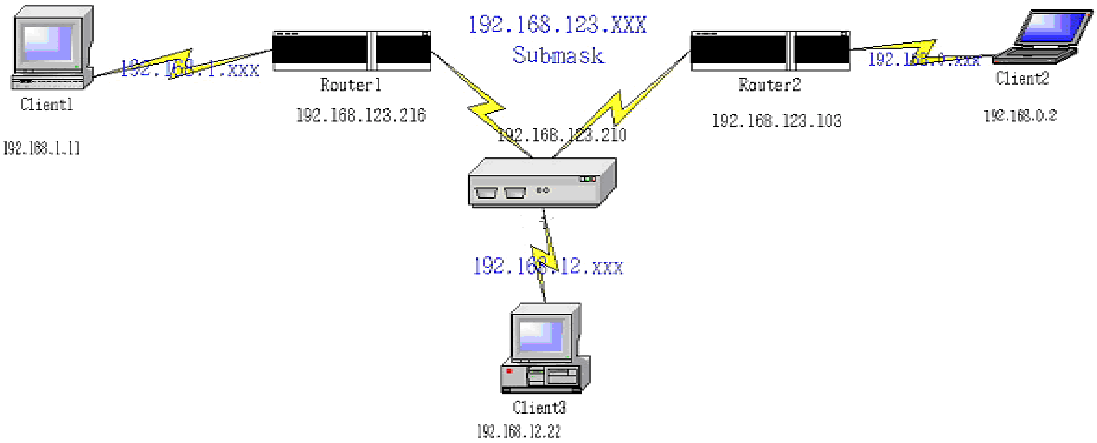
Figure 53: Routing Table

Routing Table settings are used to setup the functions of static and dynamic routing. The *Routing Table* window includes the following parameters:

Table 38: Routing Table Parameters

Parameter	Description
Dynamic Routing	Routing Information Protocol (RIP) will exchange information on destinations for computing routes throughout the network. Select RIPv2 only if you have a different subnet on your network. Otherwise, select RIPv1 if you need this protocol.
Static Routing	For static routing, you can specify up to 8 routing rules. You can enter the destination IP address, subnet mask, and gateway, hop for each routing rule, and enable/disable the individual rule.
Default Route	Sets the default route interface as WAN or LAN. For LAN, one IP for routing must be set.

Example:



Configuration on NAT Router

Destination	Subnet Mask	Gateway	Hop	Enabled
192.168.1.0	255.255.255.0	192.168.123.216	1	ˇ
192.168.0.0	255.255.255.0	192.168.123.103	1	ˇ

If, for example, Client3 wanted to send an IP datagram to 192.168.0.2 (Client2), he would use the above table to determine that he had to go via 192.168.123.103 (Gateway2).

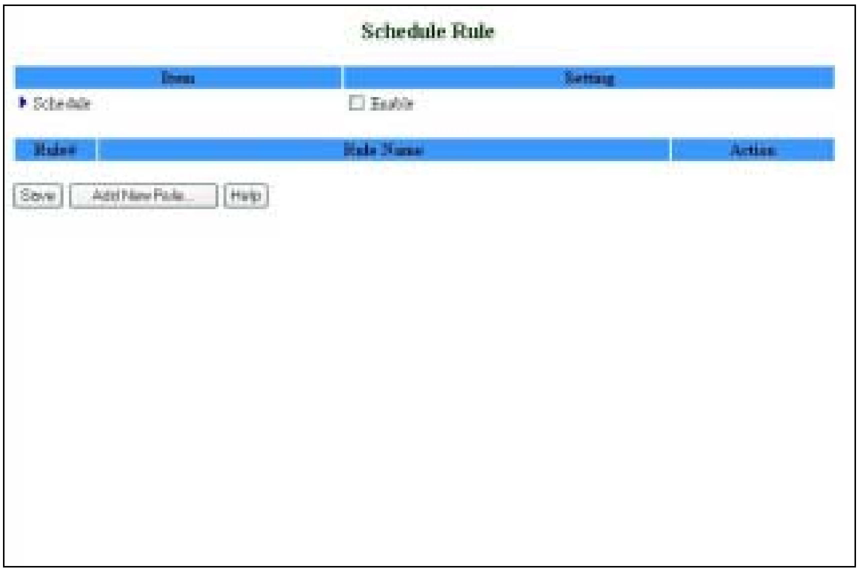
And if he sends Packets to 192.168.1.11 he will go via 192.168.123.216 (Gateway1).

Each rule can be enabled or disabled individually.

After the Routing Table setting is configured, click **Save**.

3.9.6 Schedule Rule

Schedule Rule allows to set the schedule time for which a service will be turned on or off.



Schedule Rule

Item	Setting
▸ Schedule	□ Enable

Rule#	Rule Name	Action

Figure 54: Schedule Rule

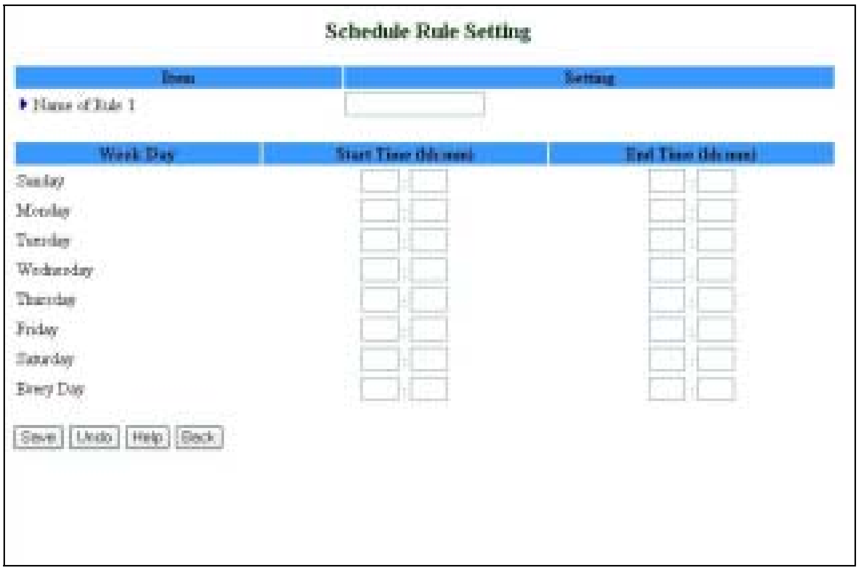
The *Schedule Rule* window includes the following parameters:

Table 39: Routing Table Parameters

Parameter	Description
Schedule	Click the checkbox to Enable the Scheduler.
Rule #	The rule number. Rules are numbered sequentially from the first rule set to the last. When a rule is deleted, the rules are automatically renumbered for all unit configurations.
Rule Name	The name of the rule.
Action	Edit and Delete - Every rule can be edited or deleted individually.

To add a new rule:

1 Click **Add New Rule** to add a rule to the list. The *Schedule Rule Setting* window opens.



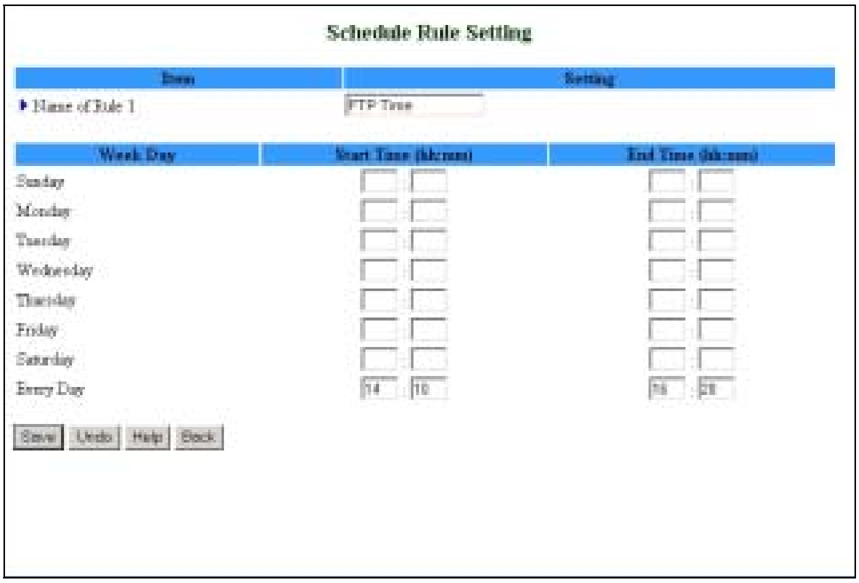
Schedule Rule Setting

Item	Setting
▸ Name of Rule 1	

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Sunday		
Monday		
Tuesday		
Wednesday		
Thursday		
Friday		
Saturday		
Every Day		

Figure 55: Schedule rule Setting

You can enter a rule name and set which day and what time to schedule from “Start Time” to “End Time”. In the following example, a rule named "FTP Time" is scheduled to operate every day between 14:10 and 16:20.



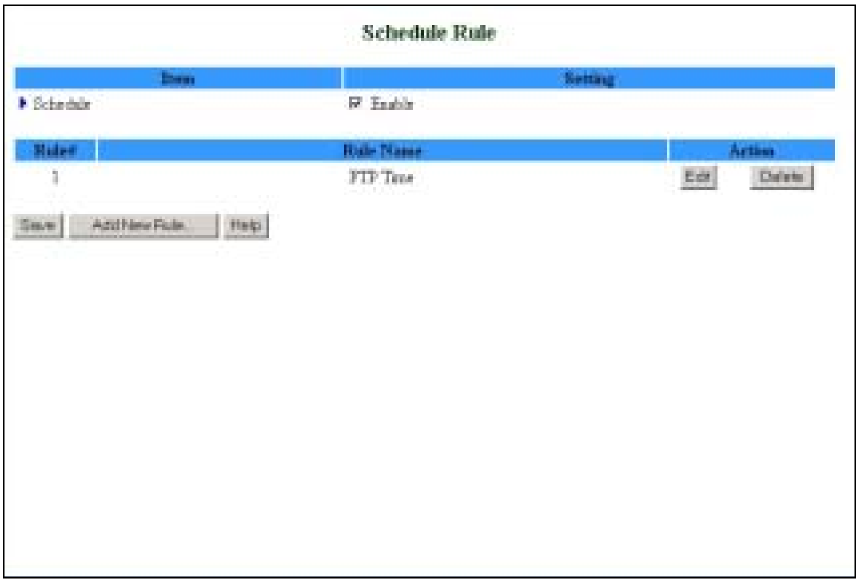
Schedule Rule Setting

Item	Setting
▸ Name of Rule 1	FTP Time

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Sunday		
Monday		
Tuesday		
Wednesday		
Thursday		
Friday		
Saturday		
Every Day	14 : 10	16 : 20

Figure 56: Schedule Rule Setting – Example Step 1

2 After configuring Rule 1, click on **Save** to save the rule and return to the *Schedule Rule* window. The new rule is now displayed on the list.



