W1310R

User’s Manual

Version 1.00

FCC CAUTION

This equipment has been tested and proven to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

---Reorient or relocate the receiving antenna.

---Increase the separation between the equipment and receiver.

---Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

---Consult the dealer or an experienced radio/TV technician for help.

Installation and use of this Wireless AP/ Router must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications (including the antennas) made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, or the substitution of the connecting cables and equipment other than manufacturer specified. It is the responsibility of the user to correct any interference caused by such unauthorized modification, substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

The device contains a low power transmitter which will send out Radio Frequency (RF) signal when transmitting. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

CE CAUTION

European standards dictate maximum radiated transmit power of 100mW EIRP and frequency range 2.400-2.4835 GHz; In France, the equipment must be restricted to the 2.4465-2.4835 GHz frequency range and must be restricted to indoor use.

For the following equipment: Wireless AP/ Router

CE ⓘ Is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility (89/336/EEC), Low-voltage Directive (73/23/EEC) and the Amendment Directive (93/68/EEC), the procedures given in European Council Directive 99/5/EC and 89/3360EEC.
The equipment was passed. The test was performed according to the following European standards:

- EN 300 328 V1.6.1 (**2004**)
- EN 301 489-17/-1 V.1.2.1/V1.4.1 (**2002**)
- EN 50371: 2002
- EN 60950-1: 2001

Table of Contents

1. Before You Start

1.1 Preface

This manual is for Hotspot owners or administrators in enterprises to set up network environment using W1310R. It contains step by step procedures and graphic examples to guide MIS staff or individuals with slight network system knowledge to complete the installation.

1.2 Document Conventions

- For any caution or warning that requires special attention of readers, a highlight box with the eye-catching italic font is used as below:

Warning: *For security purposes, you should immediately change the Administrator’s password.*

🏠 Indicates that clicking this button will return to the homepage of this section.

⬆ Indicates that clicking this button will return to the previous page.

✓ Apply Indicates that clicking this button will apply all of your settings.

✕ Clear Indicates that clicking this button will clear what you set before these settings are applied.

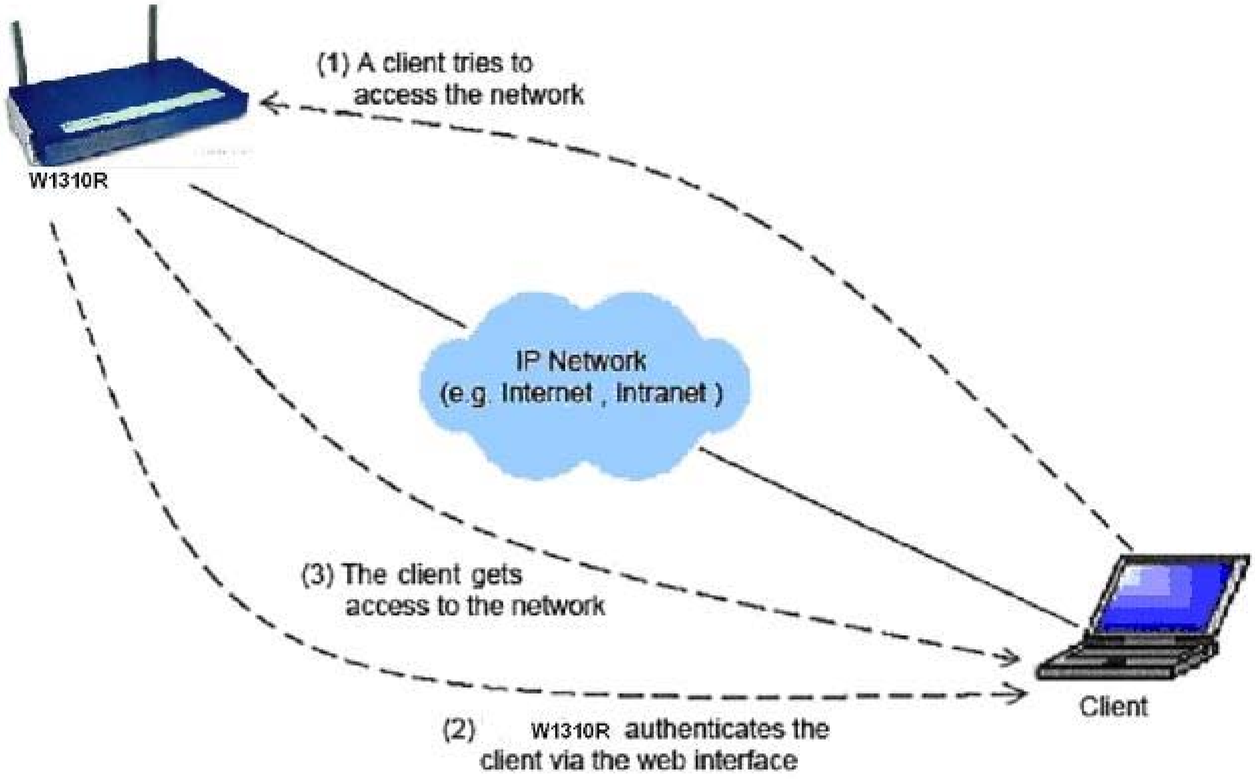
2. System Overview

2.1 Introduction of W1310R

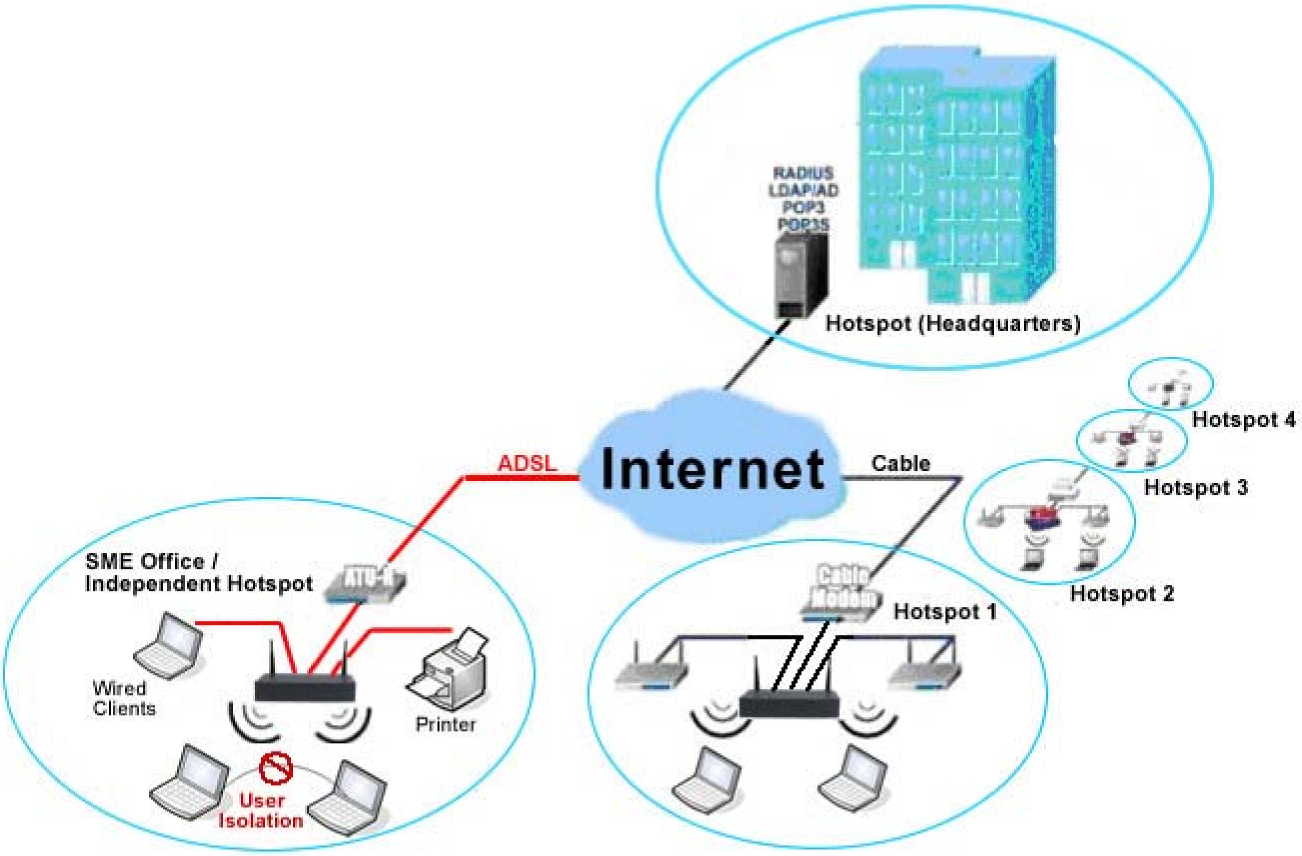
W1310R is an all-in-one product specially designed for small wireless network environment. It integrates **“Access Control”** and **“Wireless Network Access”** into one system to fulfill the needs in Hotspot environment. W1310R supports 802.11b and 802.11g dual wireless transmission modes and at the same time incorporates **“convenience,” “efficiency,”** and **“friendliness”** for services.

2.2 System Concept

W1310R is specially designed for user authentication, authorization and management. The user account information is stored in the local database or a specified external databases server. The user authentication is processed via the SSL encrypted web interface. This interface is compatible to most desktop devices and palm computers. The following figure is an example of W1310R set to control a part of the company's intranet. The whole managed network includes the cable network users and the wireless network users.


W1310R
(1) A client tries to access the network
IP Network (e.g. Internet , Intranet)
(3) The client gets access to the network
Client
(2) W1310R authenticates the client via the web interface

The users located at the managed network will be unable to access the network resource without permission. When the browser of a user attempts to connect to a website, the W1310R will force the browser to redirect to the user login webpage. The user must enter the username and password for authentication. After the identity is authenticated successfully, the user will gain proper access right defined on the W1310R.



2.3 Specification

2.3.1 Hardware Specification

- Dimensions: 243mm(W) x 150mm(D) x 45.5mm(H)
- Weight: 1.4 kg
- Power: DC12V/1A 5.5Φ
- Operating Temperature: 5-45°C
- Fast Ethernet RJ 45 Connectors
- Console Port
- Supports 10/100Mbps Full / Half Duplex Transfer Speed

2.3.2 Technical Specification

- **Standards**

  This system supports IEEE 802.1x, 802.11b and 802.11g
- **Networking**

  WAN interface supports Static IP, DHCP client, and PPPoE client

  Interface supports static IP

Supports NAT mode and router mode

Built-in DHCP server

Built-in NTP client

Supports Redirect of network data

Supports IPSec (ESP), PPTP and H.323 pass through (under NAT)

Customizable static routing table

Supports Virtual Server

Supports DMZ Server

Supports machine operation status monitoring and reporting system

- **Firewall**

Provides Several DoS protection mechanisms

Customizable packet filtering rules

Customizable walled garden (free surfing area)

- **User Management**

Supports up to 500 local users.

Supports Local, POP3 (+SSL), RADIUS, and LDAP LAN1/LAN2 mechanisms

Supports LAN1& LAN2 mechanisms simultaneously

Can choose MAC address locking for built-in user database

Can set the time for the user to log in to the system

Can set the user's idle time

Can specify the MAC addresses to enter the managed network without authentication

Can specify the IP addresses to enter the managed network without authentication

Supports the setting to pass or block all the connections when the WAN interface failed

Supports web-based login

Supports several friendly logout methods

Supports RADIUS accounting protocol to generate the billing record on RADIUS server

- **Administration**

Provides online status monitoring and history traffic

Supports SSL encrypted web administration interface and user login interface

Customizable user login & logout web interface

Customizable redirect after users are successfully authenticated during login & logout

Supports Console management interface

Supports SSH remote administration interface

Supports web-based administration interface

Supports SNMP v2

Supports user's bandwidth restriction

Supports remote firmware upgrade

- **Accounting**

Supports built-in user database and RADIUS accounting

3. Base Installation

3.1 Hardware Installation

3.1.1 System Requirements

- Standard 10/100BaseT including five network cables with RJ-45 connectors
- All PCs need to install the TCP/IP network protocol

3.1.2 Package Contents

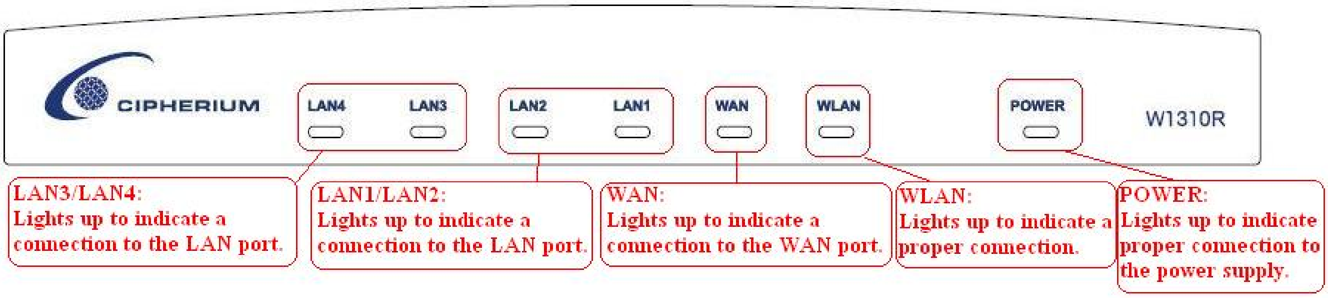
The standard package of W1310R includes:

- W1310R x 1
- CD-ROM x 1
- Quick Installation Guide x 1
- Power Adaptor (DC 12V) x 1
- Cross Over Ethernet Cable x 1
- Console Cable x 1
- 2dbi Omni-antenna x 2

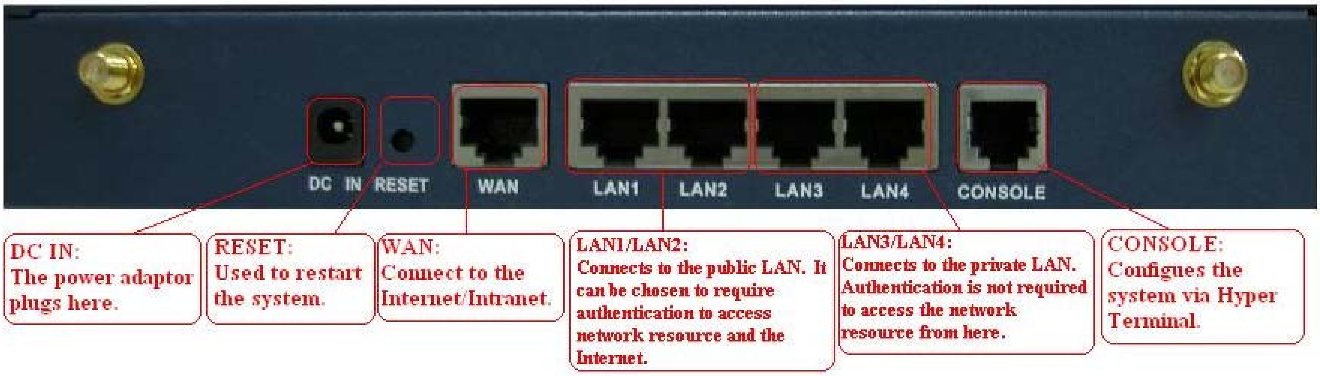
Warning: *It is highly recommended to use all the supplies in the package instead of substituting any components by other suppliers to guarantee best performance.*

3.1.3 Panel Function Descriptions

Front Panel


CIPHERIUM
LAN4
LAN3
LAN2
LAN1
WAN
WLAN
POWER
W1310R
LAN3/LAN4: Lights up to indicate a connection to the LAN port.
LAN1/LAN2: Lights up to indicate a connection to the LAN port.
WAN: Lights up to indicate a connection to the WAN port.
WLAN: Lights up to indicate a proper connection.
POWER: Lights up to indicate proper connection to the power supply.

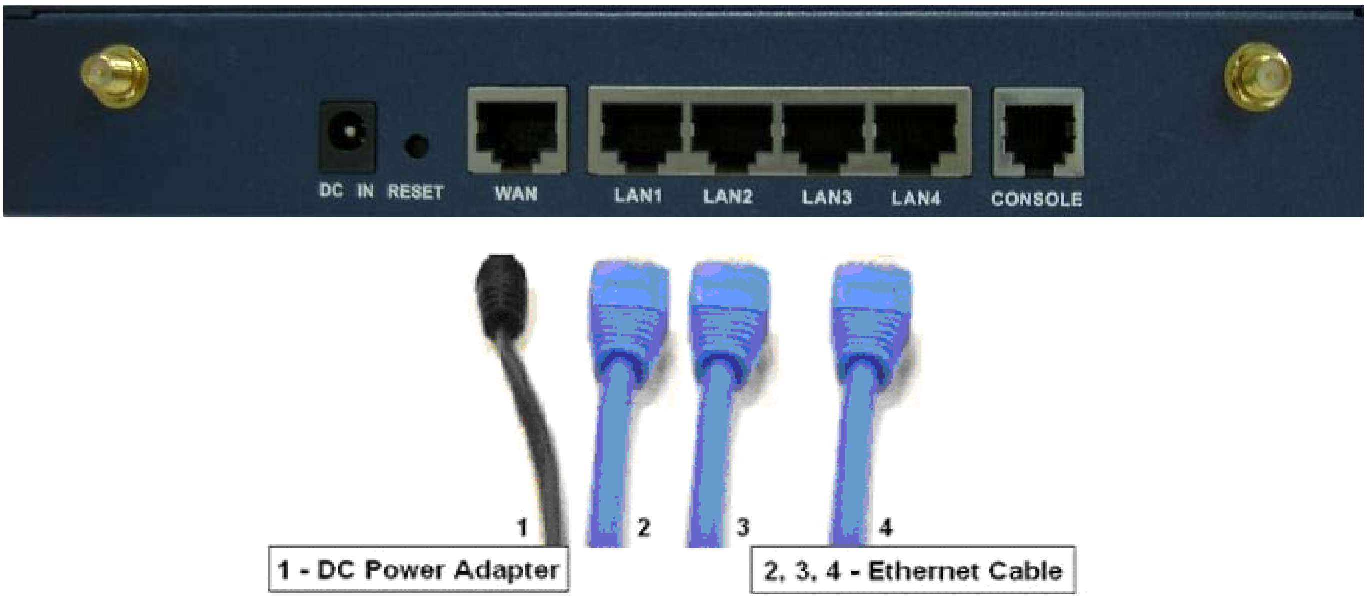
Rear Panel


DC IN
RESET
WAN
LAN1
LAN2
LAN3
LAN4
CONSOLE
DC IN: The power adaptor plugs here.
RESET: Used to restart the system.
WAN: Connect to the Internet/Intranet.
LAN1/LAN2: Connects to the public LAN. It can be chosen to require authentication to access network resource and the Internet.
LAN3/LAN4: Connects to the private LAN. Authentication is not required to access the network resource from here.
CONSOLE: Configues the system via Hyper Terminal.