Schedule Rule

Item	Setting
Schedule	☑ Enable

Rule#	Rule Name	Action
1	FTP Time	Edit Delete

Figure 57: Schedule Rule Setting – Example Step 2

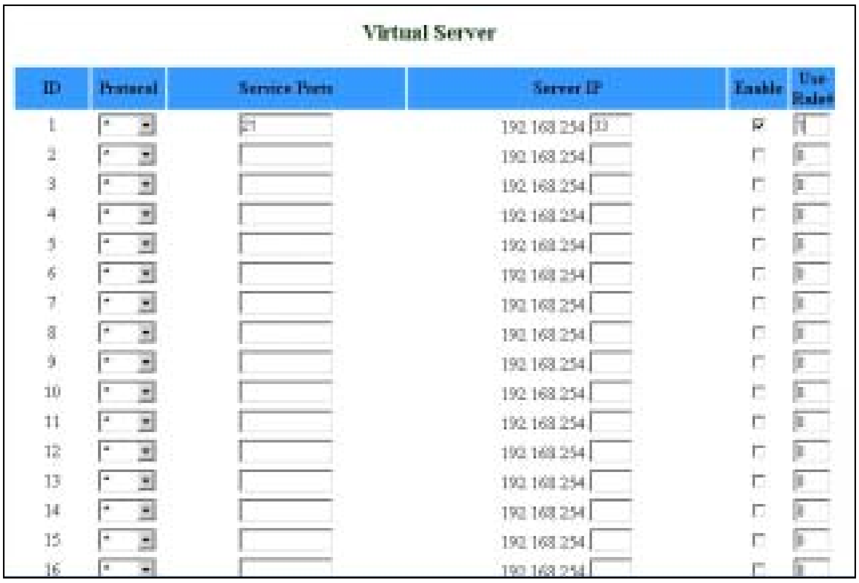
When rules are set, you can:

- Edit – Click to edit the specific rule.

- Delete – Click to delete the specific rule. When the rule is deleted, all subsequent rules are automatically renumbered.

Schedule Rule can be applied to Virtual server and Packet Filter, for example:

Example1: **Virtual Server** – Apply Rule#1 using the scheduled rule #1 (ftp time: every day 14:10 to 16:20).

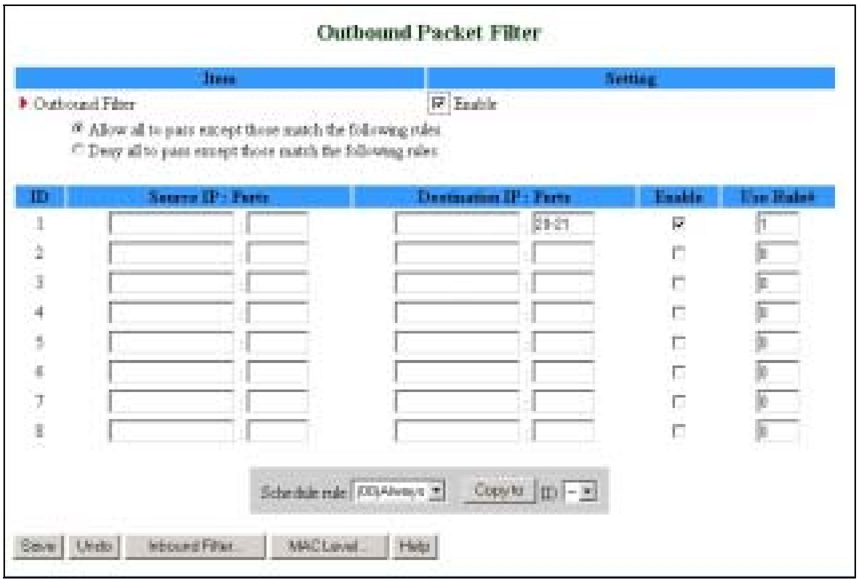


Virtual Server

ID	Protocol	Service Ports	Server IP	Enable	Use Rule#
1	*	21	192.168.254.33	☑	1
2	*		192.168.254.	☐	0
3	*		192.168.254.	☐	0
4	*		192.168.254.	☐	0
5	*		192.168.254.	☐	0
6	*		192.168.254.	☐	0
7	*		192.168.254.	☐	0
8	*		192.168.254.	☐	0
9	*		192.168.254.	☐	0
10	*		192.168.254.	☐	0
11	*		192.168.254.	☐	0
12	*		192.168.254.	☐	0
13	*		192.168.254.	☐	0
14	*		192.168.254.	☐	0
15	*		192.168.254.	☐	0
16	*		192.168.254.	☐	0

Figure 58: Virtual Server - Schedule Rule#1

Example2: **Packet Filter** – Apply Rule#1 using scheduled rule #1 (ftp time: every day 14:10 to 16:20).



Outbound Packet Filter

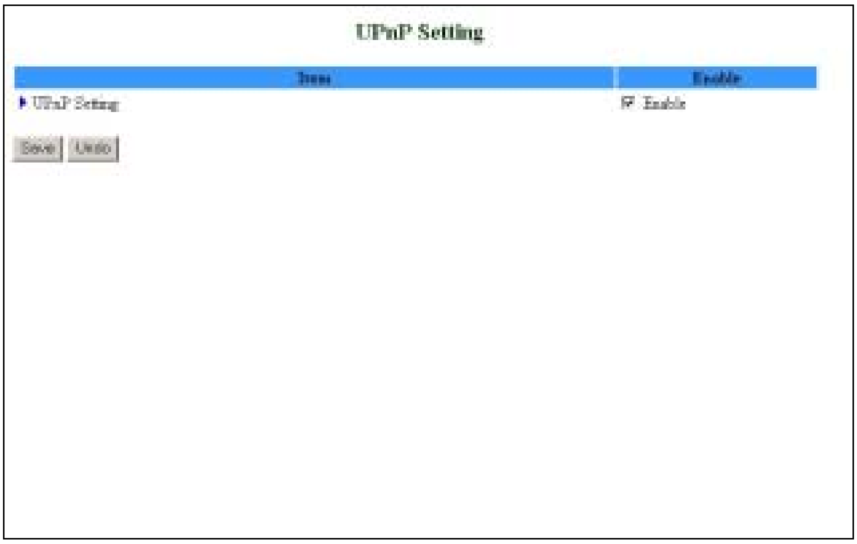
Item	Setting
Outbound Filter ● Allow all to pass except those match the following rules ○ Deny all to pass except those match the following rules	☑ Enable

ID	Source IP : Ports		Destination IP : Ports		Enable	Use Rule#
1				21-21	☑	1
2					☐	0
3					☐	0
4					☐	0
5					☐	0
6					☐	0
7					☐	0
8					☐	0

Figure 59: Packet Filter - Schedule Rule#1

3.9.7 UPnP Setting

Universal Plug and Play (UPnP) is a protocol for connecting voice/video applications through the Networking Gateway when in NAT mode.



UPnP Setting

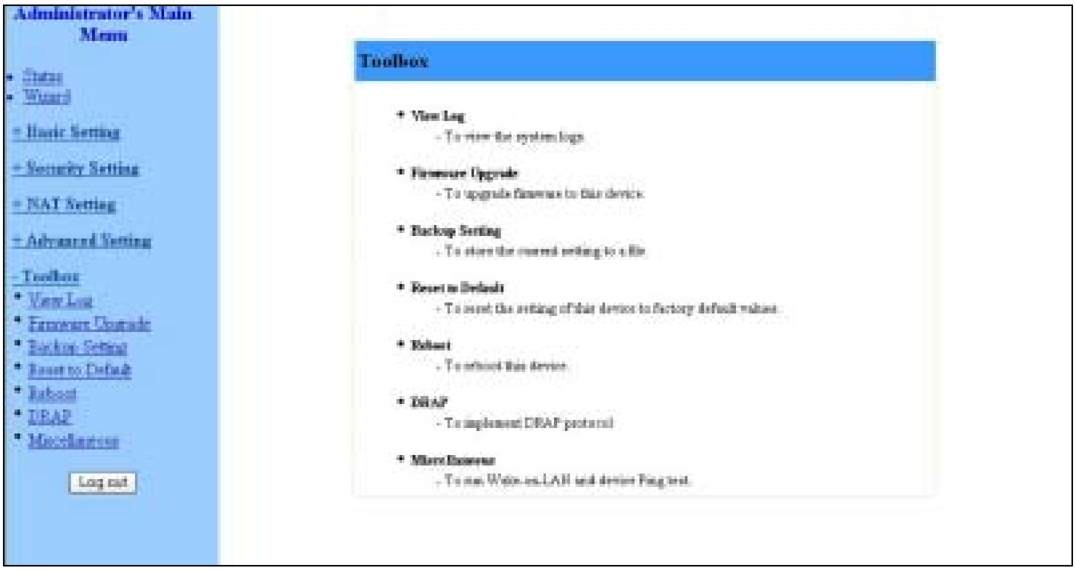
Item	Enable
UPnP Setting	☑ Enable

Figure 60: UPnP Setting

UPnP Setting - Enable/Disable – enables/disables the feature. NAT should be enabled.

3.10 Toolbox

The Toolbox menu provides access to viewing the system log, to firmware upgrade, backup setting, resetting the system to the factory default values, to rebooting the system, implementing DRAP protocol, running Wake-on-LAN and performing Ping tests.



Toolbox

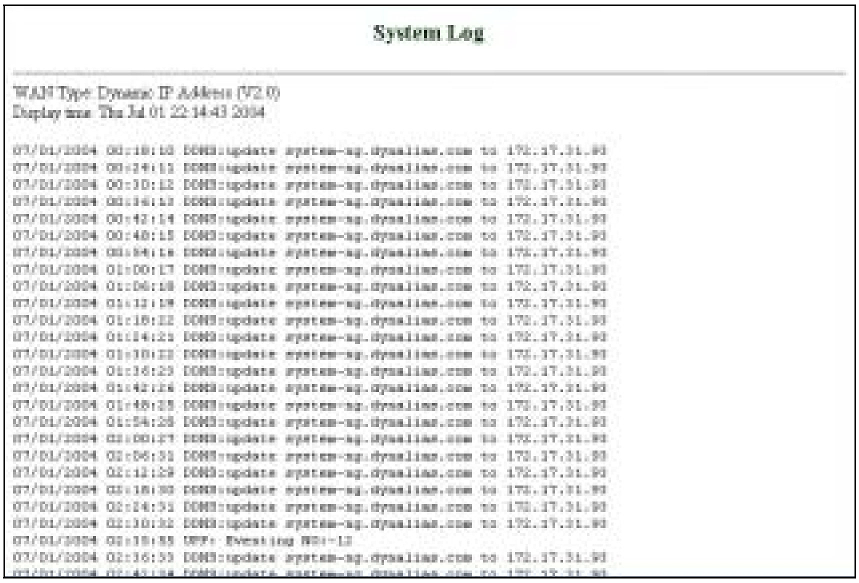
- **View Log**
  - To view the system logs
- **Firmware Upgrade**
  - To upgrade firmware to this device
- **Backup Setting**
  - To store the current setting to a file
- **Reset to Default**
  - To reset the setting of this device to factory default values
- **Reboot**
  - To reboot this device
- **DRAP**
  - To implement DRAP protocol
- **Miscellaneous**
  - To run Wake-on-LAN and device Ping test

Figure 61: Toolbox

3.10.1 View Log

Clicking on *View Log* opens the *System Log* file. The System Log file can also be accessed from the *System Log* window in the *Advanced Setting* menu.