- **DC IN:** The power adaptor attaches here.
- **RESET:** Press this button to restart the system.
- **WAN:** The WAN port is used to connect to a network which is not managed by the W1310R system, and this port can be used to connect the ATU-Router of ADSL, the port of Cable Modem, or the Switch or Hub on the LAN of a company.
- **LAN1/LAN2:** The two LAN ports are connected to the managed network or WLAN. They can be selected to require or not require authentication to access network resources and Internet.
- **LAN3/LAN4:** The two LAN ports are connected to a trustful network where the users can always use the network resources without authentication. This port can be connected to a server such as File Server or a Database Server, etc.
- **Console:** The system can be configured via HyperTerminal. For example, if you need to set the Administrator's Password, you can connect a PC to this port as a Console Serial Port via a terminal connection program (such as the super terminal with the parameters of 9600, 8, N, 1, None flow control) to change the Administrator's Password.

3.1.4 Installation Steps

Please follow the following steps to install W1310R:



1. Connect the DC power adapter to the power connector socket on the rear panel. The Power LED should be on to indicate a proper connection.
2. Connect an Ethernet cable to the WAN Port on the rear panel. Connect the other end of the Ethernet cable to ADSL modem, cable modem or a switch/hub of the internal network. The LED of this WAN port should be on to indicate a proper connection.
3. Connect an Ethernet cable to the LAN1/LAN2 Port on the rear panel. Connect the other end of the Ethernet cable to an AP or switch. The LED of LAN1/LAN2 should be on to indicate a proper connection. (Note: Authentication is required for the users to access the network via these LAN Ports. The LAN port with authentication function is referred to as ***Public LAN***.)
4. Connect an Ethernet cable to the LAN3/LAN4 Port on the rear panel. Connect the other end of the Ethernet cable to a client's PC. The LED of LAN3/LAN4 should be on to indicate a proper connection. (Note: No authentication is required for the users to access the network via these LAN Ports. The LAN port without authentication function is referred to as ***Private LAN*** and the administrator can enter the administrative user interface to perform configurations via Private LAN.)

Attention: *W1310R supports Auto Sensing MDI/MDIX. You may also use either straight through or cross over cable to connect the Ethernet Port.*

After the hardware of W1310R is installed completely, the system is ready to be configured in the following sections. The manual will guide you step by step to set up the system using a single W1310R to manage the network.

3.2 Software Configuration

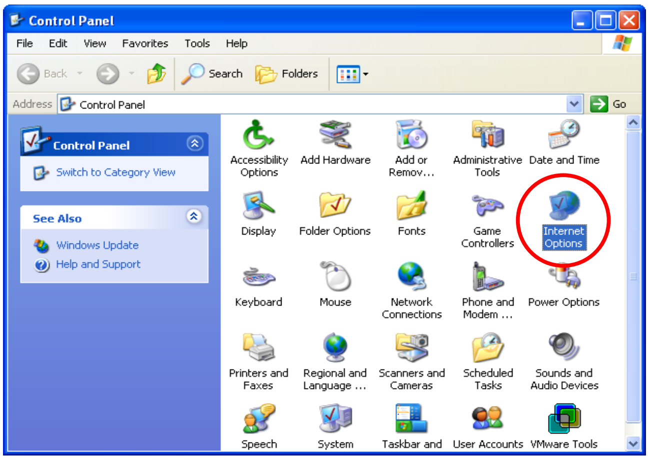
3.2.1 Network Configuration on PC

After W1310R is installed, the following configurations must be set up on the PC: **Internet Connection Setup** and **TCP/IP Network Setup**.

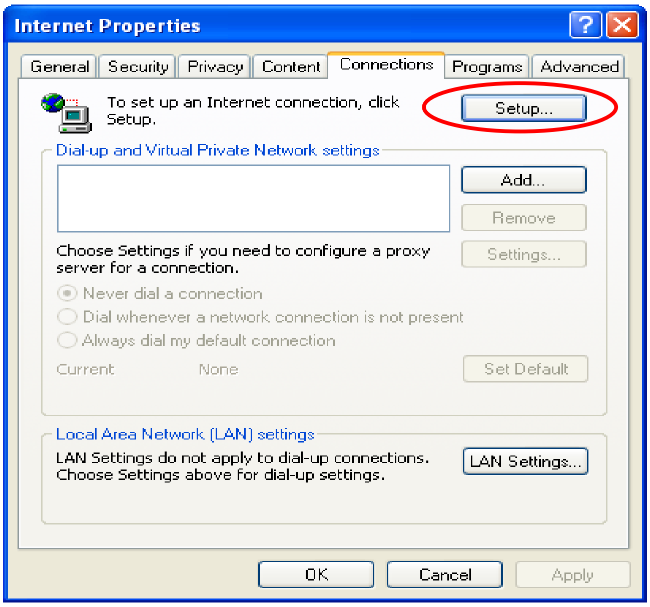
- **Internet Connection Setup**

◆ **Windows XP**

1. Choose **Start** > **Control Panel** > **Internet Option**.



2. Choose the **"Connections"** label, and then click ***Setup***.



To set up an Internet connection, click Setup.

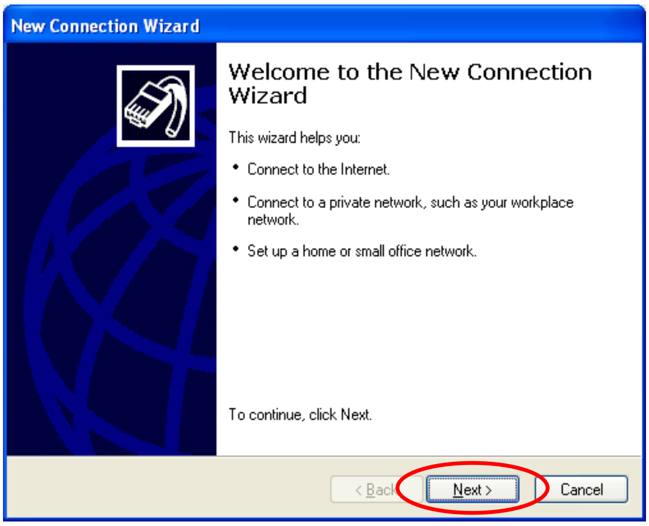
Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection
○ Dial whenever a network connection is not present
○ Always dial my default connection

Current None

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

3. Click ***Next*** when **Welcome to the New Connection Wizard** screen appears.



New Connection Wizard

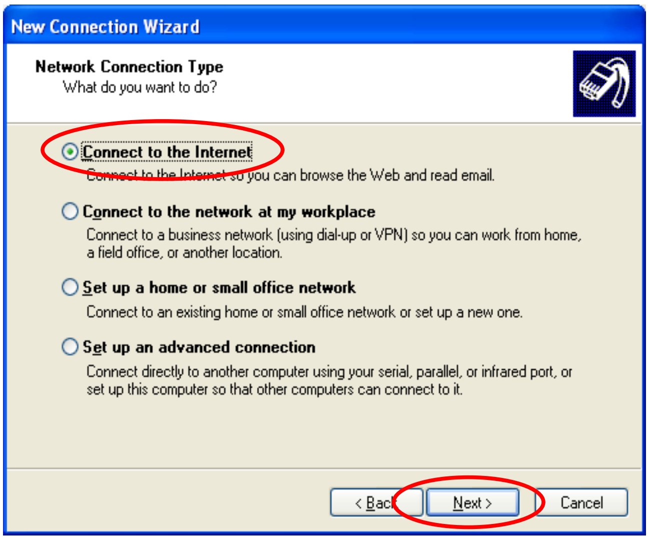
Welcome to the New Connection Wizard

This wizard helps you:

- Connect to the Internet.
- Connect to a private network, such as your workplace network.
- Set up a home or small office network.

To continue, click Next.

4. Choose **"Connect to the Internet"** and then click ***Next***.



New Connection Wizard

Network Connection Type
What do you want to do?

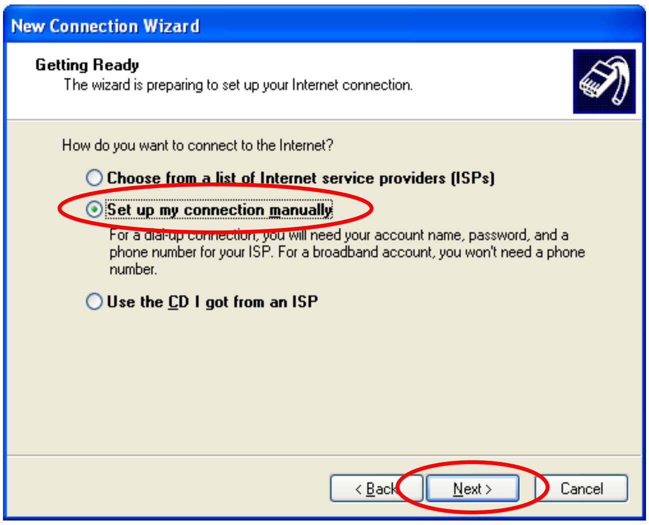
● **Connect to the Internet**
Connect to the Internet so you can browse the Web and read email.

○ **Connect to the network at my workplace**
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

○ **Set up a home or small office network**
Connect to an existing home or small office network or set up a new one.

○ **Set up an advanced connection**
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

5. Choose **"Set up my connection manually"** and then click ***Next***.



New Connection Wizard

Getting Ready
The wizard is preparing to set up your Internet connection.

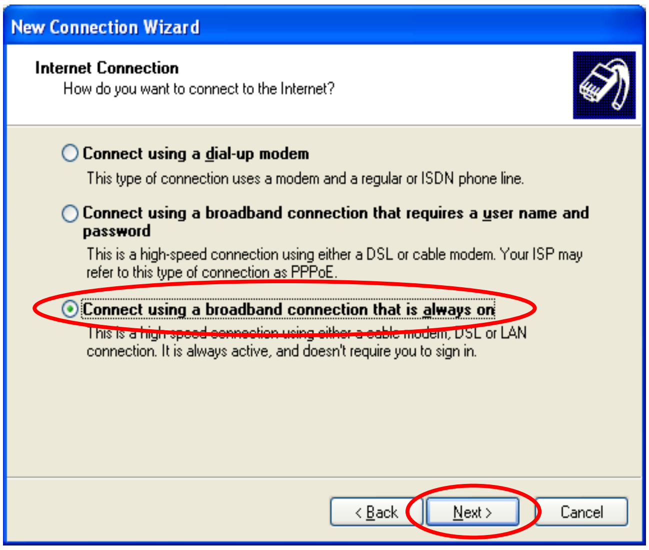
How do you want to connect to the Internet?

○ **Choose from a list of Internet service providers (ISPs)**

● **Set up my connection manually**
For a dial-up connection, you will need your account name, password, and a phone number for your ISP. For a broadband account, you won't need a phone number.

○ **Use the CD I got from an ISP**

6. Choose **"Connect using a broadband connection that is always on"** and then click ***Next***.



New Connection Wizard

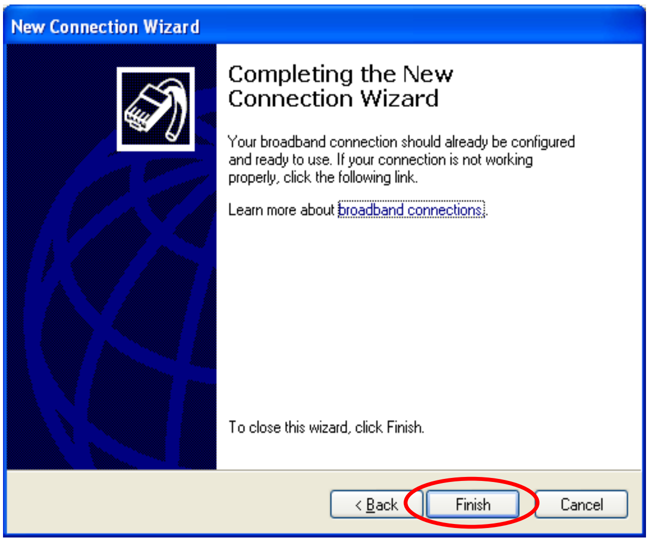
Internet Connection
How do you want to connect to the Internet?

○ Connect using a dial-up modem
This type of connection uses a modem and a regular or ISDN phone line.

○ Connect using a broadband connection that requires a user name and password
This is a high-speed connection using either a DSL or cable modem. Your ISP may refer to this type of connection as PPPoE.

● Connect using a broadband connection that is always on
This is a high-speed connection using either a cable modem, DSL or LAN connection. It is always active, and doesn't require you to sign in.

7. Finally, click ***Finish*** to exit the **Connection Wizard**. Now, the setup is complete.



New Connection Wizard

Completing the New Connection Wizard

Your broadband connection should already be configured and ready to use. If your connection is not working properly, click the following link.

Learn more about broadband connections.

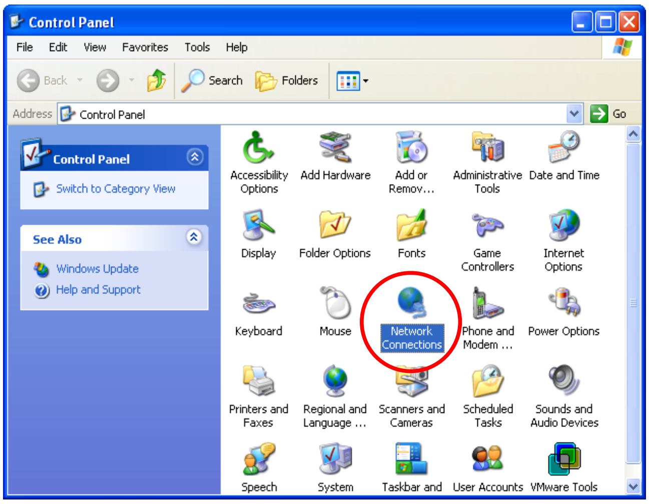
To close this wizard, click Finish.

- **TCP/IP Network Setup**

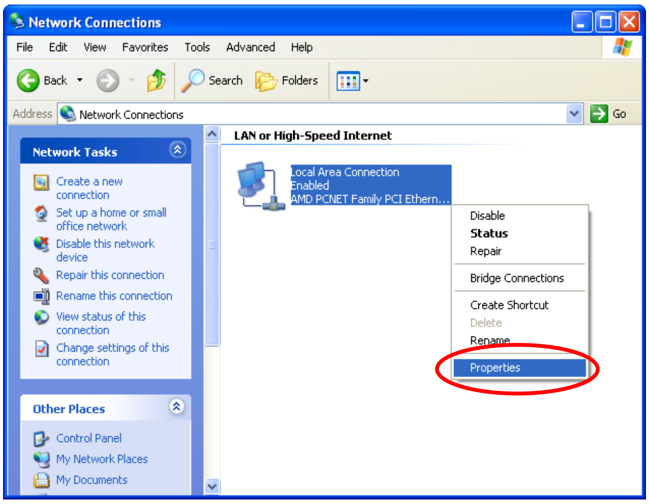
  If the operating system of the PC in use is Windows 95/98/ME/2000/XP, keep the default settings without any change to directly start/restart the system. With the factory default settings, during the process of starting the system, W1310R with DHCP function will automatically assign an appropriate IP address and related information for each PC. If the Windows operating system is not a server version, the default settings of the TCP/IP will regard the PC as a DHCP client, and this function is called **"Obtain an IP address automatically"**. If checking the TCP/IP setup or using the static IP in the LAN1/LAN2 or LAN3/LAN4 section is desired, please follow these steps:

◆ Check the TCP/IP Setup of Window XP

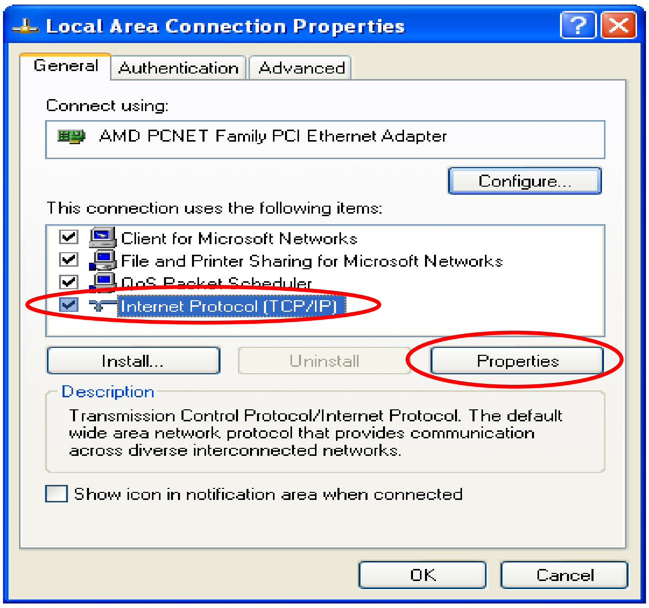
1. Select **Start > Control Panel > Network Connection**.