The log file logs all the activities performed since the last reset.



System Log

WAN Type: Dynamic IP Address (V2.0)
Display time: Thu Jul 01 22:14:43 2004

```
07/01/2004 00:18:10 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 00:24:11 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 00:30:12 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 00:36:13 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 00:42:14 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 00:48:15 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 00:54:16 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 01:00:17 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 01:06:18 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 01:12:19 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 01:18:22 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 01:24:21 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 01:30:22 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 01:36:23 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 01:42:24 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 01:48:25 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 01:54:26 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 02:00:27 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 02:06:31 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 02:12:29 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 02:18:30 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 02:24:31 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 02:30:32 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 02:35:55 UPP: Eventing NO:-12
07/01/2004 02:36:33 DDNS:update system-ng.dynalias.com to 172.17.31.93
07/01/2004 02:42:34 DDNS:update system-ng.dynalias.com to 172.17.31.93
```

Figure 62: View System Log

While in Log View, you can:

- Click **Back** to return to the *System Log* window.

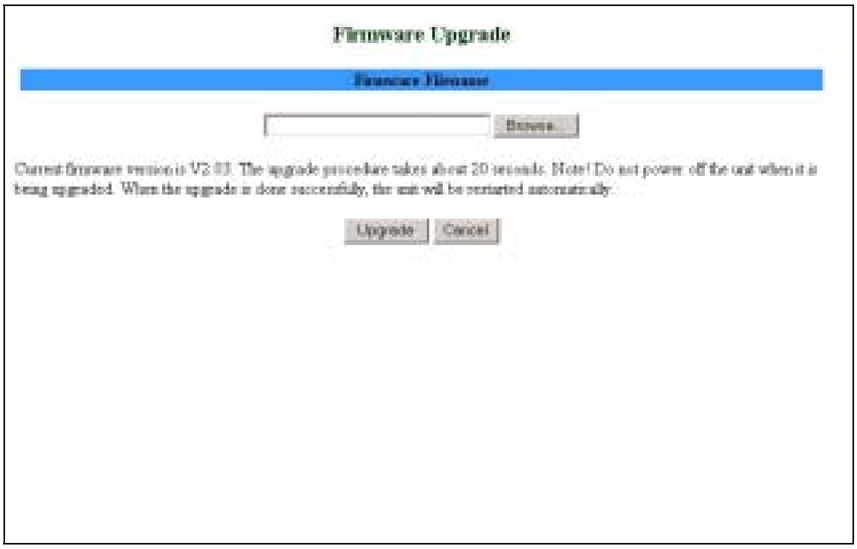
- Click **Refresh** to manually update the Log.

- Click **Download** to download the Log file (***system.log***) and save it locally, on your PC.

- Click **Clear** to clear the log file of its content.

3.10.2 Firmware Upgrade (Administrator only)

The Firmware Upgrade window displays the currently installed firmware version.



Current firmware version is V2.03. The upgrade procedure takes about 20 seconds. Note! Do not power off the unit when it is being upgraded. When the upgrade is done successfully, the unit will be restarted automatically.

Figure 63: Firmware Upgrade

To upgrade the firmware:

1. Click on **Browse** to browse to the upgrade file's location. The upgrade file is a *.BIN file.
2. Click **Upgrade** to begin the upgrading process, or **Cancel** to terminating it.

When the upgrade process is complete, the unit will automatically restart.

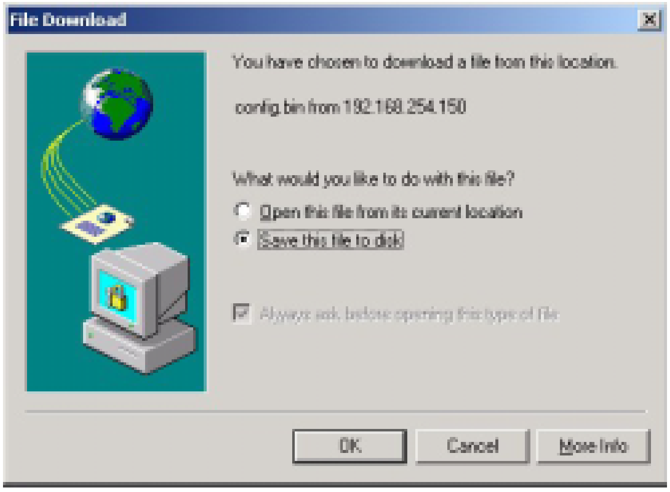
CAUTION

Do not turn off power to the unit during the upgrading process.

3.10.3 Backup Setting

To backup your settings:

1. Click *Backup Setting* in the menu list. This automatically opens the *File Download* window.
2. Select the **Save this file to disk** option and click **OK**. Follow the instructions on screen to save the file. The file is saved as a *.bin* file.



File Download

You have chosen to download a file from this location.

config.bin from 192.168.254.150

What would you like to do with this file?

○ Open this file from its current location

● Save this file to disk

☑ Always ask before opening this type of file

Figure 64: Backup

To restore your settings:

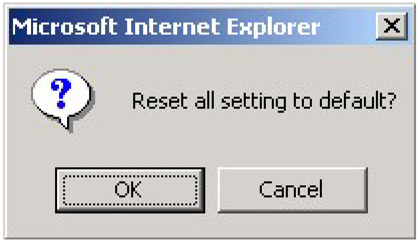
Select **Firmware Upgrade** from the Menu list, browse to the *.bin* file you saved, and click **Upgrade** (see Firmware Upgrade on page 85).

You can also upload the configuration file to the unit using TFTP client.

3.10.4 Reset to Default

To reset the unit to factory defaults:

1 Click *Reset to default* in the menu list. The following message appears.



Microsoft Internet Explorer

Reset all setting to default?

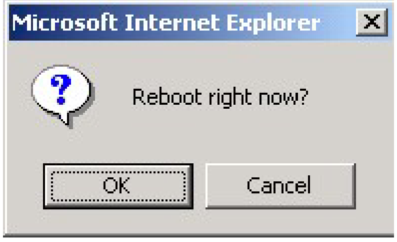
Figure 65: Reset to Default

2 Click **OK** to reset the settings to default, or **Cancel** to keep the current settings.

3.10.5 Reboot

To reboot the system:

1 Click *Reboot* in the menu list. The following message appears.



Microsoft Internet Explorer

Reboot right now?

Figure 66: Reboot

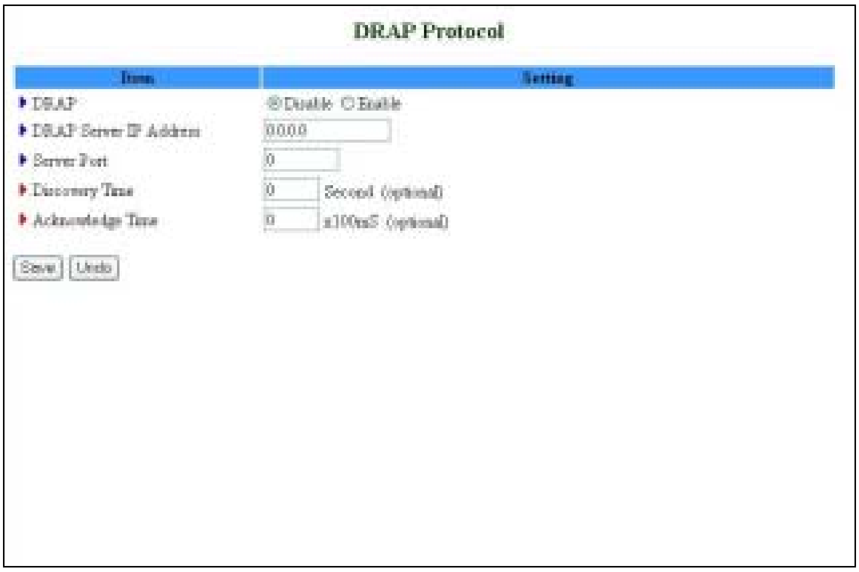
2 Click **OK** to reboot, or **Cancel** to continue working.

NOTE

Most of the configurations performed, require to reboot the system for them to take effect.

3.10.6 DRAP

Dynamic Resource Allocation Protocol (DRAP) is used for registration to the Base Station to which the SU is connected (by performing "Discovery").



DRAP Protocol

Item	Setting
DRAP	● Disable ○ Enable
DRAP Server IP Address	0.0.0.0
Server Port	0
Discovery Time	0 Second (optional)
Acknowledge Time	0 x100mS (optional)

Figure 67: DRAP Protocol

The *DRAP Protocol* window includes the following parameters:

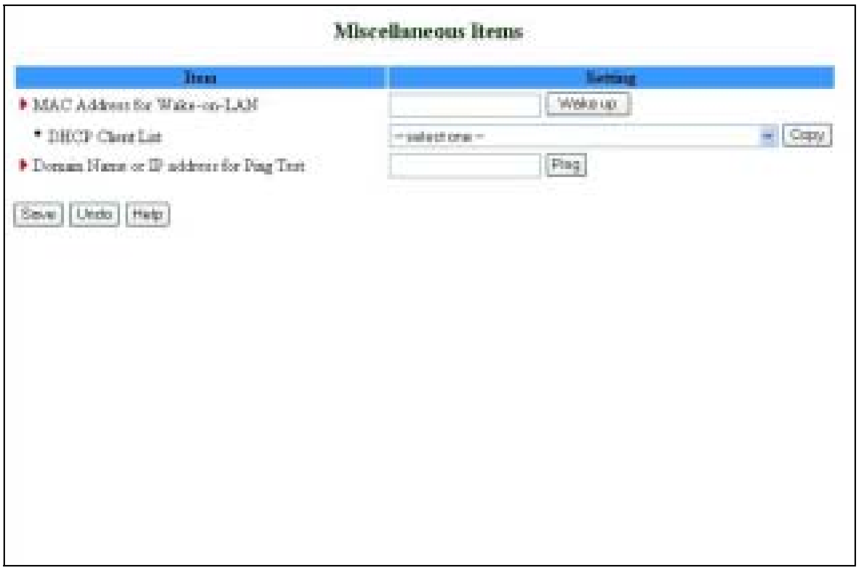
Table 40: DRAP Protocol Parameters

Parameter	Description
DRAP	Select Enable/Disable to enable/disable this feature. When enabled, a DRAP Server must be available. The default is Disable.
DRAP Server IP Address	The IP address of the DRAP Server. Leave empty for Auto

Parameter	Description
	Discovery. The default is 0.0.0.0.
Server Port	The UDP port used for the DRAP server. For WMAX use port 8171 The default is 0.
Discovery Time	The Discovery Time is the timeout to be used when the Auto Discovery process is used for finding a DRAP server. The Auto Discovery process is based on sending empty broadcast, and the Discovery Time is the time that the unit will wait for a response before sending a new request. The default is 0.
Acknowledge Time	The Acknowledge Time is the timeout to be used between messages. If no confirmation is received within this time, a new message should be sent. The default is 0.

3.10.7 Miscellaneous Items

From the Miscellaneous Items page, you can set the MAC Address for Wake-on-LAN, and the Domain name or IP address for performing ping tests to the device.



Miscellaneous Items

Item	Setting
MAC Address for Wake-on-LAN	
DHCP Client List	-- select one --
Domain Name or IP address for Ping Test	

Figure 68: Toolbox - Miscellaneous Items

The *Miscellaneous Items* window includes the following parameters:

Table 41: Miscellaneous Items Parameters

Parameter	Description
MAC Address for Wake-on-LAN	Wake-on-LAN enables to remotely power up a networked device. To use this feature, the target device must be Wake-on-LAN enabled and you need to know the device's MAC address, e.g., 00-11-22-33-44-55. Click on **Wake up** to have the gateway immediately send the wake-up frame to the target device. Â DHCP Client List – Select a client from the dropdown list for which you want to perform Wake-on-LAN. Â Copy – Click to copy the DHCP client's MAC Address to the Wake-on-LAN.
Domain Name or IP address for Ping Test	Allows to configure an IP, and ping the device. You can ping a specific IP to test that it is up and running. The IP must allow receiving and returning ICMP packets

Click on **Save** to save your settings.

3.11 Web Configuration Server’s Parameters Summary

Table 42: Web Configuration Server’s Parameters Summary

Parameter	Range/Options	Default
Status		
Printer (USB0) Status	Â Not Ready Â Off-line or no paper Â Printing Â Ready Â Device error	
Primary Setup		
WAN Type	Â Static IP Address Â Dynamic IP Address Â Dynamic IP Address with RRSM Â PPP over Ethernet Â PPTP	Dynamic IP Address
Primary Setup - Static IP Address		
WAN IP Address	x.x.x.x	0.0.0.0
WAN Subnet Mask	x.x.x.x	255.255.255.0
WAN Gateway	x.x.x.x	0.0.0.0
Primary DNS	x.x.x.x	0.0.0.0
Secondary DNS	x.x.x.x	0.0.0.0
NAT Disable	Check/Uncheck	Uncheck
Primary Setup - Dynamic IP Address		
Host Name	A string of maximum 39 characters	
WAN's MAC Address		

Parameter	Range/Options	Default
Renew IP Forever Enable	Check/Uncheck	Check
NAT Disable	Check/Uncheck	Uncheck
Primary Setup - Dynamic IP Address with Road Runner Session Management		
Account	A string of maximum 53 characters	
Password	A string of maximum 53 characters	
Login Server	A string of maximum 31 characters	
Renew IP Forever	Enable Check/Uncheck	Check
NAT	Disable Check/Uncheck	Uncheck
Primary Setup – PPP over Ethernet		
PPPoE Account	A string of maximum 53 characters	
PPPoE Password	A string of maximum 53 characters	
Primary DNS	x.x.x.x	0.0.0.0
Secondary DNS	x.x.x.x	0.0.0.0
Maximum Idle Time	0~65535	300 seconds
Connection Control	Â Connect-on-demand Â Auto Reconnect(always on) Â Manually	Auto Reconnect(always on)
MTU	0~9999	1492 bytes
Primary Setup - PPTP		
IP Mode	Â Dynamic IP Address Â Static IP Address	Dynamic IP Address
My IP Address	x.x.x.x	0.0.0.0
My Subnet Mask	x.x.x.x	0.0.0.0
WAN Gateway IP	x.x.x.x	0.0.0.0
Server IP Address/Name		

Parameter	Range/Options	Default
PPTP Account	A string of maximum 53 characters	
PPTP Password	A string of maximum 53 characters	
Connection ID	(Optional)	
Maximum Idle Time	0~65535	300 seconds
Connection Control	Â Connect-on-demand Â Auto Reconnect(always on) Â Manually	Auto Reconnect(always on)
LAN Setup		
LAN IP Address	x.x.x.x	192.168.254.253
LAN Subnet Mask	x.x.x.x	255.255.255.0
DHCP Server	Â Disable Â Enable	Enable
DHCP Proxy	Â Disable Â Enable Â Proxy IP x.x.x.x	Disable 0.0.0.0
LAN Setup – DHCP Enabled		
Range of IP addresses Pool	Â Start: 1~254 Â End: 1~254	192.168.254.100 192.168.254.199
Domain suffix	A string of maximum 31 characters	
Primary DNS	x.x.x.x	0.0.0.0
Secondary DNS	x.x.x.x	0.0.0.0
Primary WINS	x.x.x.x	0.0.0.0
Secondary WINS	x.x.x.x	0.0.0.0
Lease Time	0~99999	0 seconds
MAC Address Control/Fixed Mapping		
MAC Address Control Enable	Check/Uncheck	Uncheck

Parameter	Range/Options		Default
Connection Control	Â Check/Uncheck Â Allow/Deny		Â Uncheck Â Deny
Connection Control	Â Check/Uncheck Â Allow/Deny		Â Uncheck Â Deny
MAC Address Rules 1-4	MAC Address	A string of maximum 32 characters	
	IP Address	1~254	
	C	Check/Uncheck	Uncheck
	A	Check/Uncheck	Uncheck
Wireless Setting			
Wireless Enable	Check/Uncheck		Check
Network ID(SSID)	A string of maximum 32 characters		default
Channel	1~13		1
Security	Â None Â WEP Â 802.1X Â WPA-PSK Â WPA		None
Advanced Wireless Setting			
Beacon Interval	1~1000 msec		100 msec
RTS Threshold	256~2432 bytes		2432 bytes
Fragmentation Threshold	256~2346 bytes - even numbers only		2346 bytes
DTIM Interval	1~65535 seconds		3 seconds
Wireless Mode	Â 802.11b only Â 802.11g only Â mixed		Mixed
TX Rates	Dropdown List		Auto

Parameter	Range/Options	Default
Preamble Type	Â Short Preamble Â Long Preamble Â Auto	Auto
Authentication Type	Â Open System Â Shared Key Â Both	Both
SSID broadcast	Â Enable Â Disable	Enable
Antenna Transmit Power	Â 100% 17dBM Â 50% 15dBM Â 25% 12dBM Â 12.5% 10dBM	100% 17dBM
Change Password		
Administrator Password	A string of maximum 9 characters	private
User Password	A string of maximum 9 characters	public
Outbound Packet Filter		
Outbound Filter Enable	Check/Uncheck	Uncheck
Outbound Filter Mode	Â Allow all…except Â Deny all…except	Allow all…except
Outbound Rules 1-8	Â Source IP: x.x.x.x Â Source Port: 065535 Â Destination IP: x.x.x.x Â Destination Port: 0~65535 Â Enable Check/Uncheck Â Use Rule#: 1~10	0

Parameter	Range/Options	Default
InBound Packet Filter		
Inbound Filter Enable	Check/Uncheck	Uncheck
Inbound Filter Mode	Â Allow all…except Â Deny all…except	Allow all…except
Inbound Rules 1-8	Â Source IP: x.x.x.x Â Source Port: 0~65535 Â Destination IP: x.x.x.x Â Destination Port: 0~65535 Â Enable Check/Uncheck Â Use Rule#: 1~10	0
URL Blocking		
URL Blocking Enable	Check/Uncheck	Uncheck
URL Rules 1-10	Â URL: A string of maximum 50 characters Â Enable Check/Uncheck Â Use Rule#: 1-10	Uncheck 0
Domain Filter		
Domain Filter Enable	Check/Uncheck	
Log DNS Query Enable	Check/Uncheck	
Privilege IP Addresses Range	Â From:1~254 Â To: 1~254	
Domain Filter Rules 1-10	Â Domain Suffix 1-9 Â Drop Check/Uncheck Â Log Check/Uncheck	Â Uncheck Â Uncheck

Parameter	Range/Options		Default
	Â Enable Check/Uncheck		Â Uncheck
Firewall			
Firewall Rules 1-8	Source Interface	Â All Â LAN Â WAN	All
	Source IP	x.x.x.x	
	Destination Interface	Â All Â LAN Â WAN	All
	Destination IP	x.x.x.x	
	Protocol	Â All Â TCP Â UDP Â ICMP	All
	Destination Port	Â 0~65535	
	Action	Â Allow Â Deny	Allow
	Enable Check/Uncheck		Uncheck
Miscellaneous Items			
Remote Administrator Host	x.x.x.x or x.x.x.x/y		0.0.0.0
Remote Administrator Port	0~65535		88
Enable Remote Administrator	Check/Uncheck		Check
Administrator Time-out	0~9999 sec (0=never)		120
TFTP Access Client	x.x.x.x		0.0.0.0

Parameter	Range/Options		Default
TFTP Access Port	0~65535		69
Enable TFTP Access	Check/Uncheck		Uncheck
Discard PING from WAN side Enable	Check/Uncheck		Check
SPI mode Enable	Check/Uncheck		Uncheck
DoS Attack Detection Enable	Check/Uncheck		Uncheck
Virtual Server			
Virtual Server Rules 1-20	Â Protocol	Â All	All
		Â TCP	
		Â UDP	
	Â Service Ports	Â 0~65535	
	Â Server IP	Â 1~254	
	Â Enable	Â Check/Uncheck	Uncheck
	Â Use Rule#	Â 1~10	0
Special Applications			
Rules 1-10	Â Trigger Port	Â 0~65535	
	Â Incoming Ports	Â A string of max 119 characters	
	Â Enable	Â Check/Uncheck	Uncheck
DMZ Host			
IP Address of DMZ Host	1~254		
	Enable: Check/Uncheck		Uncheck
VPN Pass through			
VPN PPTP Pass-Through Enable	Check/Uncheck		Check