2. Click the right button of the mouse on the **"Local Area Connection"** icon and select **"Properties"**



3. Select **"General"** label and choose **"Internet Protocol (TCP/IP)"** and then click ***Properties***. Now, choose to use **DHCP** or **specific IP address**, please proceed to the following steps.



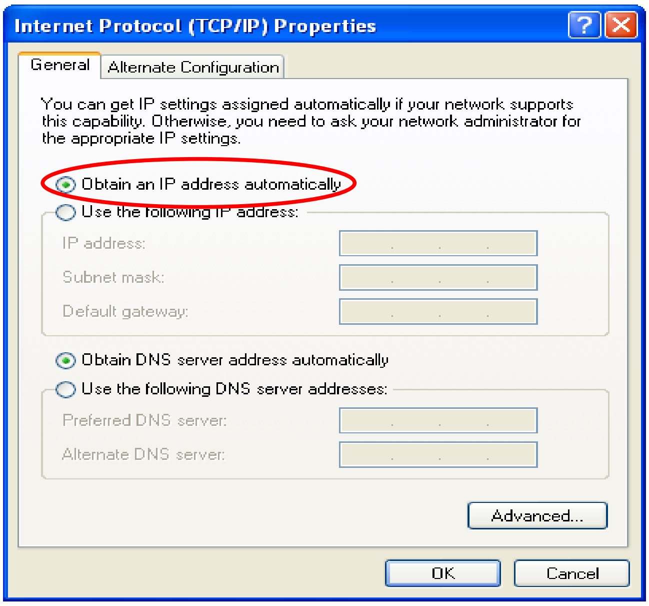
Connect using:
AMD PCNET Family PCI Ethernet Adapter

This connection uses the following items:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

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

□ Show icon in notification area when connected

4-1. **Using DHCP:** If want to use DHCP, please choose **"Obtain an IP address automatically"** and click ***OK***. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from W1310R.



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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

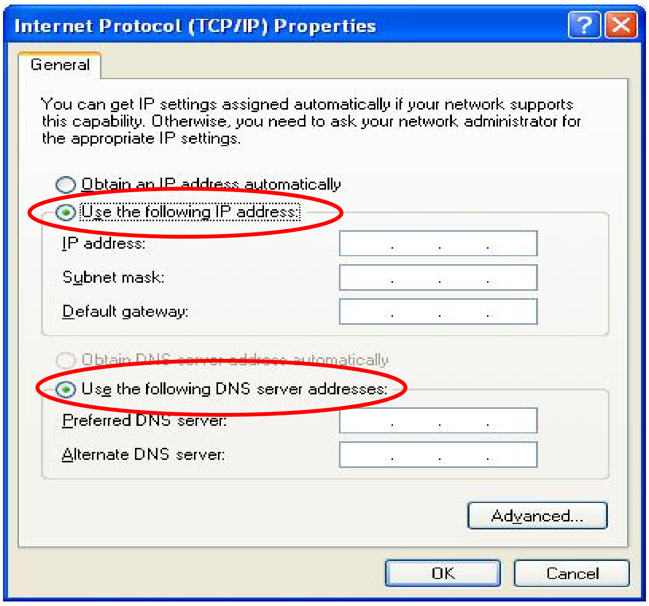
Preferred DNS server: . . .

Alternate DNS server: . . .

4-2. **Using Specific IP Address:** If using specific IP address is desired, ask the network administrator for the information of the W1310R: ***IP address***, ***Subnet Mask***, ***New gateway*** and ***DNS server address***.

Caution: *If your PC has been set up completed, please inform the network administrator before proceeding to the following steps.*

- Please choose **"Use the following IP address"** and enter the information given from the network administrator in **"IP address"** and **"Subnet mask"** If the DNS Server column is blank, please choose **"Using the following DNS server addresses"** and then enter the DNS address or the DNS address provided by ISP and then click ***OK***.



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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

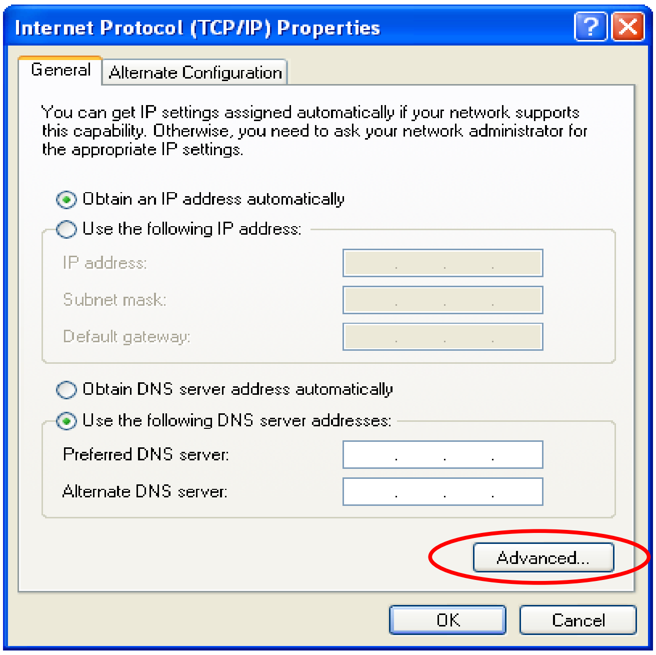
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

- Then, click ***Advanced*** in the window of **"Internet Protocol (TCP/IP)"**.



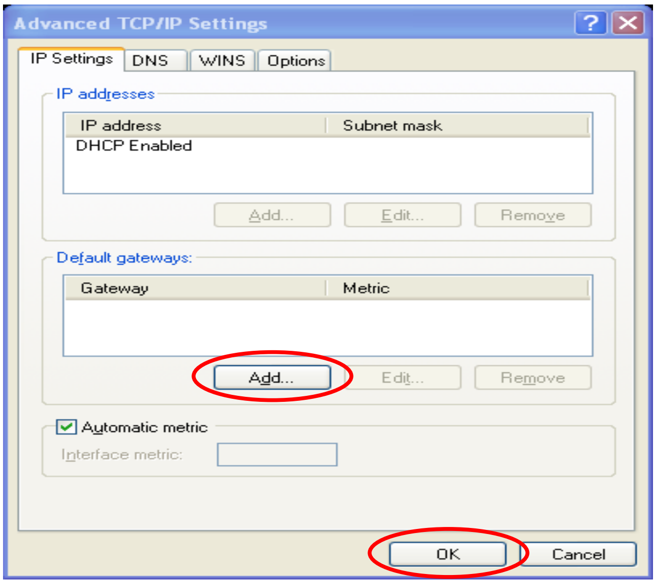
Internet Protocol (TCP/IP) Properties

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

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

- Choose the **"IP Settings"** label and click **"Add"** below the **"Default Gateways"** column and the **"TCP/IP Gateway Address"** window will appear. Enter the gateway address of W1310R in the **"Gateway"** of **"TCP/IP Gateway Address"** window, and then click ***Add***. After back to the **"IP Settings"** label, click ***OK*** to finish.



Advanced TCP/IP Settings

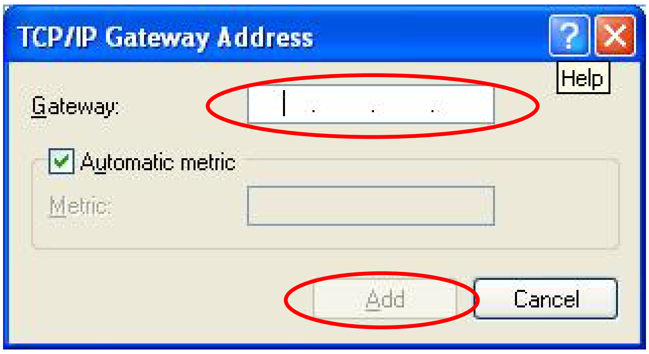
IP addresses

IP address	Subnet mask
DHCP Enabled	

Default gateways:

Gateway	Metric

☑ Automatic metric
Interface metric:



TCP/IP Gateway Address

Gateway: . . .

☑ Automatic metric
Metric:

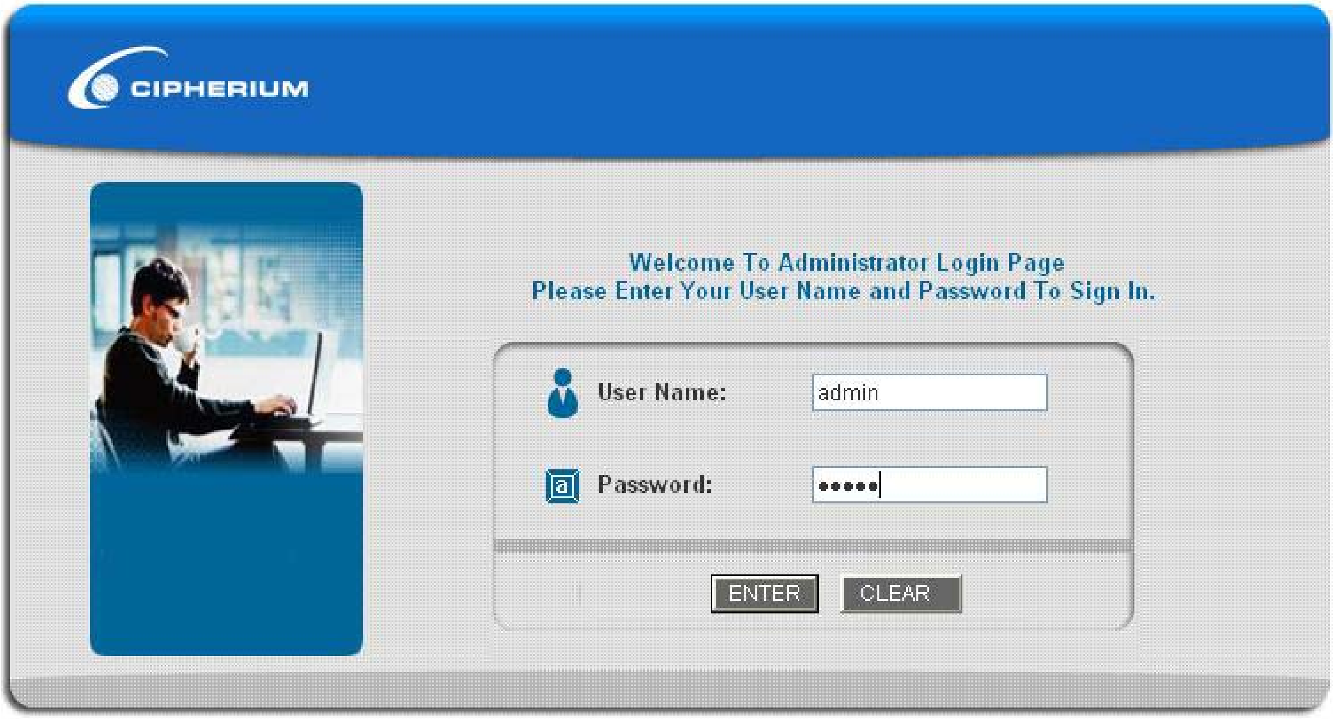
3.2.2 Quick Configuration

There are two ways to configure the system: using **Configuration Wizard** or change the setting by demands manually. The Configuration Wizard has 7 steps providing a simple and easy way to guide you through the setup of W1310R. Follow the procedures and instructions given by the Wizard to enter the required information step by step. After saving and restarting W1310R, it is ready to use. There will be **7** steps as listed below:

1. Change Admin's Password
2. Choose System's Time Zone
3. Set System Information
4. Select the Connection Type for WAN Port
5. Set Authentication Methods
6. Set Wireless – Access Point Connection
7. Save and Restart W1310R

Please follow the following steps to complete the quick configuration

1. Use the network cable of the 10/100BaseT to connect PC to the LAN3/LAN4 port, and then start a browser (such as Microsoft IE). Next, enter the gateway address for that port, the default is https://192.168.2.254. In the opened webpage, a login screen will appear. Enter ***"admin"***, the default username, and ***"admin"***, the default password, in the User Name and Password columns. Click ***Enter*** to log in.



Welcome To Administrator Login Page
Please Enter Your User Name and Password To Sign In.

User Name: admin

Password: •••••

Caution: *If you can't get the login screen, you may have incorrectly set your PC to obtain an IP address automatically from authentication LAN port or the IP address used does not have the same subnet as the URL. Please use default IP address such as 192.168.2.xx in your network and then try it again.*

You can log in as **admin**, **manager** or **operator**. The default username and password as follows.

Admin: The administrator can access all area of the W1310R.

User Name: **admin**

Password: **admin**

Manager: The manager only can access the area under ***User Authentication*** to manager the user account, but no permission to change the settings of the profiles of Firewall, Specific Route and Schedule.

User Name: **manager**

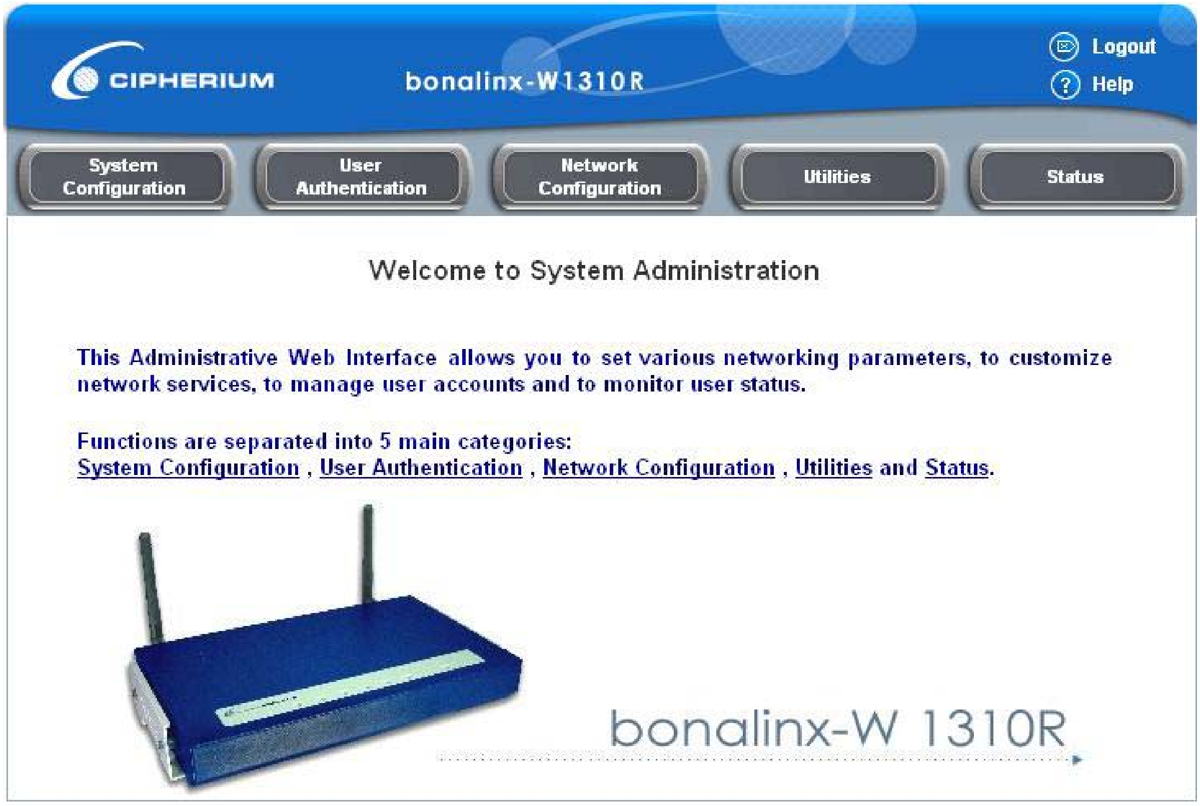
Password: **manager**

Operator: The operator only can access the area of ***Create On-demand User*** to create and print out the new on-demand user accounts.

User Name: **operator**

Password: **operator**

2. After successfully logging into W1310R, enter the web management interface and see the welcome screen. There is a ***Logout*** button on the upper right corner to log out the system when finished.