Parameter	Range/Options	Default
VPN IPSec Pass-Through Enable	Check/Uncheck	Check
System Time		
System Time Source	Â Get Date and Time by NTP Protocol Â Set Date and Time using PC's Date and Time Â Set Date and Time Manually	Set Date and Time Manually
Time Server	Â time.nist.gov Â time-nw.nist.gov Â time.windows.com Â utcnist.colorado.edu	time.nist.gov
Time Zone	From dropdown list	GMT-08:00
Date	Â Year: 2002~2020 Â Month: Jan~Dec Â Day: 1~31	Â 2004 Â Aug Â 1
Time	Â Hour: 0~23 Â Minute: 0~59 Â Second: 0~59	Â 0 Â 0 Â 0
Daylight Saving	Â Enable Â Disable	Disable
Daylight Saving Start	Â Month: Jan~Dec Â Day: 1~31 Â Hour: 0~23	Â Jan Â 1 Â 0
Daylight Saving End	Â Month: Jan~Dec Â Day: 1~31 Â Hour: 0~23	Â Jan Â 1 Â 0
System Log		
IP Address of Syslog Server	1~254	

Parameter	Range/Options	Default
Enable IP Address	Check/Uncheck	Uncheck
E-mail Alert Enable	Check/Uncheck	Uncheck
SMTP Server IP/Port	x.x.x.x	
E-mail addresses	A string of maximum 127 characters	
E-mail Subject	A string of maximum 63 characters	
User name	A string of maximum 25 characters	
Password	A string of maximum 25 characters	
Log Type	Â System Activity: Check/Uncheck Â Debug Information: Check/Uncheck Â Attacks: Check/Uncheck Â Dropped Packets: Check/Uncheck Â Notice: Check/Uncheck	Â Uncheck Â Uncheck Â Uncheck Â Uncheck Â Uncheck
Dynamic DNS		
DDNS	Â Disable Â Enable	Disable
Provider	Â DnyDNS.org(Dynamic) Â DnyDNS.org(Custom) Â TZO.com Â dhs.org	DnyDNS.org(Dynamic)
Host Name	A string of maximum 63 characters	
Username/E-mail	A string of maximum 63 characters	
Password/Key	A string of maximum 63 characters	
SNMP Setting		
Enable SNMP	Â Local: Check/Uncheck Â Remote: Check/Uncheck	Â Uncheck Â Check

Parameter	Range/Options	Default
Get Community	A string of maximum 27 characters	Public
Set Community	A string of maximum 27 characters	Private
IP 1-4	x.x.x.x	
SNMP Version	Â V1 Â V2c	V2c
Routing Table		
Dynamic Routing	Â Disable Â RIPv1 Â RIPv2	Disable
Static Routing	Â Disable Â Enable	Disable
Default route	Â WAN Â LAN IP	WAN
Routing Rules 1-8	Â Destination Â Subnet Mask Â Gateway Â Hop Â Enable Check/Uncheck	Uncheck
Schedule Rule		
Schedule Enable	Check/Uncheck	Uncheck
Schedule Rule Setting		
Name of Rule 1-10	A string of maximum 31 characters	
Sunday-Saturday, Every Day	Start Time: hh:mm End Time: hh:mm	
UPnP Setting		
UPnP	Check/Uncheck	Uncheck
Firmware Upgrade		

Parameter	Range/Options	Default
Browse		
DRAP Protocol		
DRAP	Â Disable Â Enable	Disable
DRAP Server IP Address	x.x.x.x	0.0.0.0
Server Port		0
Discovery Time		0
Acknowledge Time		0
Miscellaneous Items		
MAC Address for Wake-on-LAN		
DHCP Client List	From dropdown list	
Domain Name or IP address for Ping Test		

A

Appendix A - Print Server

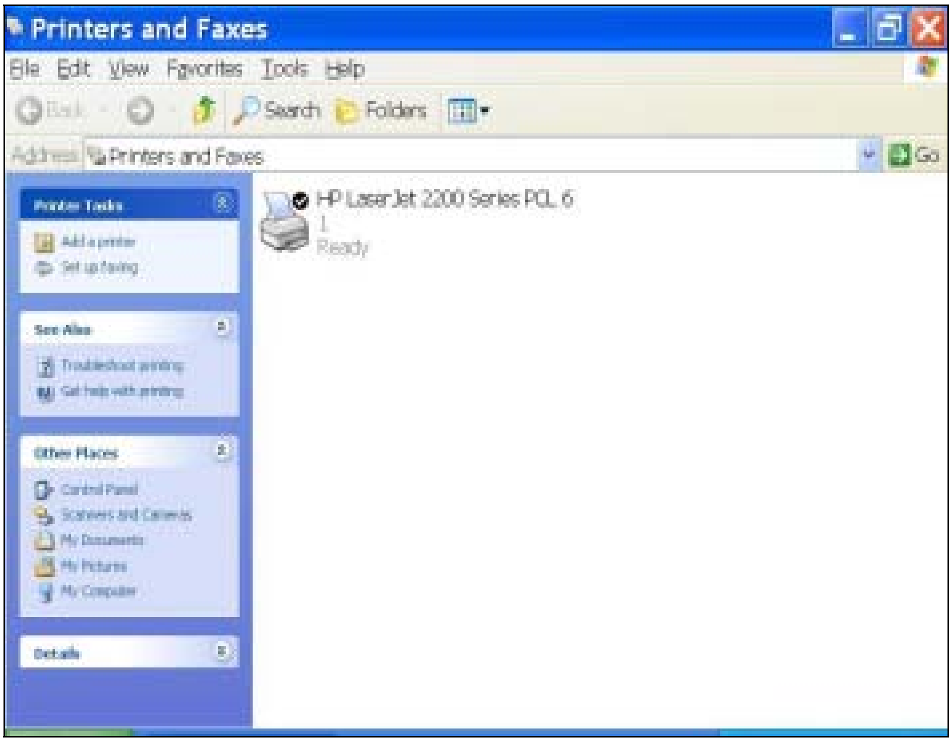
This Networking Gateway provides the function of network print server for MS Windows 2000/XP and Unix based platforms. The device comes with a USB port for connecting the printer. This Appendix will guide you through configuring the Print Server.

A.1 Configuring on Windows 2000 and XP Platforms

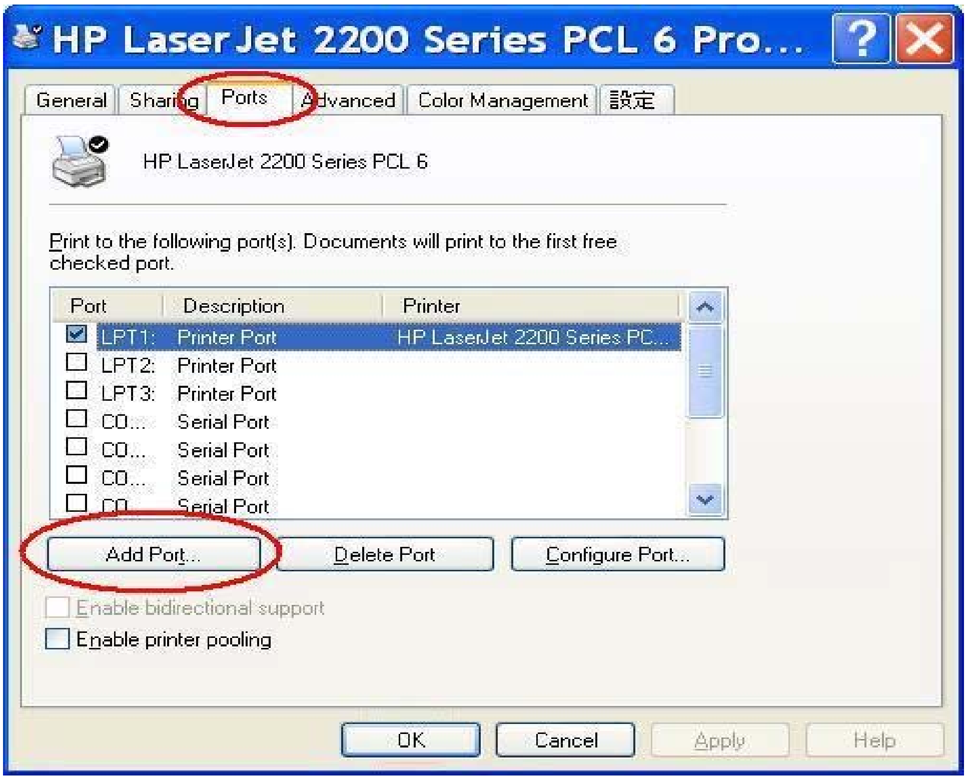
Windows 2000 and XP have a built-in LPR client, that can be used for printing.

Your Printer Driver must be installed in LPT1 or other ports before you proceed to the following procedure.

1 Open Printers and Faxes.



2 Select the printer. Right Click on it, a quick menu appears. Select Properties from the menu.



HP LaserJet 2200 Series PCL 6

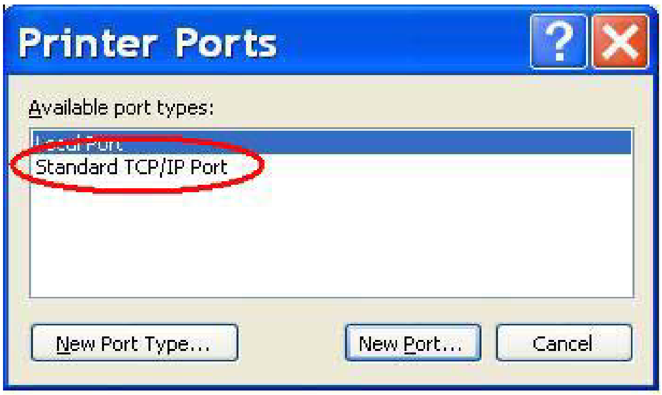
Print to the following port(s). Documents will print to the first free checked port.

Port	Description	Printer
☑ LPT1:	Printer Port	HP LaserJet 2200 Series PC...
□ LPT2:	Printer Port	
□ LPT3:	Printer Port	
□ CO...	Serial Port	
□ CO...	Serial Port	
□ CO...	Serial Port	
□ CO...	Serial Port	

□ Enable bidirectional support

□ Enable printer pooling

3 Select the Ports tab, Click "Add Port..."



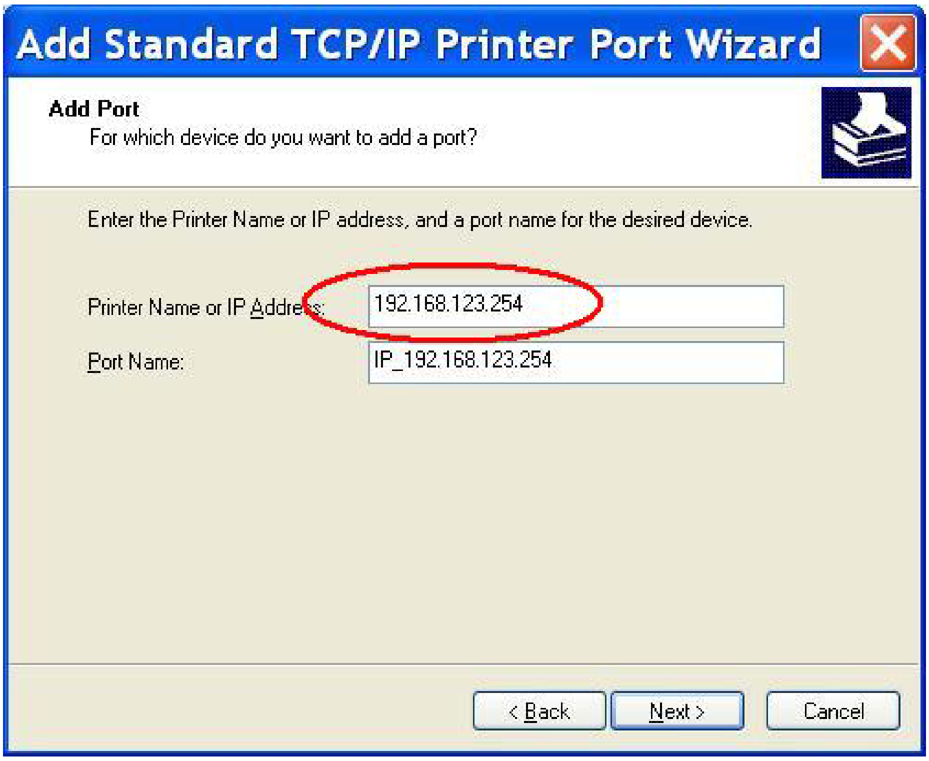
Available port types:

Local Port

Standard TCP/IP Port

4 Select "Standard TCP/IP Port", and then click "New Port..." The TCP/IP Printer Port Wizard appears.

5 Click Next. The Add Port window is displayed.



Add Standard TCP/IP Printer Port Wizard
Add Port
For which device do you want to add a port?
< Back
Next >
Cancel

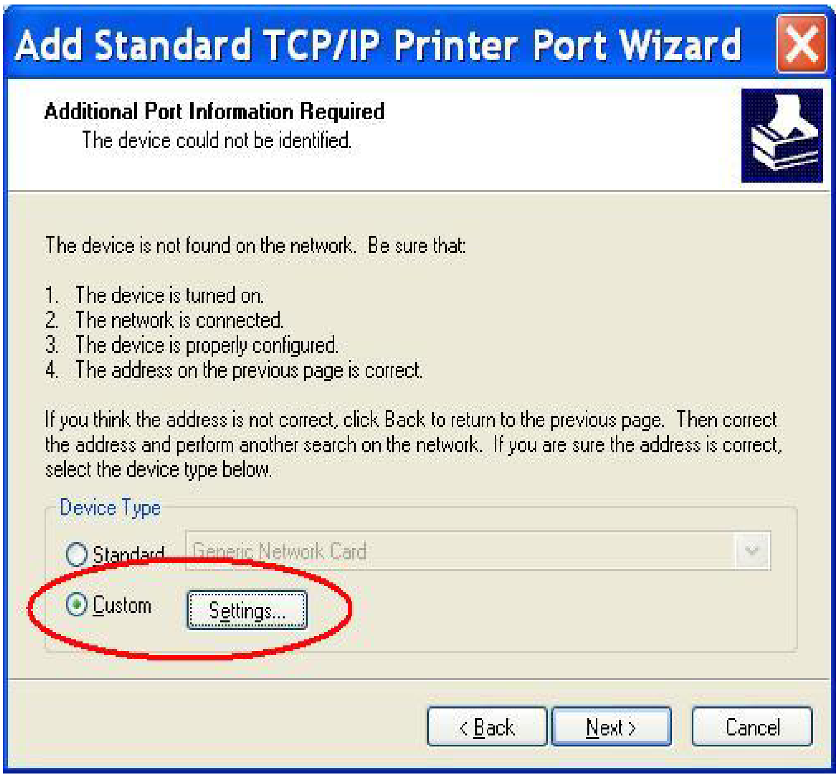
Enter the Printer Name or IP address, and a port name for the desired device.

Printer Name or IP Address: 192.168.123.254

Port Name: IP_192.168.123.254

6 Enter the IP address of the Networking Gateway device: 192.168.254.253 in the Printer Name or IP Address field. The Port Name field is automatically filled in as you type. You can change it as required.

7 Click Next. The Additional Port Information Required window appears.



Add Standard TCP/IP Printer Port Wizard

Additional Port Information Required

The device could not be identified.

The device is not found on the network. Be sure that:

1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.

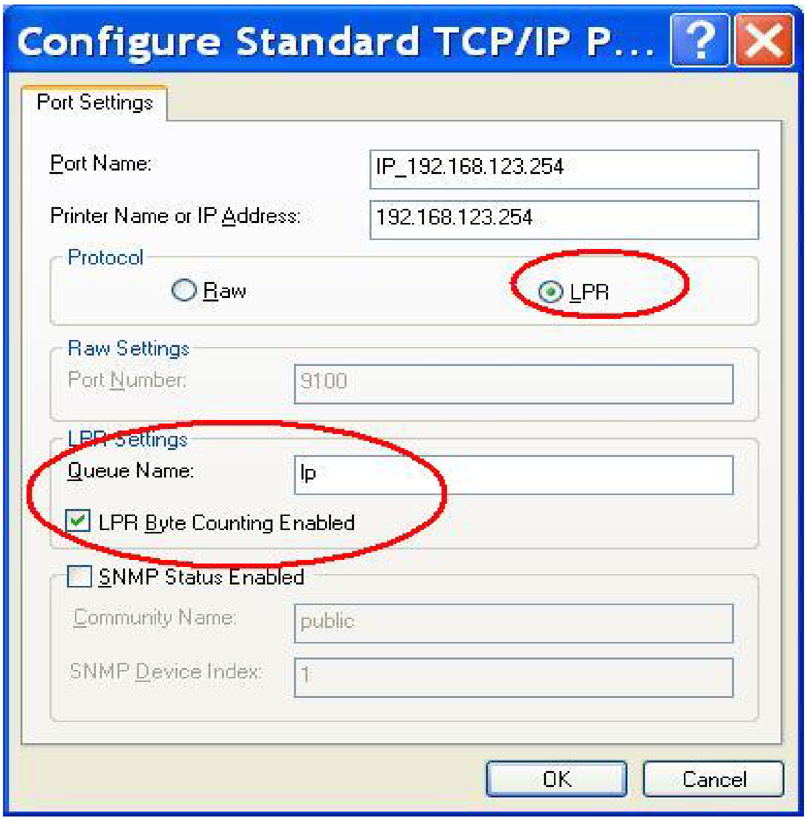
If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.

Device Type

○ Standard Generic Network Card

● Custom Settings...

8 Select Custom, and then click "Settings..." The Port Settings window is displayed.



Port Name: IP_192.168.123.254

Printer Name or IP Address: 192.168.123.254

Protocol

○ Raw ● LPR

Raw Settings

Port Number: 9100

LPR Settings

Queue Name: lp

☑ LPR Byte Counting Enabled

☐ SNMP Status Enabled

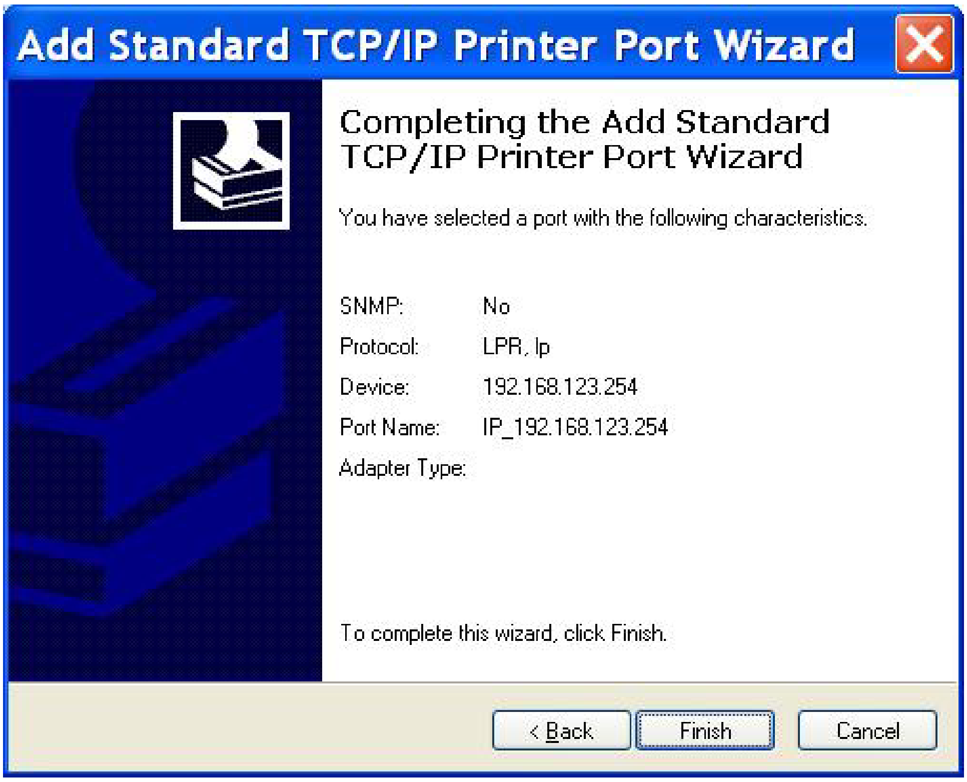
Community Name: public

SNMP Device Index: 1

9 In the Protocol field, select “LPR”. Enter ***lp*** (lowercase letters) in the “Queue Name” field and check the “LPR Byte Counting Enabled” check box.

10 Click OK to apply your settings. The Port Settings window closes and the Additional Port Information Required window reappears.

11 Click Next. The following window is displayed.



Completing the Add Standard TCP/IP Printer Port Wizard

You have selected a port with the following characteristics.