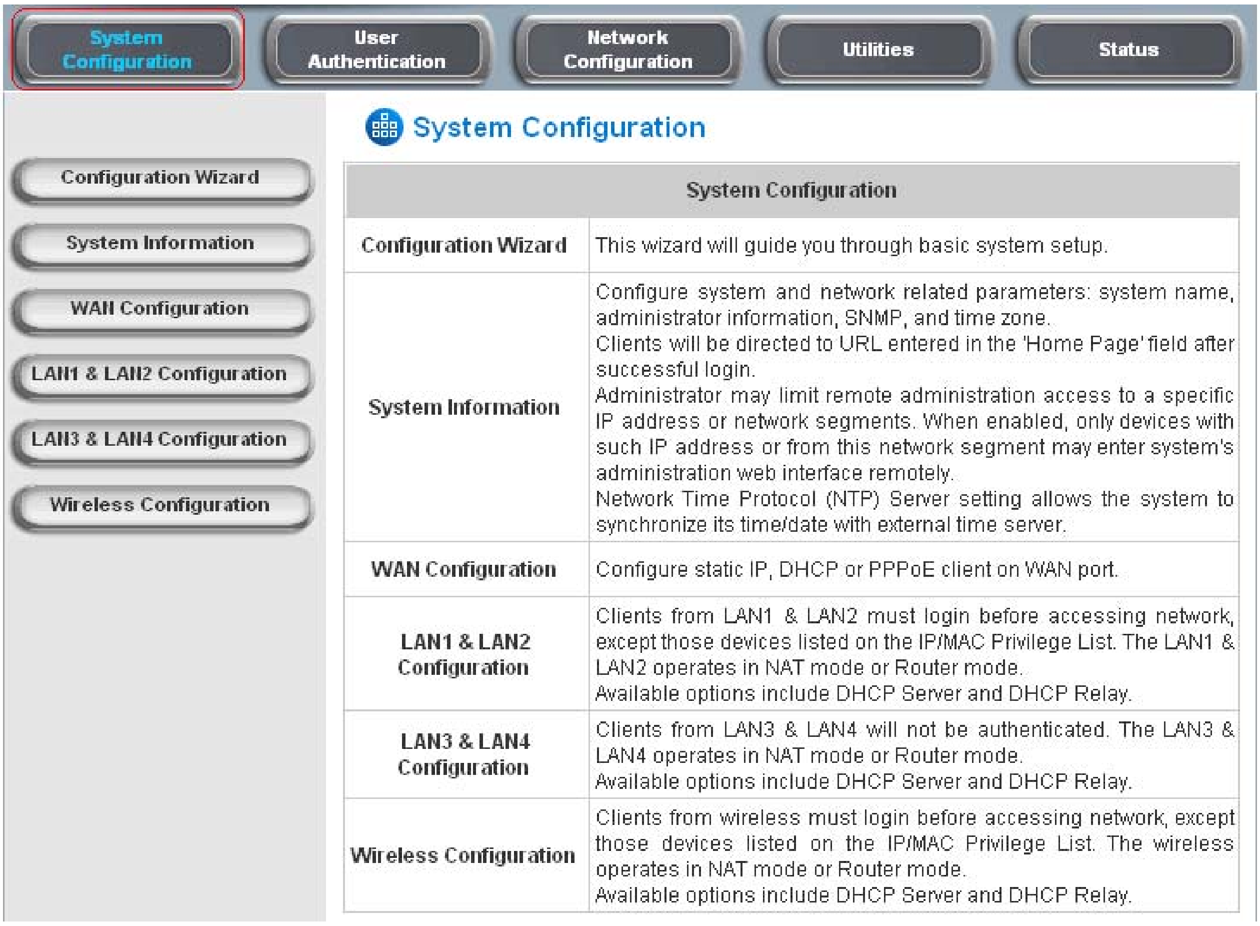


Welcome to System Administration

This Administrative Web Interface allows you to set various networking parameters, to customize network services, to manage user accounts and to monitor user status.

Functions are separated into 5 main categories:
System Configuration , User Authentication , Network Configuration , Utilities and Status.

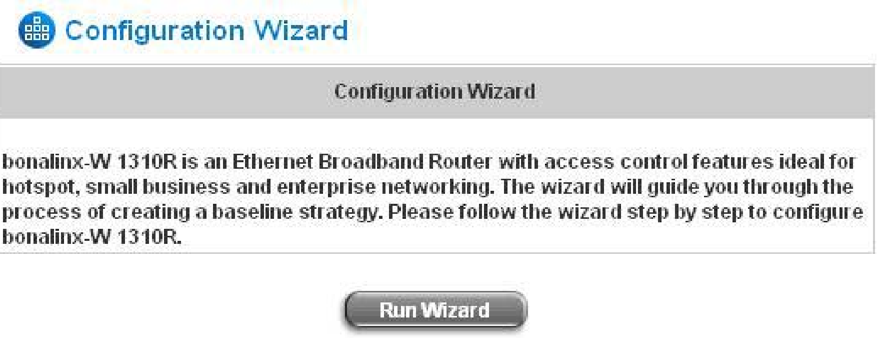
3. Then, run the configuration wizard to complete the configuration. Click ***System Configuration*** to the **System Configuration** homepage.



System Configuration

System Configuration	
Configuration Wizard	This wizard will guide you through basic system setup.
System Information	Configure system and network related parameters: system name, administrator information, SNMP, and time zone. Clients will be directed to URL entered in the 'Home Page' field after successful login. Administrator may limit remote administration access to a specific IP address or network segments. When enabled, only devices with such IP address or from this network segment may enter system's administration web interface remotely. Network Time Protocol (NTP) Server setting allows the system to synchronize its time/date with external time server.
WAN Configuration	Configure static IP, DHCP or PPPoE client on WAN port.
LAN1 & LAN2 Configuration	Clients from LAN1 & LAN2 must login before accessing network, except those devices listed on the IP/MAC Privilege List. The LAN1 & LAN2 operates in NAT mode or Router mode. Available options include DHCP Server and DHCP Relay.
LAN3 & LAN4 Configuration	Clients from LAN3 & LAN4 will not be authenticated. The LAN3 & LAN4 operates in NAT mode or Router mode. Available options include DHCP Server and DHCP Relay.
Wireless Configuration	Clients from wireless must login before accessing network, except those devices listed on the IP/MAC Privilege List. The wireless operates in NAT mode or Router mode. Available options include DHCP Server and DHCP Relay.

4. Click the ***System Configuration*** from the top menu and the homepage of **System Configuration** will appear. Then, click on ***Configuration Wizard*** and click the ***Run Wizard*** button to start the wizard.

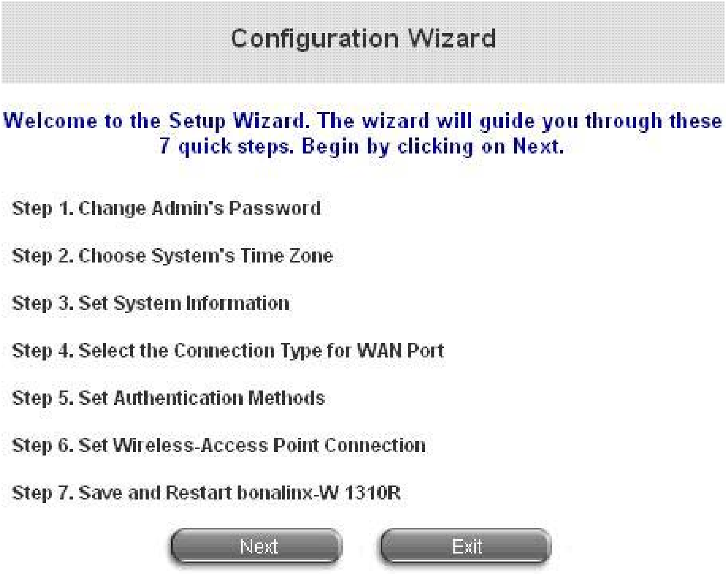


Configuration Wizard

Configuration Wizard
bonalinx-W 1310R is an Ethernet Broadband Router with access control features ideal for hotspot, small business and enterprise networking. The wizard will guide you through the process of creating a baseline strategy. Please follow the wizard step by step to configure bonalinx-W 1310R.

5. **Configuration Wizard**

A welcome screen that briefly introduces the 7 steps will appear. Click ***Next*** to begin.



Configuration Wizard

Welcome to the Setup Wizard. The wizard will guide you through these 7 quick steps. Begin by clicking on Next.

Step 1. Change Admin's Password

Step 2. Choose System's Time Zone

Step 3. Set System Information

Step 4. Select the Connection Type for WAN Port

Step 5. Set Authentication Methods

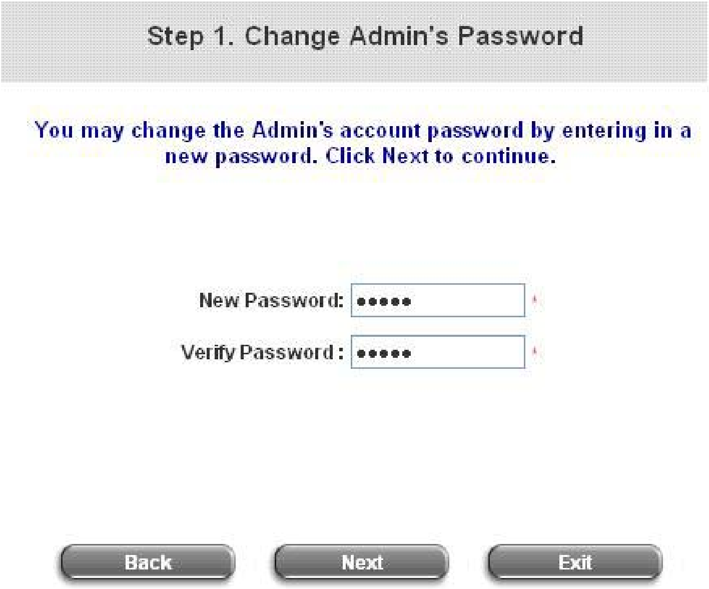
Step 6. Set Wireless-Access Point Connection

Step 7. Save and Restart bonalinx-W 1310R

- **Step 1. Change Admin's Password**

  Enter a new password for the admin account and retype it in the verify password field (twenty-character maximum and no spaces).

  Click ***Next*** to continue.



Step 1. Change Admin's Password

You may change the Admin's account password by entering in a new password. Click Next to continue.

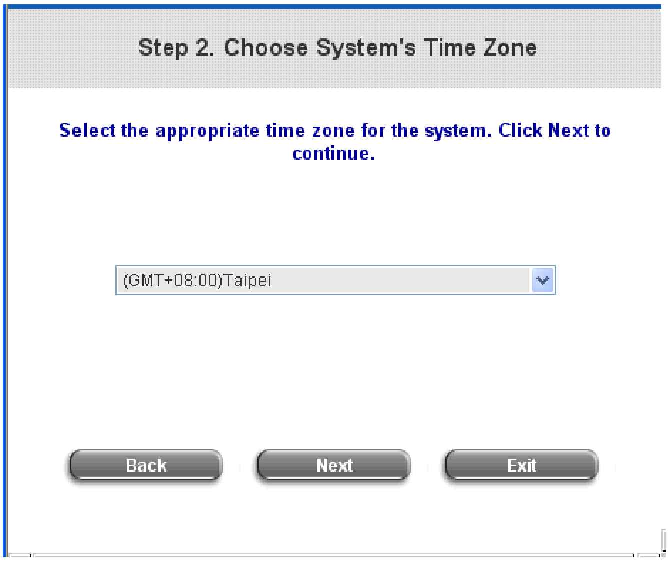
New Password: ●●●●●

Verify Password : ●●●●●

- **Step 2.: Choose System's Time Zone**

  Select a proper time zone via the drop-down menu.

  Click ***Next*** to continue.



Step 2. Choose System's Time Zone

Select the appropriate time zone for the system. Click Next to continue.

(GMT+08:00)Taipei

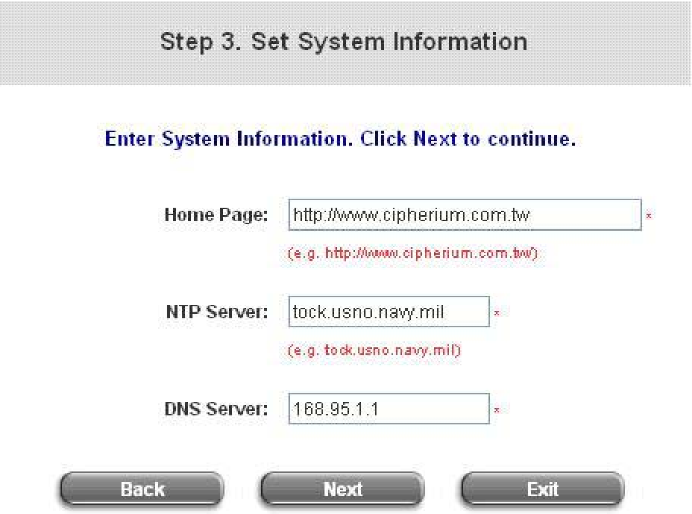
- **Step 3.: Set System Information**

  Home Page: Enter the URL to where the users should be directed when they are successfully authenticated.

  NTP Server: Enter the URL of external time server for W1310R time synchronization or use the default.

  DNS Server: Enter a DNS Server provided by the ISP (Internet Service Provider). Contact the ISP if the DNS IP Address is unknown.

  Click ***Next*** to continue.



Step 3. Set System Information

Enter System Information. Click Next to continue.

Home Page: http://www.cipherium.com.tw *
(e.g. http://www.cipherium.com.tw/)

NTP Server: tock.usno.navy.mil *
(e.g. tock.usno.navy.mil)

DNS Server: 168.95.1.1 *

- **Step 4. Select the Connection Type for WAN Port**

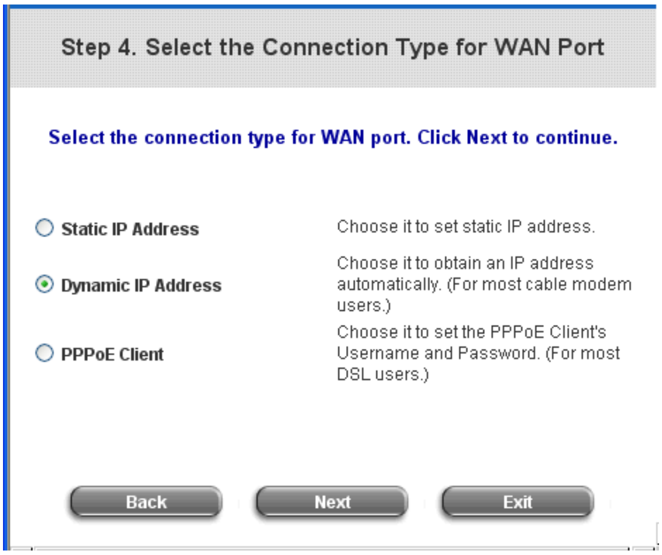
  Three are three types of WAN port to select: **Static IP Address**, **Dynamic IP Address** and **PPPoE Client**.

  Select a proper Internet connection type and click ***Next*** to continue.

  ➢ **Dynamic IP Address**

  If this option is selected, an appropriate IP address and related information will automatically be assigned.

  Click ***Next*** to continue.



Step 4. Select the Connection Type for WAN Port

Select the connection type for WAN port. Click Next to continue.

○ Static IP Address — Choose it to set static IP address.

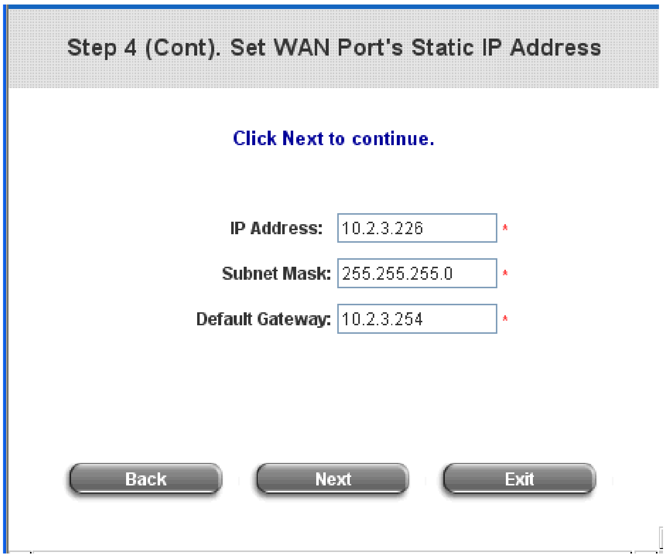
● Dynamic IP Address — Choose it to obtain an IP address automatically. (For most cable modem users.)

○ PPPoE Client — Choose it to set the PPPoE Client's Username and Password. (For most DSL users.)

  ➢ **Static IP Address: Set WAN Port's Static IP Address**

  Enter the **"IP Address"**, **"Subnet Mask"** and **"Default Gateway"** provided by the ISP.

  Click ***Next*** to continue.



Step 4 (Cont). Set WAN Port's Static IP Address

Click Next to continue.

IP Address: 10.2.3.226 *

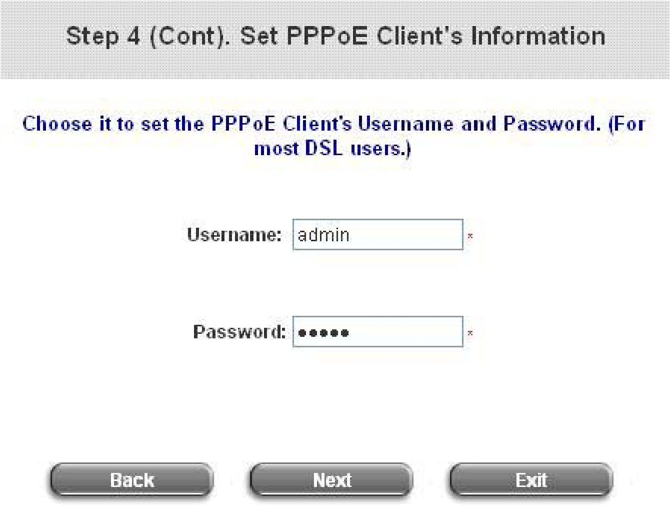
Subnet Mask: 255.255.255.0 *

Default Gateway: 10.2.3.254 *

- **PPPoE Client: Set PPPoE Client's Information**

  Enter the **"Username"** and **"Password"** provided by the ISP.

  Click ***Next*** to continue.



Step 4 (Cont). Set PPPoE Client's Information

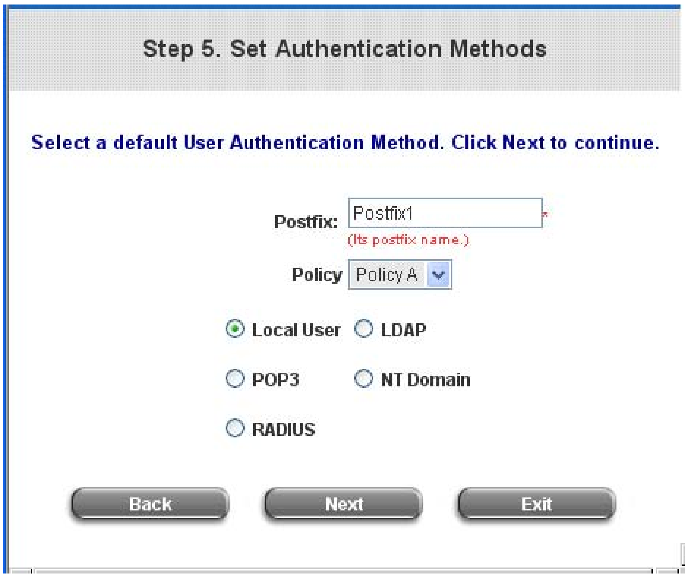
Choose it to set the PPPoE Client's Username and Password. (For most DSL users.)