SNMP: No

Protocol: LPR, lp

Device: 192.168.123.254

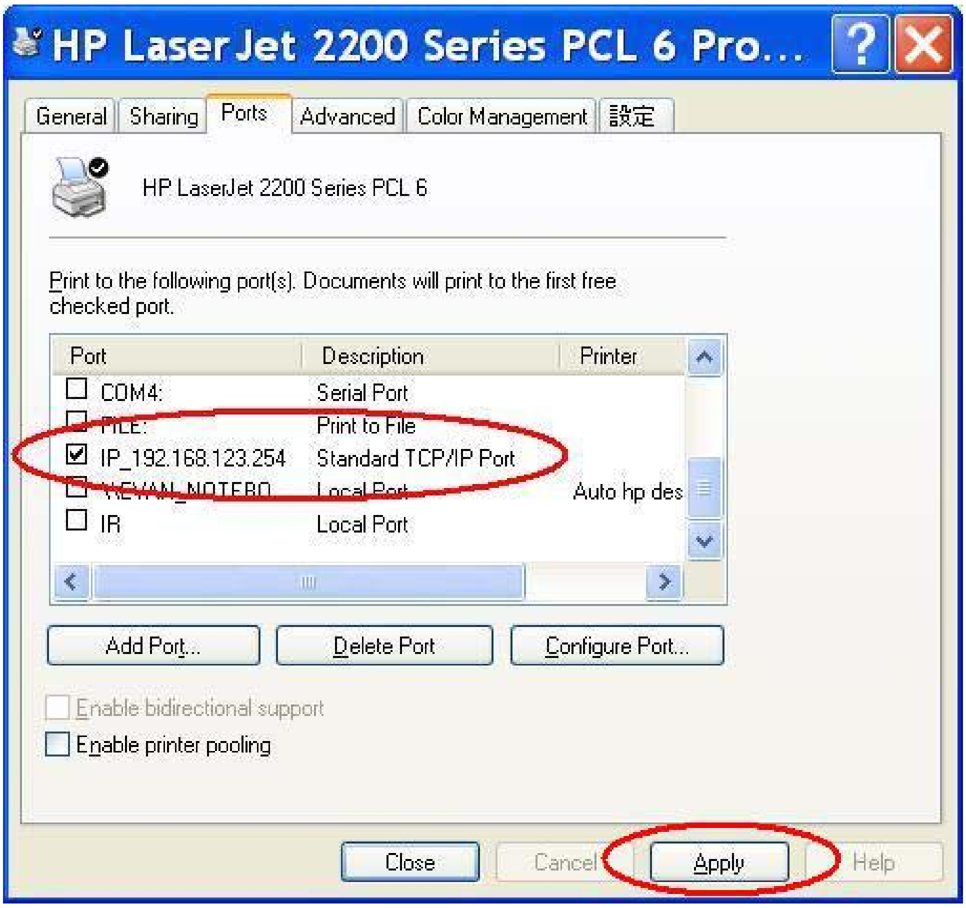
Port Name: IP_192.168.123.254

Adapter Type:

To complete this wizard, click Finish.

12 Click Finish. The window closes.

13 Close the Printer Ports window. The new printer port appears in the Ports tab.



HP LaserJet 2200 Series PCL 6

Print to the following port(s). Documents will print to the first free checked port.

	Port	Description	Printer
□	COM4:	Serial Port	
□	FILE:	Print to File	
☑	IP_192.168.123.254	Standard TCP/IP Port	
□	\\KEVAN_NOTEBO	Local Port	Auto hp des
□	IR	Local Port	

□ Enable bidirectional support

□ Enable printer pooling

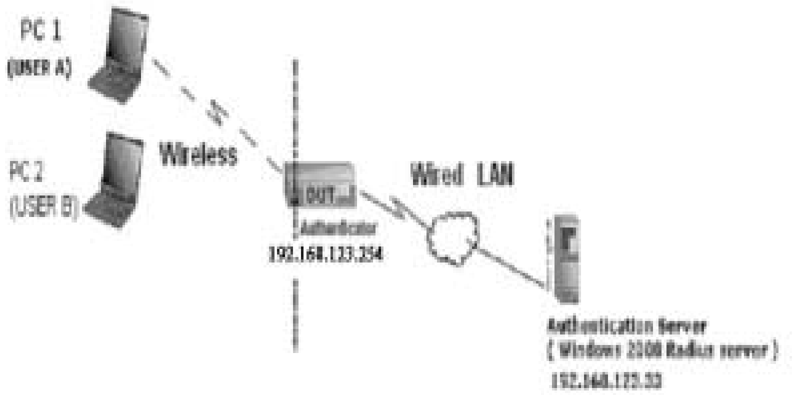
14 Click Apply and then OK to close the window.

NOTE

Print a test page to ensure that the printer is working properly.

B

Appendix B - 802.1x Setting



Testing Environment (Use Windows 2000 Radius Server)

Â Equipment Details

Ï PC1:
Microsoft Windows XP Professional without Service Pack 1.
D-Link DWL-650+ wireless LAN adapter
Driver version: 3.0.5.0 (Driver date: 03.05.2003)

Ï PC2:
Microsoft Windows XP Professional with Service Pack 1a.
Z-Com XI-725 wireless LAN USB adapter
Driver version: 1.7.29.0 (Driver date: 10.20.2001)

Ï Authentication Server: Windows 2000 RADIUS server with Service Pack 3 and HotFix Q313664.

NOTE

Windows 2000 RADIUS server only supports PEAP upgraded to service pack 3 and HotFix Q313664 (For additional information, see http://support.microsoft.com/default.aspx?scid=kb; en-us;313664)

Â DUT

Ï Configuration:

ü Enable DHCP server.

ü WAN setting: static IP address.

ü LAN IP address: 192.168.123.254/24.

ü Set RADIUS server IP.

ü Set RADIUS server shared key.

ü Configure WEP key and 802.1X setting.

The following test uses the inbuilt 802.1X authentication method such as, EAP_TLS, PEAP_CHAPv2 (Windows XP with SP1 only), and PEAP_TLS (Windows XP with SP1 only) using the Smart Card or other Certificate of the Windows XP Professional.

Â DUT and Windows 2000 Radius Server Setup

Ï Setup Windows 2000 RADIUS Server

Change authentication method to MD5_Challenge or using smart card or other certificate on RADIUS server according to the test condition.

Ï Setup DUT

1 Enable the 802.1X (check the "Enable checkbox").

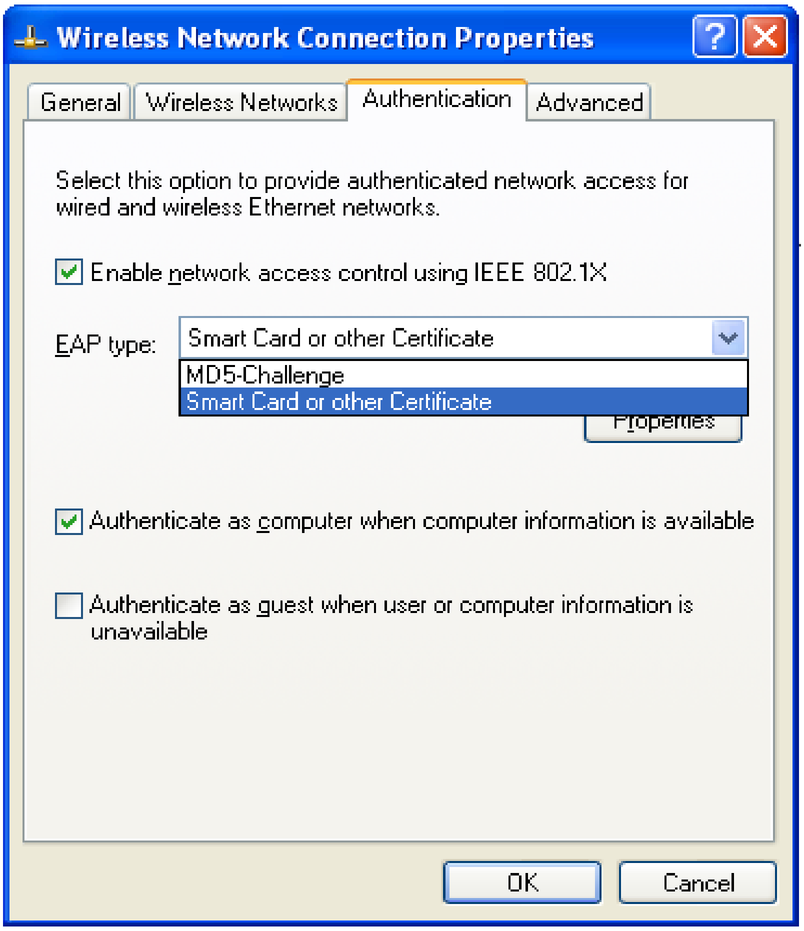
2 Enter the RADIUS server IP.

3 Enter the shared key. (The key shared by the RADIUS server and DUT).

4 Change 802.1X encryption key length to fit the variable test condition.

Ï Setup Network adapter on PC

1 Select the IEEE802.1X as the authentication method.



Wireless Network Connection Properties

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

☑ Enable network access control using IEEE 802.1X

EAP type: Smart Card or other Certificate

- MD5-Challenge
- Smart Card or other Certificate

☑ Authenticate as computer when computer information is available

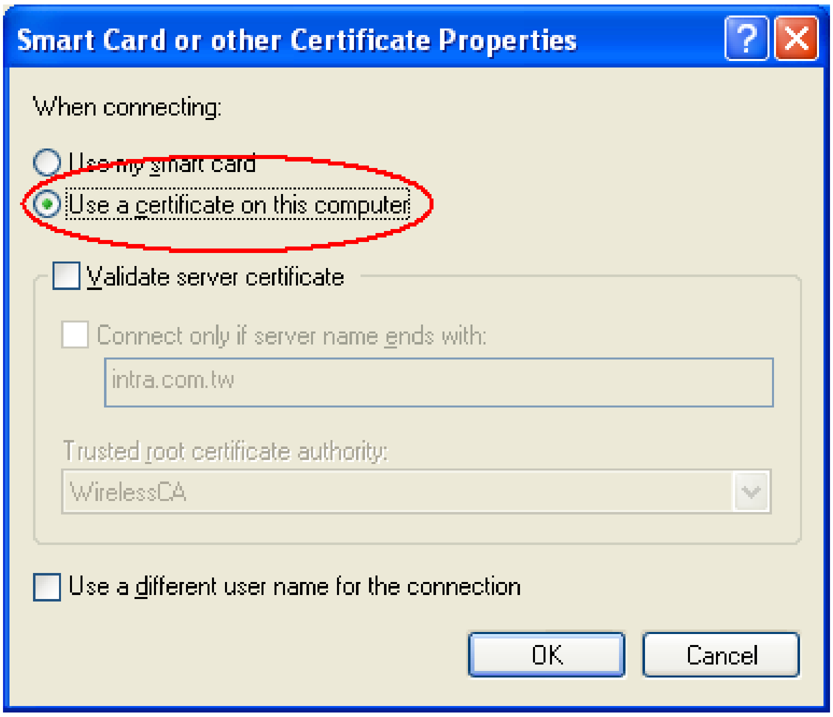
□ Authenticate as guest when user or computer information is unavailable

NOTE

The above figure shows a setting of Windows XP without service pack 1. If users upgrade to service pack 1, they will not see MD5-Challenge in the EAP type list, but they will receive a new Protected EAP (PEAP) option.

2 Select MD5-Challenge or Smart Card or other Certificate as the EAP type

3 If use smart card or the certificate is selected as the EAP type, select to use a certificate on this computer.



Smart Card or other Certificate Properties

When connecting:

○ Use my smart card

● Use a certificate on this computer

□ Validate server certificate

□ Connect only if server name ends with:

intra.com.tw

Trusted root certificate authority:

WirelessCA

□ Use a different user name for the connection

4 Change EAP type to fit the variable test condition.

Â Windows 2000 RADIUS server Authentication testing:

Ï DUT authenticate PC1 using certificate. (PC2 follows the same test procedures.)

1 Download and install the certificate on PC1. (Fig 4)

2 PC1 choose the SSID of DUT as the Access Point.

3 Set authentication type of wireless client and RADIUS server both to EAP_TLS.

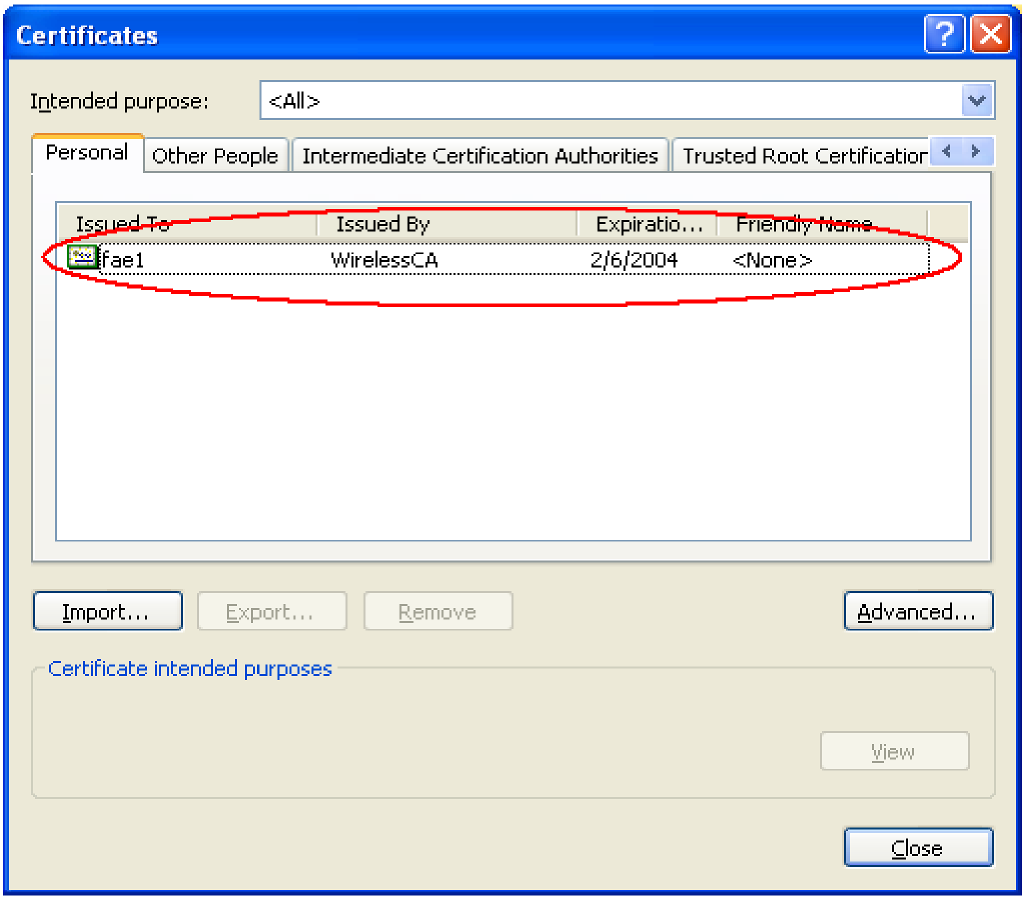
4 Disable the wireless connection and enable again.

5 The DUT will send the user's certificate to the RADIUS server, and then

6 send the message of authentication result to PC1. (Fig 5)

7 Windows XP will prompt that the authentication process is success or fail and end the authentication procedure. (Fig 6)

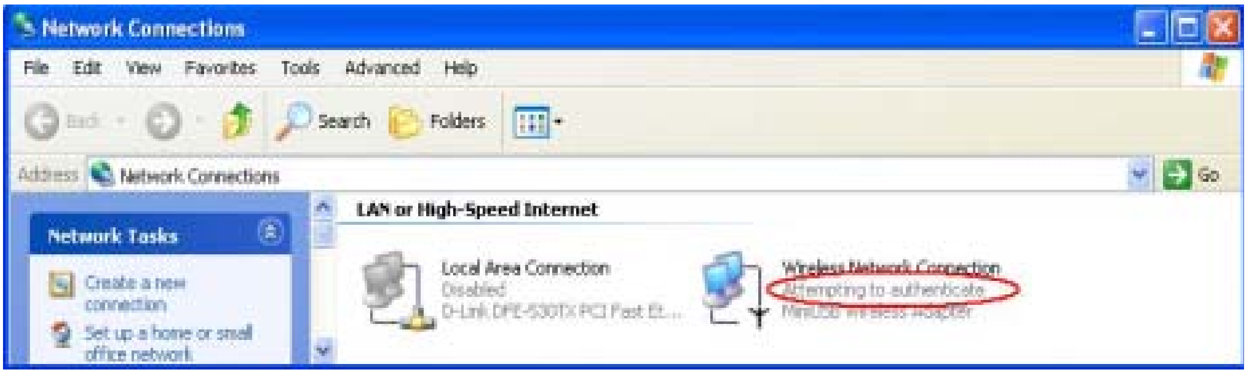
8 Terminate the test steps when PC1 get dynamic IP and PING remote host successfully.



Certificates
Intended purpose:
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certificatior
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close

Intended purpose: <All>

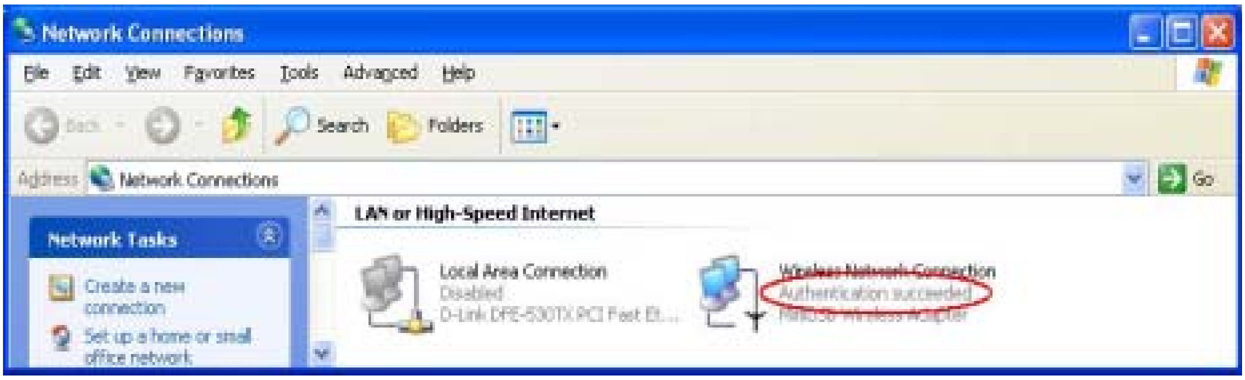
Issued To	Issued By	Expiratio...	Friendly Name
fae1	WirelessCA	2/6/2004	<None>



LAN or High-Speed Internet

Local Area Connection
Disabled
D-Link DFE-530TX PCI Fast Et...

Wireless Network Connection
Attempting to authenticate
MiniUSB Wireless Adapter



LAN or High-Speed Internet

Local Area Connection
Disabled
D-Link DFE-530TX PCI Fast Et...

Wireless Network Connection
Authentication succeeded
[illegible] Wireless Adapter

Ï DUT authenticate PC2 using PEAP-TLS.

1 PC2 choose the SSID of DUT as the Access Point.

2 Set authentication type of wireless client and RADIUS server both to PEAP_TLS.

3 Disable the wireless connection and enable again.

4 The DUT will send the user's certificate to the RADIUS server, and then send the message of authentication result to PC2.

5 Windows XP will prompt that the authentication process is success or fail and end the authentication procedure.

6 Terminate the test steps when PC2 get dynamic IP and PING remote host successfully.

Â Support Type: The router supports the types of 802.1x Authentication:

PEAP-CHAPv2 and PEAP-TLS.

NOTE

Â PC1 is on Windows XP platform without Service Pack 1.

Â PC2 is on Windows XP platform with Service Pack 1a.

Â PEAP is supported on Windows XP with Service Pack 1 only.

Â Windows XP with Service Pack 1 allows 802.1x authentication only when data encryption function is enable.

Glossary

DHCP Dynamic Host Configuration Protocol. A protocol for dynamically assigning IP addresses from a pre-defined list to nodes on a network. Using DHCP to manage IP addresses simplifies client configuration and efficiently utilizes IP addresses.

DNS Domain Name System: The name resolution system that lets users locate computers on the Internet (TCP/IP network) by domain name. The DNS server maintains a database of domain names (host names) and their corresponding IP addresses.

DRAP Dynamic Resource Allocation Protocol

IDU Indoor Unit

IEEE Institute of Electrical and Electronics Engineers. IEEE (pronounced I-triple-E) is an organization composed of engineers, scientists, and students. The IEEE is best known for developing standards for the computer and electronics industry. In particular, the IEEE 802 standards for local-area networks are widely followed.

IEEE 802.11b The standard applies to wireless LANs and provides data rate of 11 Mbps in the 2.4 GHz band.

IEEE 802.11g The standard applies to wireless LANs and provides data rate of 54 Mbps in the 2.4 GHz band.

IP Internet Protocol. The standard that defines how data is transmitted over the Internet. IP bundles data, including e-mail, faxes, voice calls and messages, and other types, into "packets", in order to transmit it over public and private networks.

LAN Local area Network. A computer network limited to a small geographical area, such as a single building. The network typically links PCs as well as shared resources such as printers.

MAC Media Access Control. The lower of the two sub-layers of the data link layer defined by the IEEE. The MAC sub-layer handles access to shared media, such as whether token passing or contention will be used.

MAC Address Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6bytes long and are controlled by the IEEE.

NAT Network Address Translation: An IETF standard that allows an organization to present itself to the Internet with far fewer IP addresses than there are nodes on its internal network. The NAT technology, which is typically implemented in a router, converts private IP addresses (such as in the 192.168.0.0 range) of the machine on the internal private network to one or more public IP addresses for the Internet. It changes the packet headers to the new address and keeps track of each session. When packets come back from the Internet, NAT performs the reverse conversion to the IP address of the client machine.

ODU Outdoor unit

PPPoE Point-to-Point Protocol over Ethernet. PPPoE relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet share a common connection, so the Ethernet principles supporting multiple users in a LAN combines with the principles of PPP, which apply to serial connections.

SNMP Simple Network Management Protocol. A network management protocol that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

SU Subscriber Unit

TCP/IP Transmission Control Protocol/Internet Protocol. A set of protocols developed by the U.S. Department of Defense to allow communication between dissimilar networks and systems over long distances. TCP/IP is the de facto standard for data transmission over networks, including the Internet.

TFTP Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication.

UDP User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

WAN Wide Area Network. A computer network that spans a relatively large geographical area. Wide area networks can be made up of interconnected smaller networks spread throughout a building, a state, or the entire globe.