Username: admin *

Password: ●●●●● *

- **Step 5. Set Authentication Methods**
  - Set the user's information in advance. Enter an easily identified name as the postfix name in the ***Postfix*** field (e.g. Local), select a policy to (or use the default value), and choose an authentication method.

    Click ***Next*** to continue.



Step 5. Set Authentication Methods

Select a default User Authentication Method. Click Next to continue.

Postfix: Postfix1 *
(Its postfix name.)

Policy: Policy A

● Local User ○ LDAP

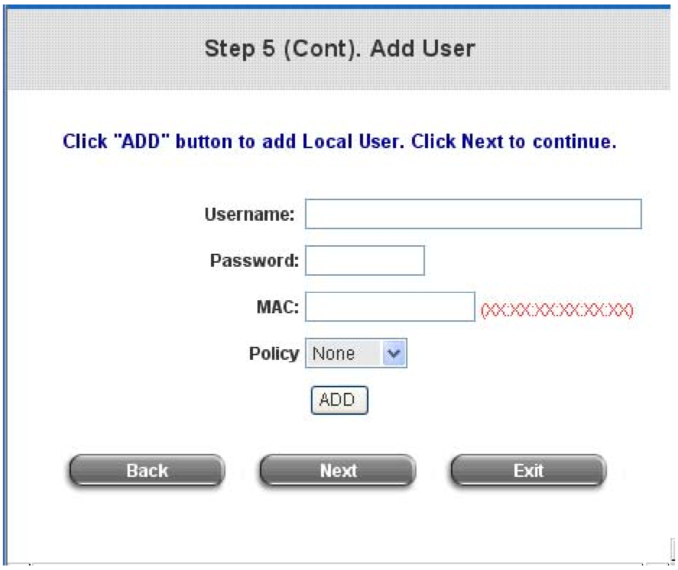
○ POP3 ○ NT Domain

○ RADIUS

- **Local User: Add User**

  A new user can be added to the local user data base. To want to add a user here, enter the ***Username*** (e.g. test), ***Password*** (e.g. test), ***MAC*** (optional) and assign it a policy (or use the default). Upon completing a user adding, more users can be added to this authentication method by clicking the ***ADD*** bottom.

  Click ***Next*** to continue.



Step 5 (Cont). Add User

Click "ADD" button to add Local User. Click Next to continue.

Username:

Password:

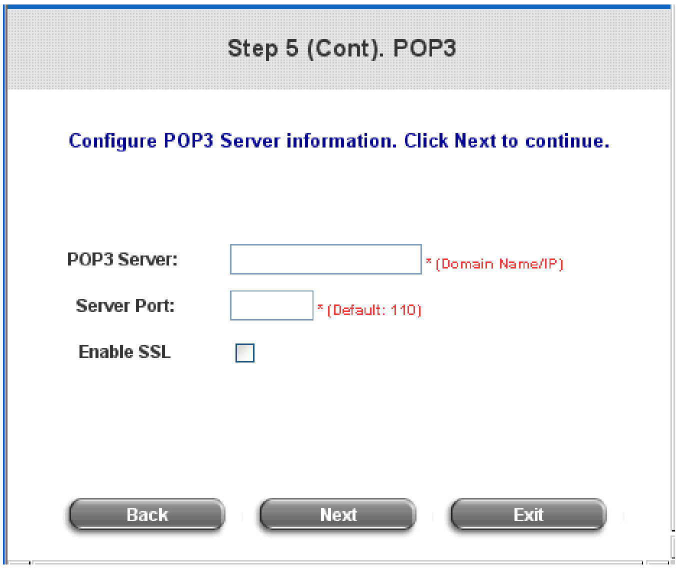
MAC: (XX:XX:XX:XX:XX:XX)

Policy: None

POP3 User: POP3

Enter IP/Domain Name and server port of the POP3 server provided by the ISP, and then choose enable SSL or not.

Click ***Next*** to continue.



Step 5 (Cont). POP3

Configure POP3 Server information. Click Next to continue.

POP3 Server: * (Domain Name/IP)

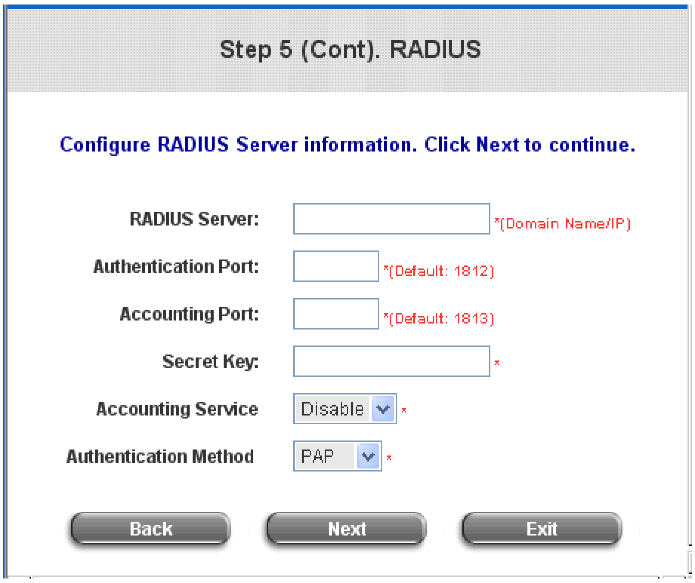
Server Port: * (Default: 110)

Enable SSL □

- **RADIUS User: RADIUS**

Enter RADIUS server IP/Domain Name, authentication port, accounting port and secret key. Then choose to enable accounting service or not, and choose the desired authentication method.

Click ***Next*** to continue.



Step 5 (Cont). RADIUS

Configure RADIUS Server information. Click Next to continue.

RADIUS Server: *(Domain Name/IP)

Authentication Port: *(Default: 1812)

Accounting Port: *(Default: 1813)

Secret Key: *

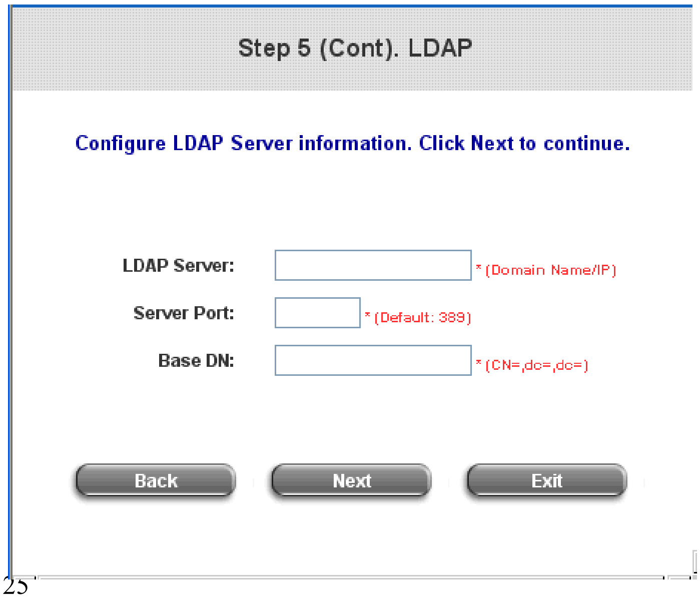
Accounting Service: Disable *

Authentication Method: PAP *

- **LDAP User: LDAP**

Add a new user to the LDAP user data base if desired. Enter the **"LDAP Server"**, **"Server Port"**, and **"Base DN"**.

Click **Next** to continue.



Step 5 (Cont). LDAP

Configure LDAP Server information. Click Next to continue.

LDAP Server: * (Domain Name/IP)

Server Port: * (Default: 389)

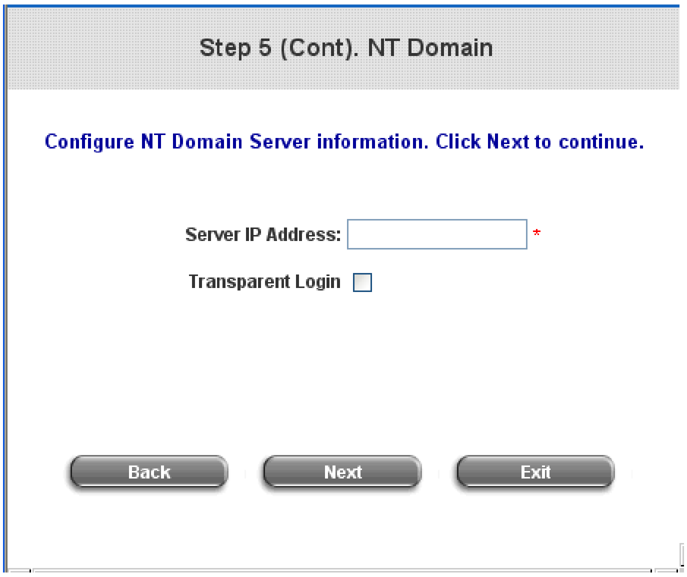
Base DN: * (CN=,dc=,dc=)

- **NT Domain User: NT Domain**

  When NT Domain User is selected, enter the information for **"Server IP Address"**, and choose to enable/disable **"Transparent Login"**.

  If "Transparent Login" is enabled, users are logged in W1310R's NT Domain active directory and authenticated automatically when they log into their Windows OS domain.

  Click ***Next*** to continue.



Step 5 (Cont). NT Domain

Configure NT Domain Server information. Click Next to continue.

Server IP Address: *

Transparent Login □

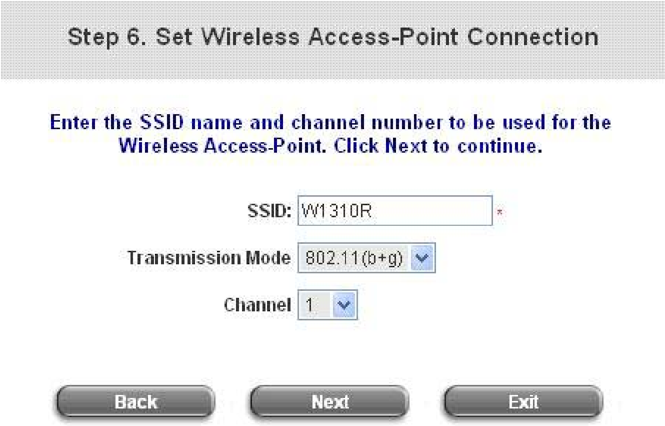
- **Step 6. Set Wireless – Access Point Connection**

  SSID: Enter a SSID (up to 32 characters) for system. **SSID** (**S**ervice **S**et **Id**entifier) is a unique identifier used for the wireless users' devices to get associated with W1310R.

  Transmission Mode: W1310R supports two transmission modes, **802.11b** and **802.11 (b+g)**. Select the appropriate transmission mode to work with the wireless clients in the network.

  Channel: Select a channel from the **"Channel"** field for W1310R to function properly. ***(Note: the available channels depend upon the region. For instance, Channel 1~11 are available in Taiwan, and Channel 1-13 are available in Europe).***

  Click ***Next*** to continue.



Step 6. Set Wireless Access-Point Connection

Enter the SSID name and channel number to be used for the Wireless Access-Point. Click Next to continue.

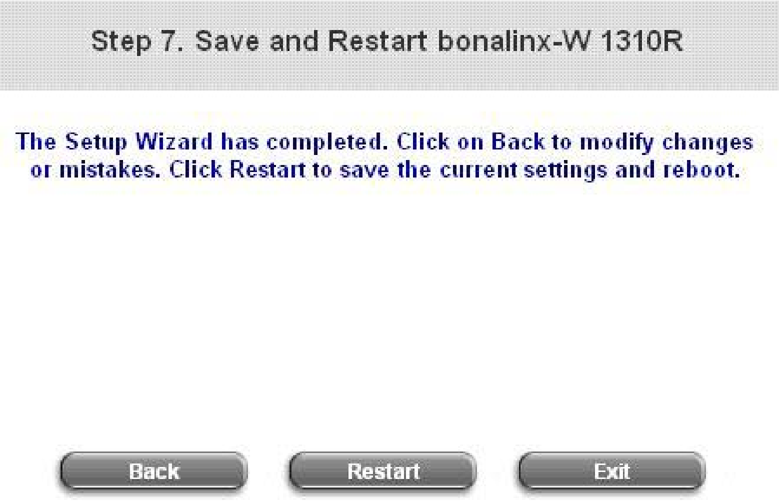
SSID: W1310R *

Transmission Mode 802.11(b+g)

Channel 1

- **Step 7. Save and Restart W1310R**

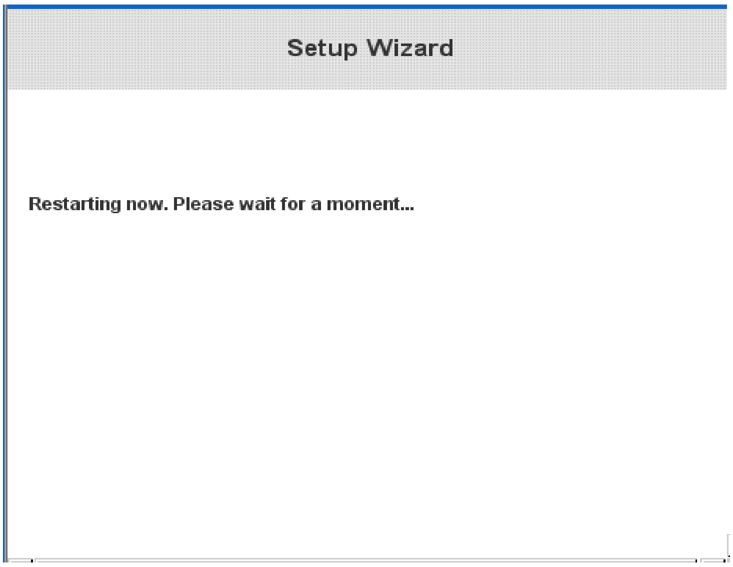
  Click ***Restart*** to save the current settings and restart W1310R. The Setup Wizard is now completed.



Step 7. Save and Restart bonalinx-W 1310R

The Setup Wizard has completed. Click on Back to modify changes or mistakes. Click Restart to save the current settings and reboot.

- **Setup Wizard.** During W1310R restart, a **"Restarting now. Please wait for a while."** message will appear on the screen. Please do not interrupt W1310R until the message has disappeared. This indicates that a complete and successful restart process has finished.



Setup Wizard

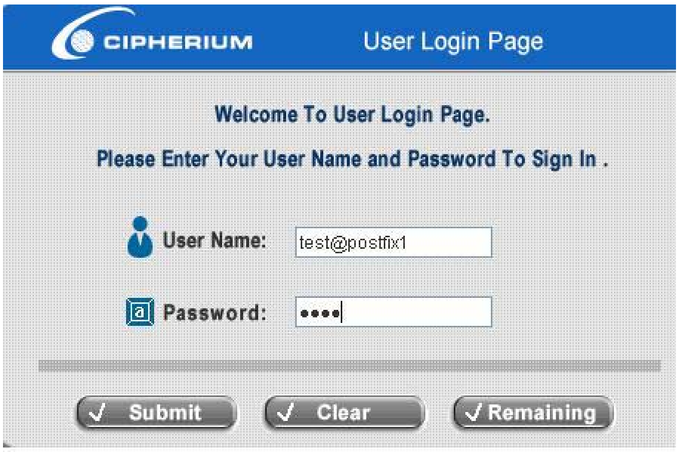
Restarting now. Please wait for a moment...

> ***Caution:*** *During every step of the wizard, if you wish to go back to modify the settings, please click the **Back** button to go back to the previous step.*

3.2.3 External Network Access

If all the steps are set properly, W1310R can be further connected to the managed network to experience the controlled network access environment. Firstly, connect an end-user device to the network at W1310R's LAN1/LAN2 and set to obtain an IP address automatically. After the network address is obtained at the user end, open an Internet browser and link to any website. Then, the default logon webpage will appear in the Internet browser.

1. First, connect a user-end device to LAN1/LAN2 port of the W1310R, and set the dynamical access network. After the user end obtains the network address, please open an Internet browser and the default login webpage will appear on the Internet browser.
   Key in the username and password created in the local user account or the on-demand user account in the interface and then click ***Submit*** button. Here, we key in the local user account (e.g. ***test@Local*** for the username and ***test*** for the password) to connect the network.



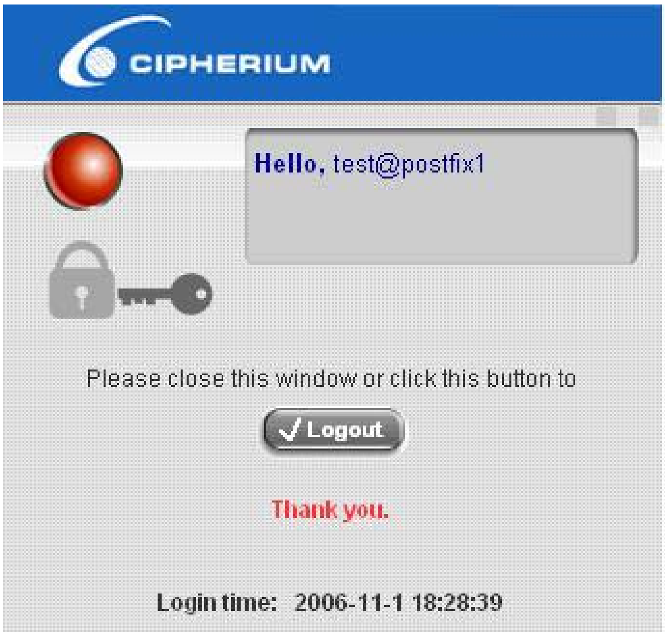
Welcome To User Login Page.

Please Enter Your User Name and Password To Sign In .

User Name: test@postfix1

Password: ••••

2. Login page appearing means W1310R has been installed and configured successfully. Now, the user can browse the network or surf the Internet!



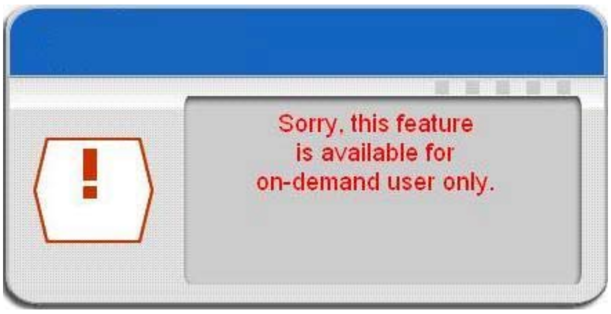
Hello, test@postfix1

Please close this window or click this button to

Thank you.

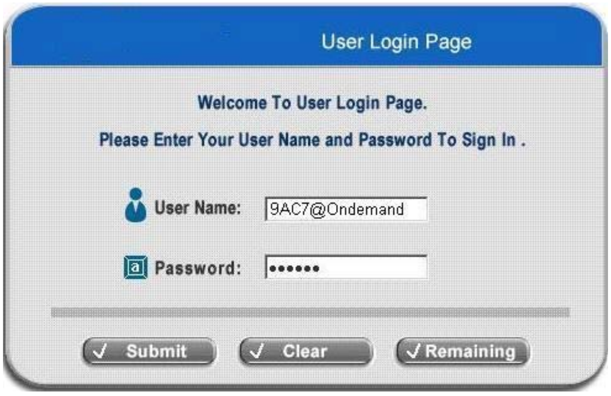
Login time: 2006-11-1 18:28:39

3. If the screen shows **"Sorry, this feature is available for on-demand user only"**, the **"Remaining"** button has been clicked. This button is only for on-demand users. For users other than on-demand users, please click the ***Submit*** button.



Sorry, this feature is available for on-demand user only.

4. An on-demand user can enter the username and password in the **"User Login Page"** and click the ***Remaining*** button to view the remaining time the account.



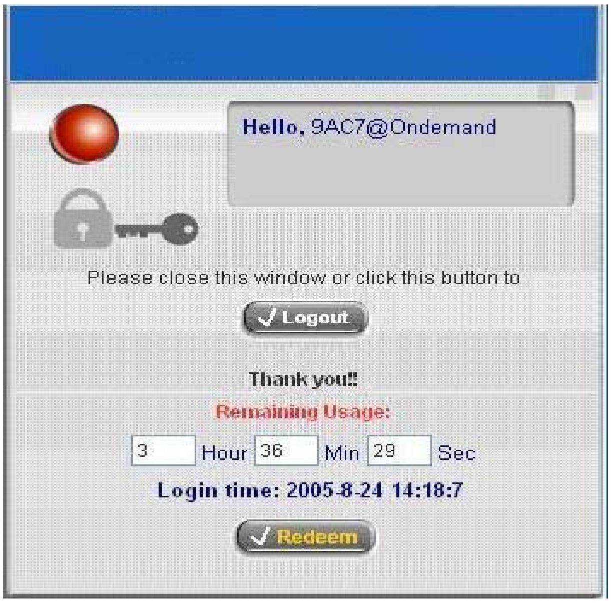
Welcome To User Login Page.

Please Enter Your User Name and Password To Sign In .

User Name: 9AC7@Ondemand

Password: ••••••

5. When an on-demand user logs in successfully, the following **Login Successfully** screen will appear. There is an extra line showing **"Remaining usage"** and a **"Redeem"** button.



Hello, 9AC7@Ondemand

Please close this window or click this button to

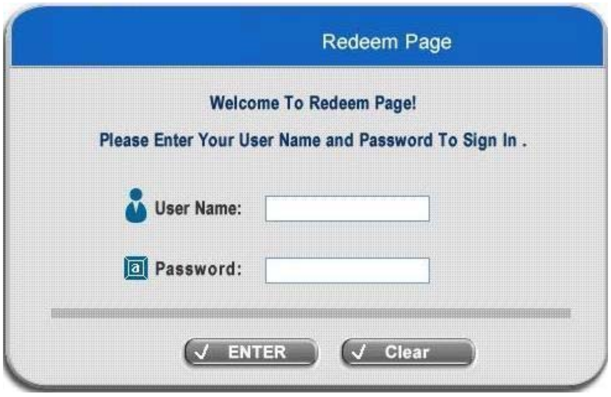
Thank you!!

Remaining Usage:

3 Hour 36 Min 29 Sec

Login time: 2005-8-24 14:18:7

- **Remaining usage:** Show the rest of use time that the on-demand user can surf Internet.
- **Redeem:** When the remaining time or data size is insufficient, the user has to pay for adding credit at the counter, and then, the user will get a new username and password. After clicking the ***Redeem*** button, a login screen will appear. Please enter the new username and password obtained and click ***Redeem*** button. The total available use time and data size after adding credit will show up.



Redeem Page

Welcome To Redeem Page!

Please Enter Your User Name and Password To Sign In .

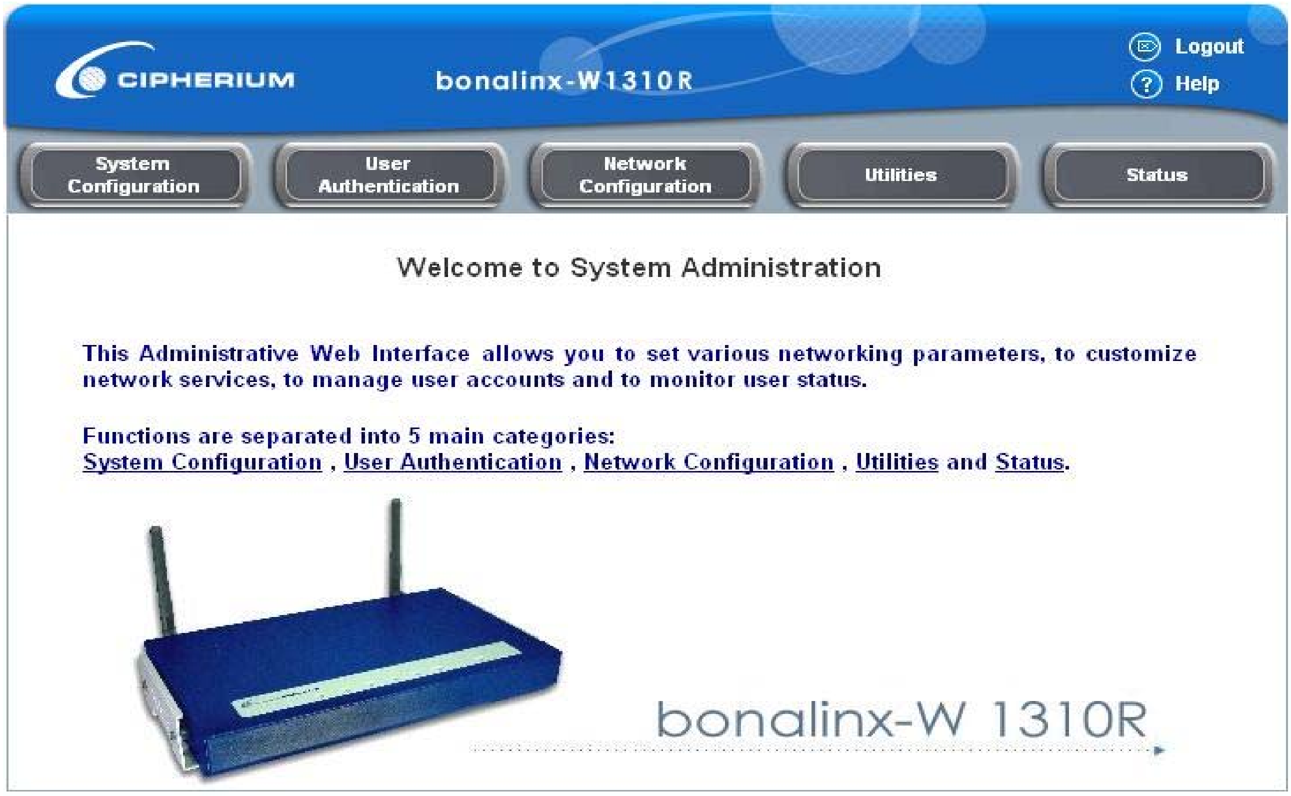
User Name:

Password:

Caution: *The system will automatically reject the redeem process when the redeem amount exceeds the maximum time/data volume provided by W1310R.*

4. Web Interface Configuration

This chapter will guide you through further detailed settings. The following table shows all the functions of W1310R.



Welcome to System Administration

This Administrative Web Interface allows you to set various networking parameters, to customize network services, to manage user accounts and to monitor user status.

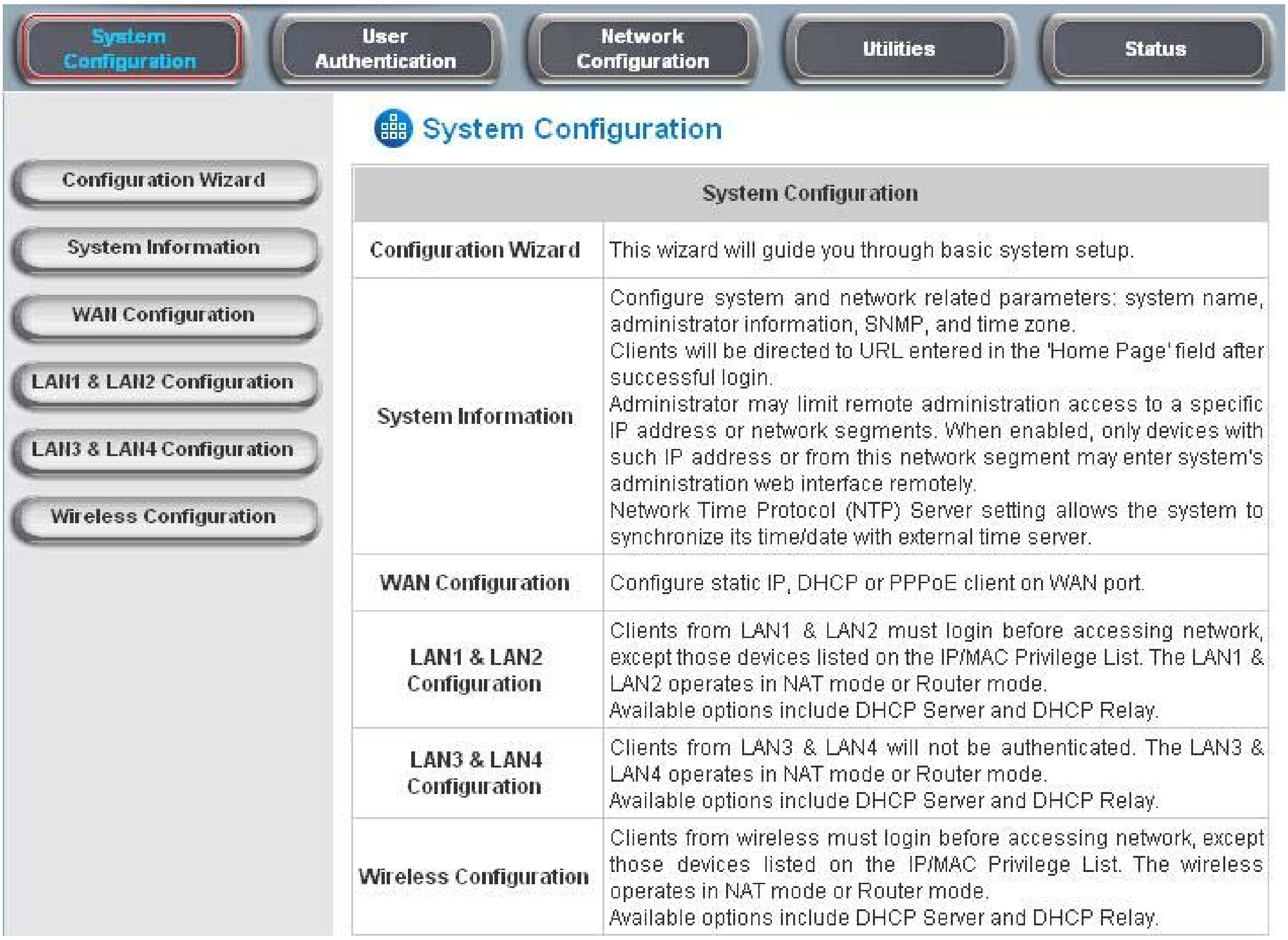
Functions are separated into 5 main categories:
System Configuration , User Authentication , Network Configuration , Utilities and Status.

OPTION	System Configuration	User Authentication	Network Configuration	Utilities	Status
FUNCTION	Configuration Wizard	Authentication Configuration	Network Address Translation	Change Password	System Status
	System Information	Black List Configuration	Privilege List	Backup/Restore Settings	Interface Status
	WAN Configuration	Policy Configuration	Monitor IP List	Firmware Upgrade	Current Users
	LAN1 & LAN2 Configuration	Guest User Configuration	Walled Garden List	Restart	Traffic History
	LAN3 & LAN4 Configuration	Additional Configuration	Proxy Server Properties		Notify Configuration
	Wireless Configuration		Dynamic DNS		

***Caution:** After finishing the configuration of the settings, please click **Apply** and pay attention to see if a restart message appears on the screen. If such message appears, system must be restarted to allow the settings to take effect. All on-line users will be disconnected during restart.*

4.1 System Configuration

This section includes the following functions: **Configuration Wizard**, **System Information**, **WAN Configuration**, **LAN1 & LAN2 Configuration**, **LAN3 & LAN4 Configuration** and **Wireless Configuration**.

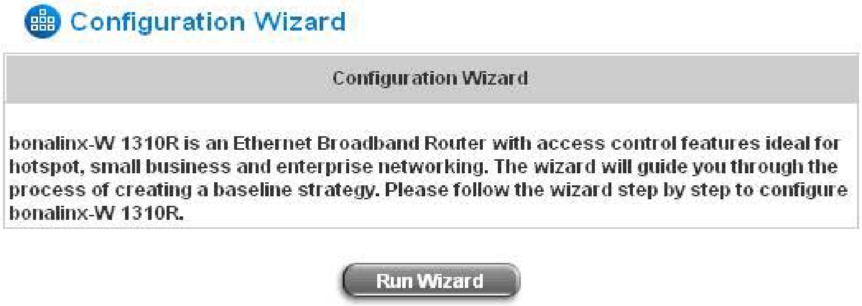


System Configuration

System Configuration	
Configuration Wizard	This wizard will guide you through basic system setup.
System Information	Configure system and network related parameters: system name, administrator information, SNMP, and time zone. Clients will be directed to URL entered in the 'Home Page' field after successful login. Administrator may limit remote administration access to a specific IP address or network segments. When enabled, only devices with such IP address or from this network segment may enter system's administration web interface remotely. Network Time Protocol (NTP) Server setting allows the system to synchronize its time/date with external time server.
WAN Configuration	Configure static IP, DHCP or PPPoE client on WAN port.
LAN1 & LAN2 Configuration	Clients from LAN1 & LAN2 must login before accessing network, except those devices listed on the IP/MAC Privilege List. The LAN1 & LAN2 operates in NAT mode or Router mode. Available options include DHCP Server and DHCP Relay.
LAN3 & LAN4 Configuration	Clients from LAN3 & LAN4 will not be authenticated. The LAN3 & LAN4 operates in NAT mode or Router mode. Available options include DHCP Server and DHCP Relay.
Wireless Configuration	Clients from wireless must login before accessing network, except those devices listed on the IP/MAC Privilege List. The wireless operates in NAT mode or Router mode. Available options include DHCP Server and DHCP Relay.

4.1.1 Configuration Wizard

There are two ways to configure the system: using **Configuration Wizard** or change the setting by demands manually. The Configuration Wizard has 7 steps providing a simple and easy way to go through the basic setups of W1310R and is served as **Quick Configuration**. Please refer to **3.2.2 Quick Configuration** for the introduction and description of **Configuration Wizard**.



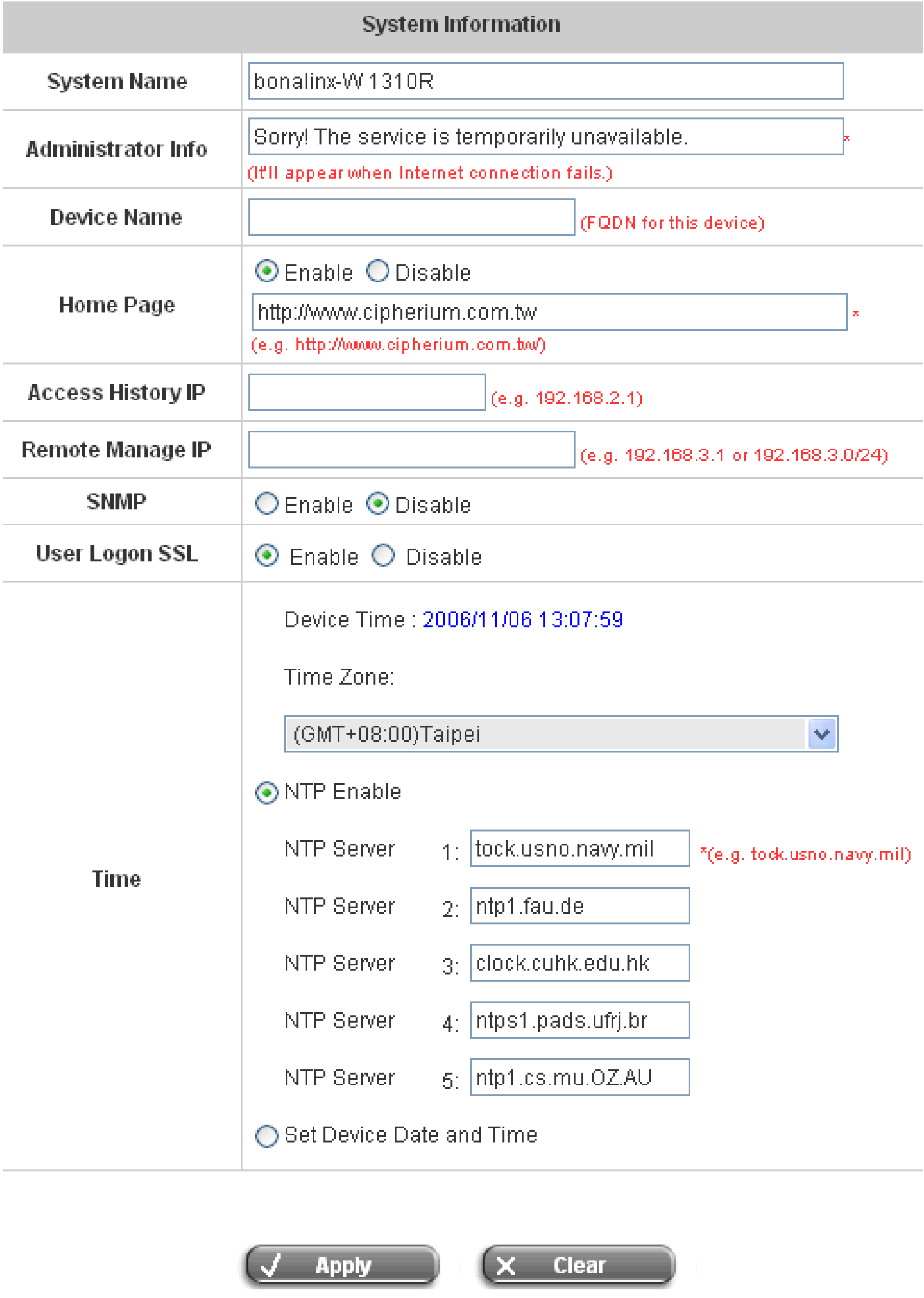
Configuration Wizard

Configuration Wizard

bonalinx-W 1310R is an Ethernet Broadband Router with access control features ideal for hotspot, small business and enterprise networking. The wizard will guide you through the process of creating a baseline strategy. Please follow the wizard step by step to configure bonalinx-W 1310R.

4.1.2 System Information

These are some main information about W1310R. Please refer to the following description for these blanks:



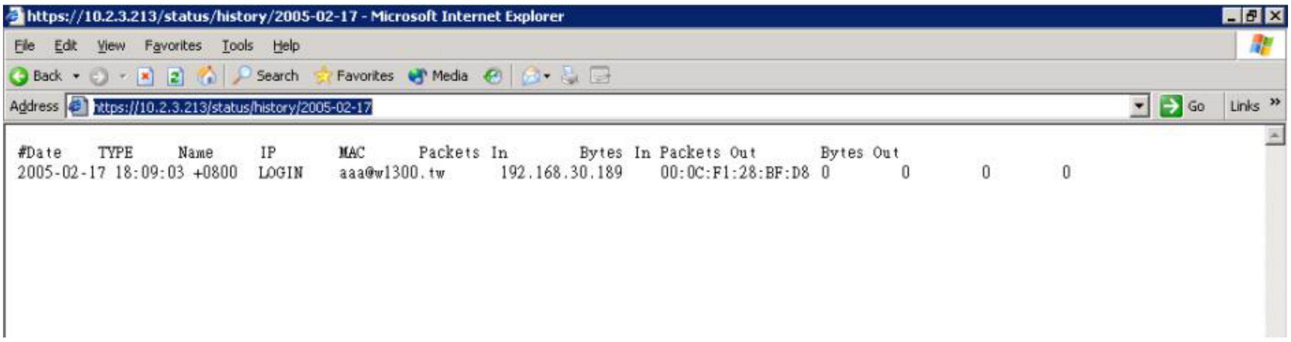
System Information

System Name	bonalinx-W1310R
Administrator Info	Sorry! The service is temporarily unavailable. * (It'll appear when Internet connection fails.)
Device Name	(FQDN for this device)
Home Page	● Enable ○ Disable http://www.cipherium.com.tw * (e.g. http://www.cipherium.com.tw/)
Access History IP	(e.g. 192.168.2.1)
Remote Manage IP	(e.g. 192.168.3.1 or 192.168.3.0/24)
SNMP	○ Enable ● Disable
User Logon SSL	● Enable ○ Disable
Time	Device Time : 2006/11/06 13:07:59 Time Zone: (GMT+08:00)Taipei ● NTP Enable NTP Server 1: tock.usno.navy.mil *(e.g. tock.usno.navy.mil) NTP Server 2: ntp1.fau.de NTP Server 3: clock.cuhk.edu.hk NTP Server 4: ntps1.pads.ufrj.br NTP Server 5: ntp1.cs.mu.OZ.AU ○ Set Device Date and Time

- **System Name:** Set the system's name or use the default.
- **Administrator Info:** Enter the Administrator's information here, such as administrator's name, telephone number, e-mail address, etc. If users encountered problems in the connection of the WAN port to the system, this information will appear on the user's login screen.
- **Home Page:** Enter the website of a Web Server to be the homepage. When users log in successfully, they will be directed to the homepage set, such as http://www.yahoo.com. Regardless of the original webpage set in the users' computers, they will be redirect to this page after login.

- **Access History IP:** Specify an IP address of the administrator's computer or a billing system to get billing history information of W1310R.   An example is provided as follows and "10.2.3.213" is the WAN IP of W1310R.

  Traffic History：https://10.2.3.213/status/history/2005-02-17

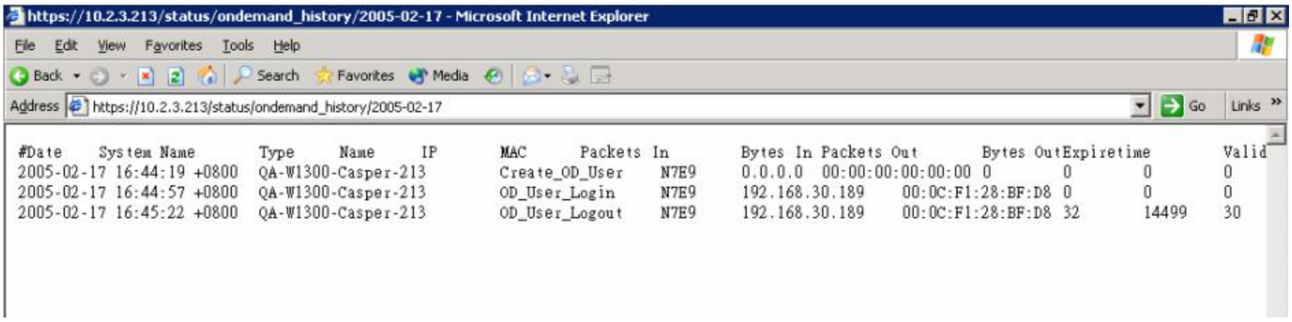


https://10.2.3.213/status/history/2005-02-17 - Microsoft Internet Explorer

Address https://10.2.3.213/status/history/2005-02-17

```
#Date     TYPE      Name      IP        MAC       Packets In          Bytes In Packets Out        Bytes Out
2005-02-17 18:09:03 +0800   LOGIN     aaa@w1300.tw        192.168.30.189      00:0C:F1:28:BF:D8 0         0         0         0
```

  On-demand History：https://10.2.3.213/status/ondemand_history/2005-02-17

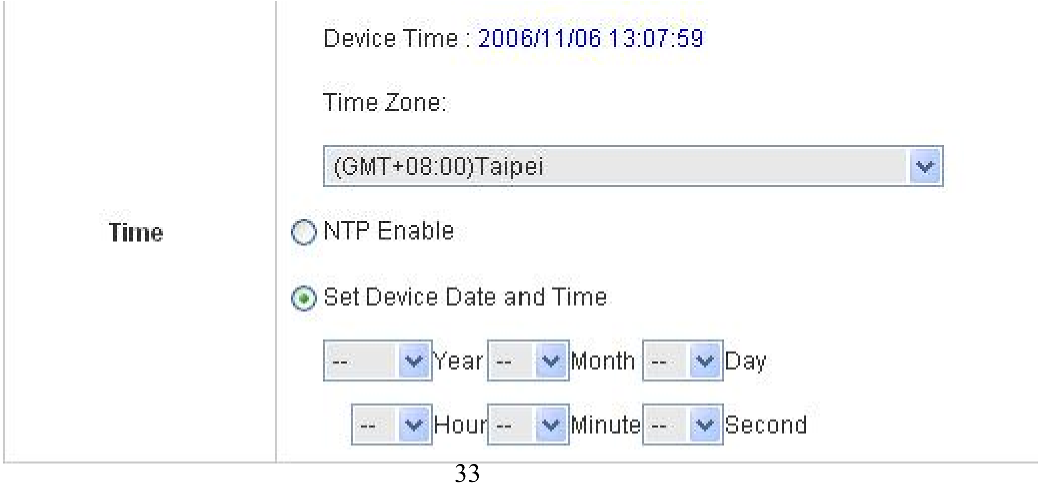


https://10.2.3.213/status/ondemand_history/2005-02-17 - Microsoft Internet Explorer

Address https://10.2.3.213/status/ondemand_history/2005-02-17

```
#Date     System Name         Type      Name      IP        MAC       Packets In          Bytes In Packets Out        Bytes OutExpiretime          Valid
2005-02-17 16:44:19 +0800   QA-W1300-Casper-213           Create_OD_User      N7E9      0.0.0.0   00:00:00:00:00:00 0         0         0         0
2005-02-17 16:44:57 +0800   QA-W1300-Casper-213           OD_User_Login       N7E9      192.168.30.189      00:0C:F1:28:BF:D8 0         0         0
2005-02-17 16:45:22 +0800   QA-W1300-Casper-213           OD_User_Logout      N7E9      192.168.30.189      00:0C:F1:28:BF:D8 32        14499     30
```

- **Remote Manage IP:** Set the IP block with a system which is able to connect to the web management interface via the authenticated port. For example, 10.2.3.0/24 means that as long as you are within the IP address range of 10.2.3.0/24, you can reach the administration page of W1310R.
- **SNMP:** W1310R supports SNMPv2. If the function is enabled, administrators can assign the Manager IP address and the SNMP community name used to access the management information base (MIB) of the system.
- **User logon SSL:** Enable to activate https (encryption) or disable to activate http (non encryption) login page.
- **Time:** W1310R supports NTP communication protocol to synchronize the network time. Please specify the IP address of a server in the system configuration interface for adjusting the time automatically. (Universal Time is Greenwich Mean Time, GMT). Time can be set manually by selecting **"Set Device Date and Time"**. Please enter the date and time for these fields.



Time

Device Time : 2006/11/06 13:07:59

Time Zone:

(GMT+08:00)Taipei

○ NTP Enable

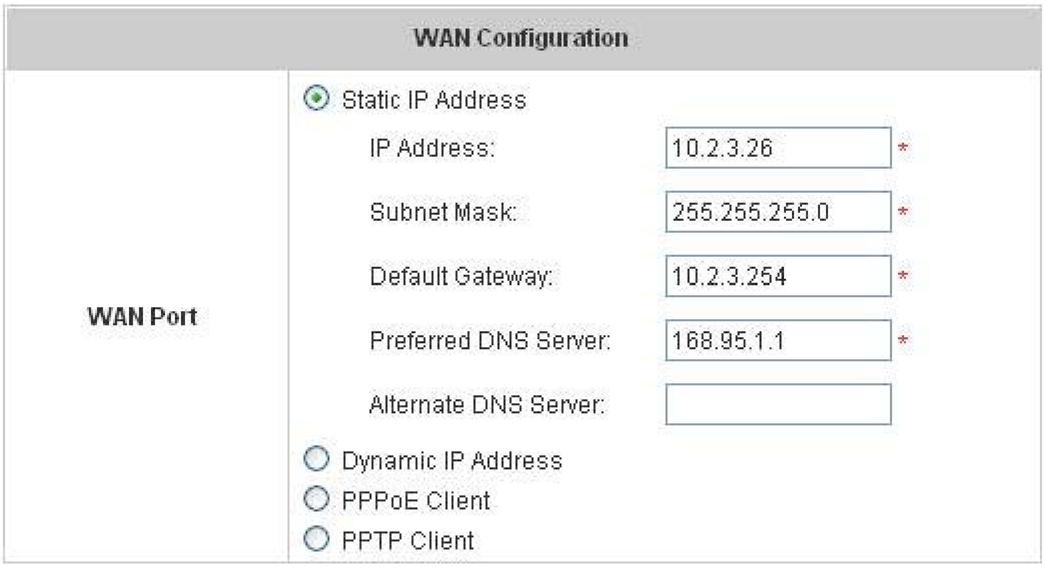
● Set Device Date and Time

-- Year -- Month -- Day

-- Hour -- Minute -- Second

4.1.3 WAN Configuration

There are 4 methods of obtaining IP address for the WAN Port: **Static IP Address**, **Dynamic IP Address**, **PPPoE** and **PPTP Client**.



WAN Configuration

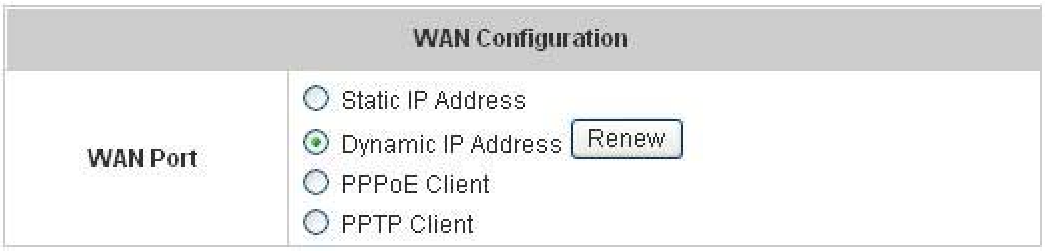
WAN Port

● Static IP Address

IP Address:	10.2.3.26	*
Subnet Mask:	255.255.255.0	*
Default Gateway:	10.2.3.254	*
Preferred DNS Server:	168.95.1.1	*
Alternate DNS Server:		

○ Dynamic IP Address
○ PPPoE Client
○ PPTP Client

- **Static IP Address:** Manually specifying the IP address of the WAN Port is applicable for the network environment where the DHCP service is unavailable. The fields with red asterisks are required to be filled in.
  IP address: the IP address of the WAN port.
  Subnet mask: the subnet mask of the WAN port.
  Default gateway: the gateway of the WAN port.
  Preferred DNS Server: the primary DNS Server of the WAN port.
  Alternate DNS Server: The substitute DNS Server of the WAN port. This is not required.
- **Dynamic IP address:** It is only applicable for the network environment where the DHCP Server is available in the network. Click the ***Renew*** button to get an IP address.

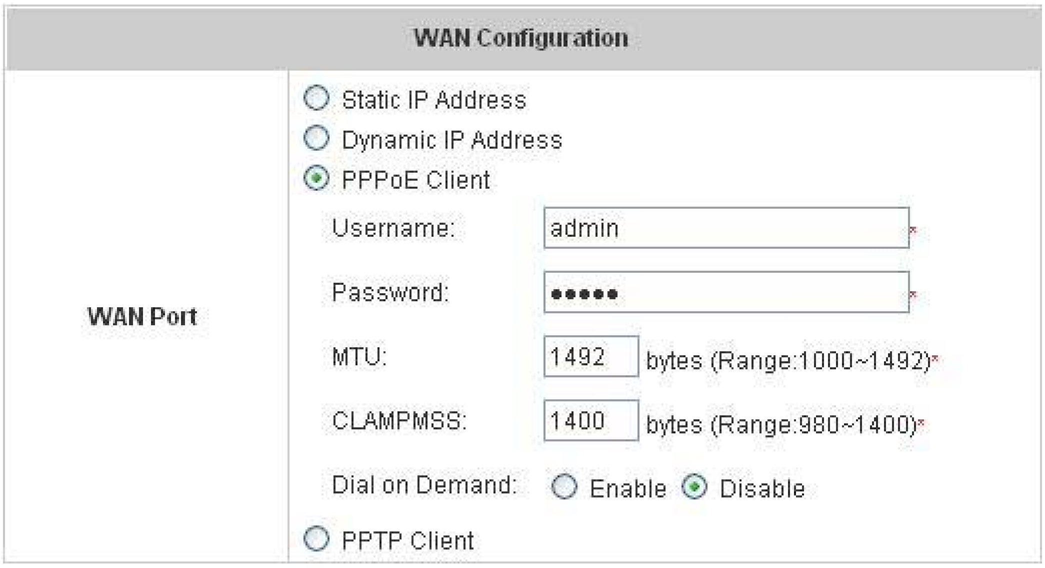


WAN Configuration

WAN Port

○ Static IP Address
● Dynamic IP Address
○ PPPoE Client
○ PPTP Client

- **PPPoE Client:** When selecting PPPoE to connect to the network, please set the **"User Name"**, **"Password"**, **"MTU"** and **"CLAMPMSS"**. There is a **Dial on demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** can be set. When the idle time is reached, the system will automatically disconnect itself.



WAN Configuration

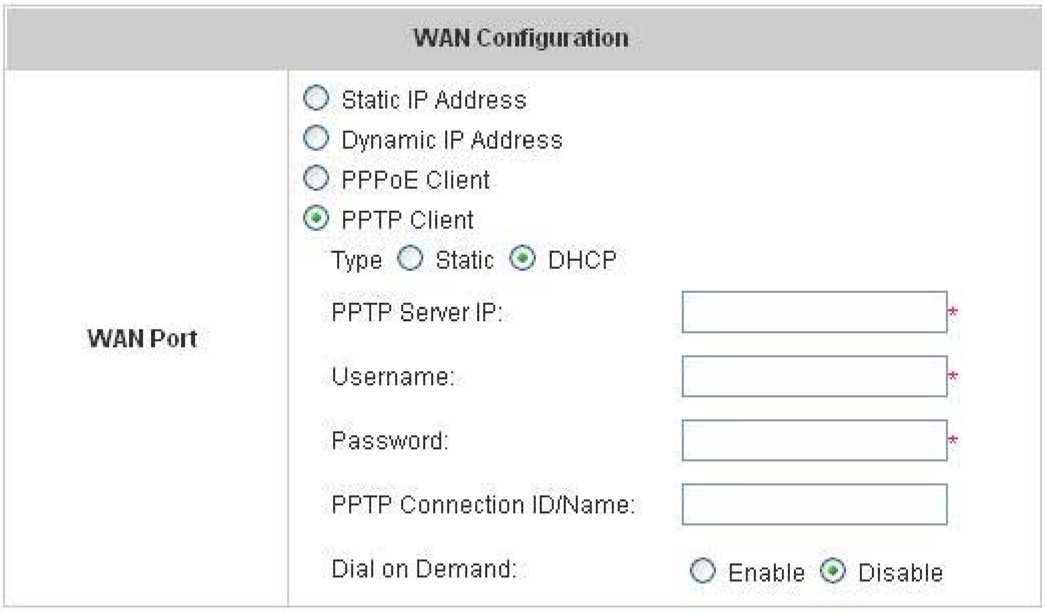
WAN Port

○ Static IP Address
○ Dynamic IP Address
● PPPoE Client

Username:	admin *
Password:	●●●●● *
MTU:	1492 bytes (Range:1000~1492)*
CLAMPMSS:	1400 bytes (Range:980~1400)*
Dial on Demand:	○ Enable ● Disable

○ PPTP Client

- **PPTP Client:** Select **STATIC** to specify the IP address of the PPTP Client manually or select **DHCP** to get the IP address automatically. The fields with red asterisks are required to be filled in. There is a **Dial on demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** can be set. When the idle time is reached, the system will automatically disconnect itself.



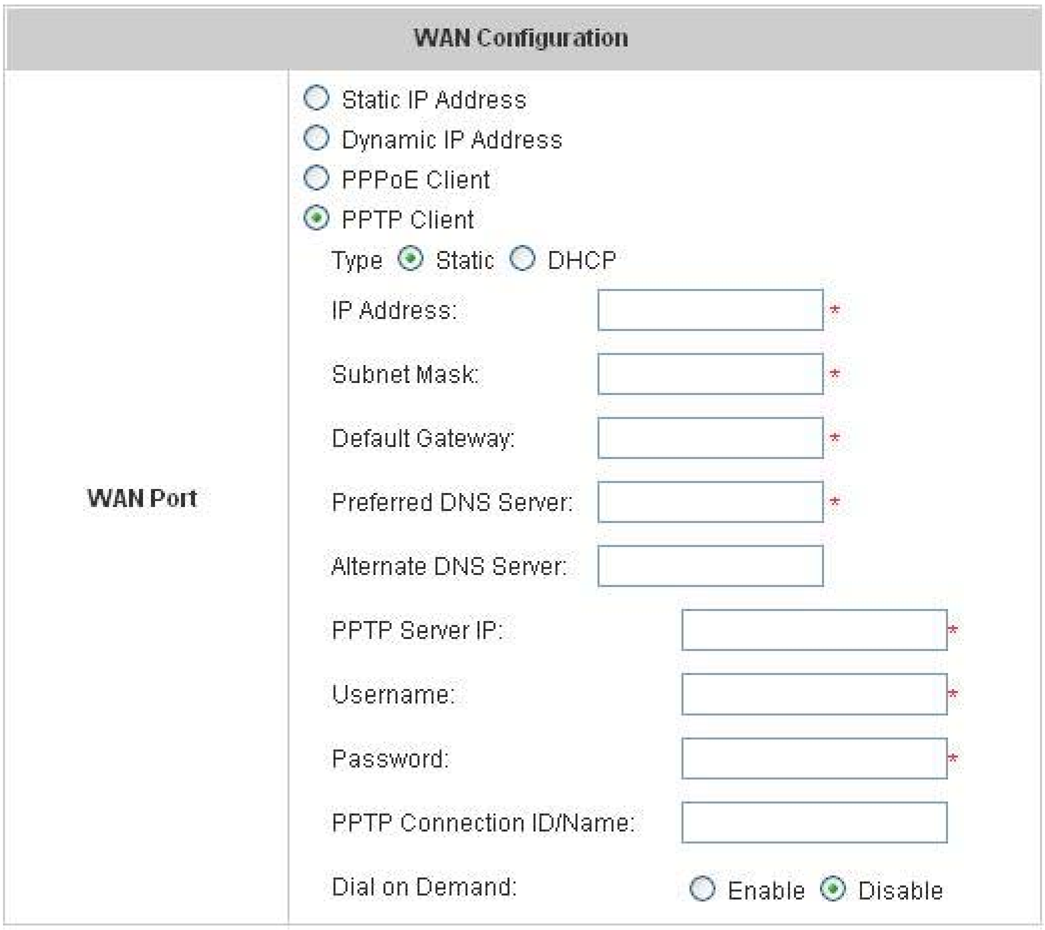
WAN Configuration

WAN Port

○ Static IP Address
○ Dynamic IP Address
○ PPPoE Client
● PPTP Client

Type ○ Static ● DHCP

PPTP Server IP:	*
Username:	*
Password:	*
PPTP Connection ID/Name:	
Dial on Demand:	○ Enable ● Disable

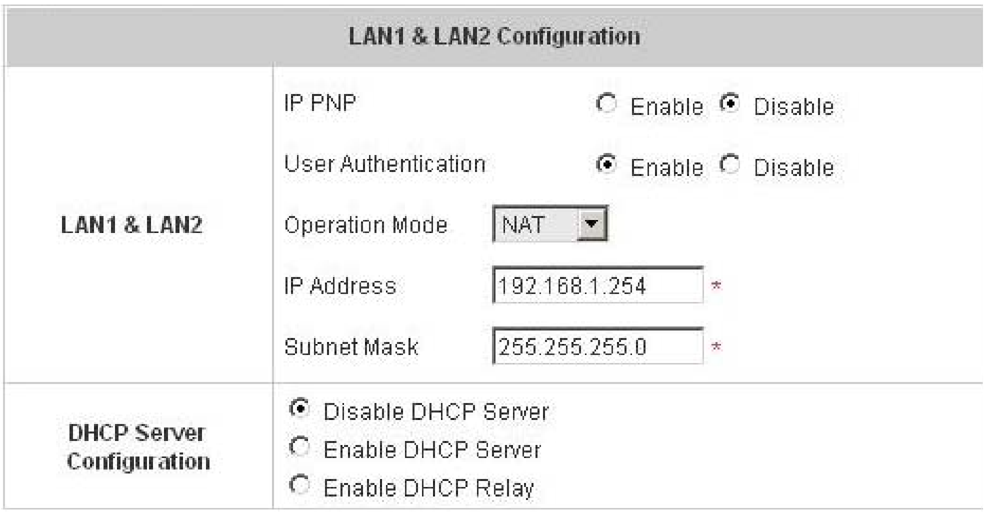


WAN Configuration

WAN Port	○ Static IP Address ○ Dynamic IP Address ○ PPPoE Client ● PPTP Client Type ● Static ○ DHCP IP Address: □ * Subnet Mask: □ * Default Gateway: □ * Preferred DNS Server: □ * Alternate DNS Server: □ PPTP Server IP: □ * Username: □ * Password: □ * PPTP Connection ID/Name: □ Dial on Demand: ○ Enable ● Disable

4.1.4 LAN1 & LAN2 Configuration

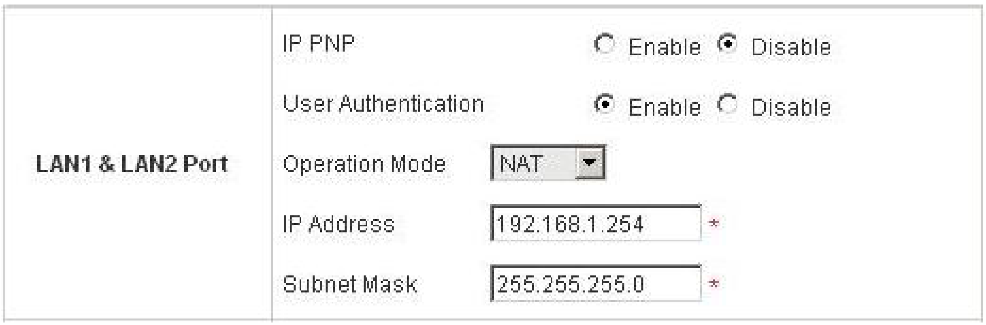
User authentication for the two LAN ports can be enabled or disabled.



LAN1 & LAN2 Configuration

LAN1 & LAN2	IP PNP ○ Enable ● Disable User Authentication ● Enable ○ Disable Operation Mode NAT IP Address 192.168.1.254 * Subnet Mask 255.255.255.0 *
DHCP Server Configuration	● Disable DHCP Server ○ Enable DHCP Server ○ Enable DHCP Relay

- **LAN1 & LAN2 Port**



LAN1 & LAN2 Port

IP PNP ○ Enable ● Disable

User Authentication ● Enable ○ Disable

Operation Mode NAT

IP Address 192.168.1.254 *

Subnet Mask 255.255.255.0 *

IP PNP: Users can use static IP address to connect to the system. Regardless of what the IP address at the user end is, users can still be authenticated through W1310R and access the network.

User Authentication: Choose to enable or disable this function. If **"User Authentication"** is disabled, users can access Internet without being authenticated.

Operation Mode: Choose one of the two modes, **NAT** mode and **Router** mode, by the requirements.

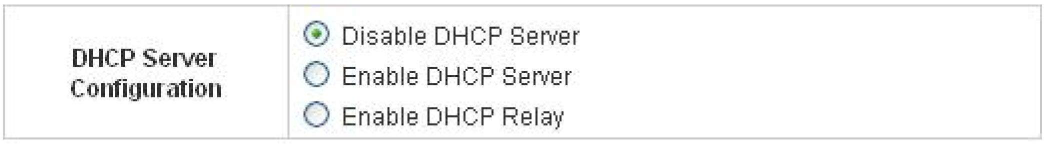
IP Address: Enter the desired IP address for the LAN1 & LAN2 port.

Subnet Mask: Enter the desired subnet mask for the LAN1 & LAN2 port.

- **DHCP Server Configuration**

There are three methods to set the DHCP server: **Disable DHCP Server**, **Enable DHCP Server** and **Enable DHCP Relay**.

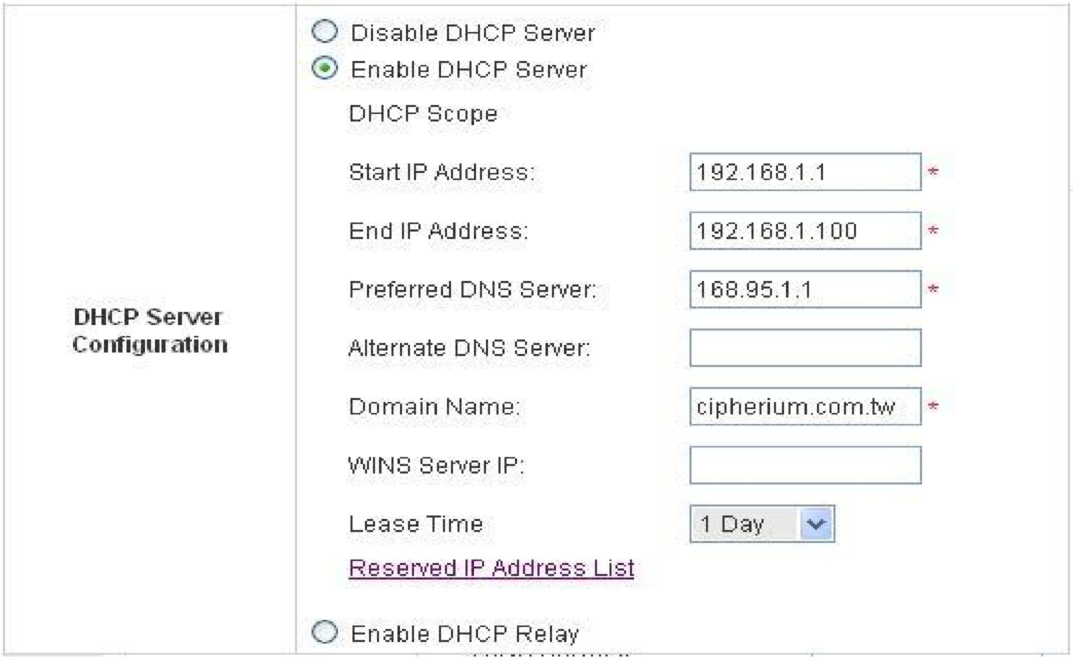
1. **Disable DHCP Server:** Disable DHCP Server function.



DHCP Server Configuration

● Disable DHCP Server
○ Enable DHCP Server
○ Enable DHCP Relay

2. **Enable DHCP Server:** Choose **"Enable DHCP Sever"** function and set the appropriate configuration for the DHCP server. The fields with red asterisks are required to be filled in.



DHCP Server Configuration

○ Disable DHCP Server
● Enable DHCP Server

DHCP Scope

Start IP Address: 192.168.1.1 *

End IP Address: 192.168.1.100 *

Preferred DNS Server: 168.95.1.1 *

Alternate DNS Server:

Domain Name: cipherium.com.tw *

WINS Server IP:

Lease Time 1 Day

Reserved IP Address List

○ Enable DHCP Relay

DHCP Scope: Enter the **"Start IP Address"** and the **"End IP Address"** of this DHCP block. These fields define the IP address range that will be assigned to the Public LAN clients.

Preferred DNS Server: The primary DNS server for the DHCP.

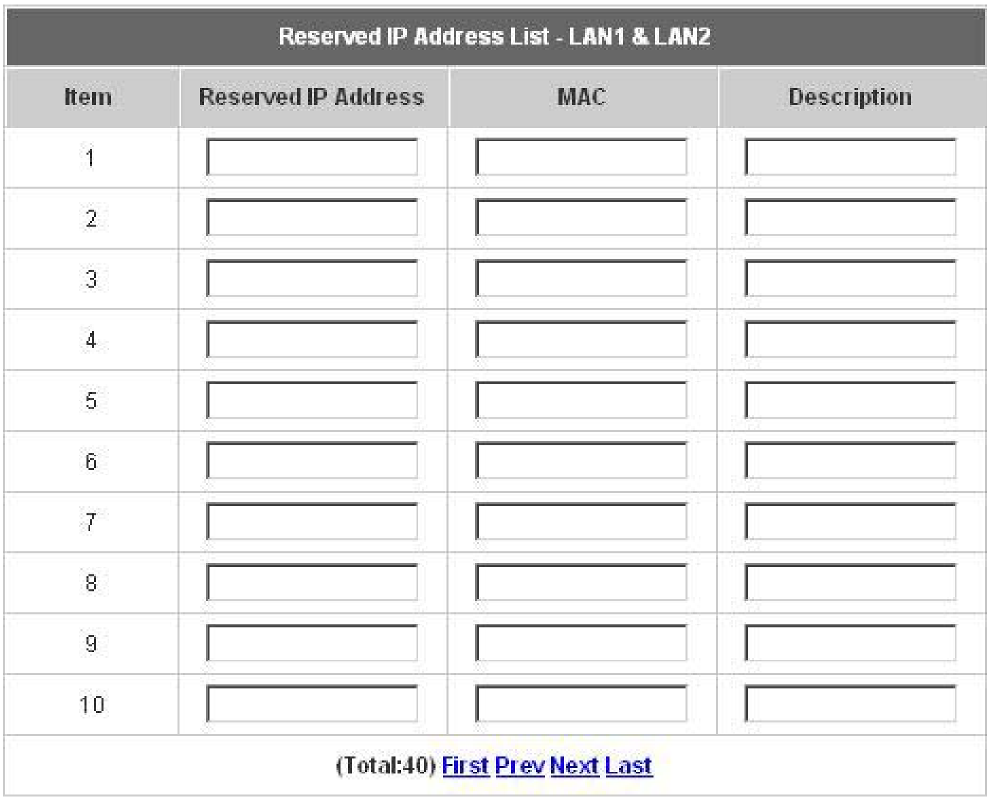
Alternate DNS Server: The substitute DNS server for the DHCP.

Domain Name: Enter the domain name.

WINS IP Address: Enter the IP address of WINS

Lease Time: Choose the time to change the DHCP.

Reserved IP Address List: For reserved IP address settings in detail, please click the hyperlink of ***Reserved IP Address***. If using the **Reserved IP Address List** function for IP address outside the DHCP range is desired, click on the **Reserved IP Address List** on the management interface. Then, the setup of the Reserved IP Address List as shown in the following figure will appear. Enter the related Reserved IP Address, MAC, and some description (not mandatory). Click ***Apply*** to complete the setup.

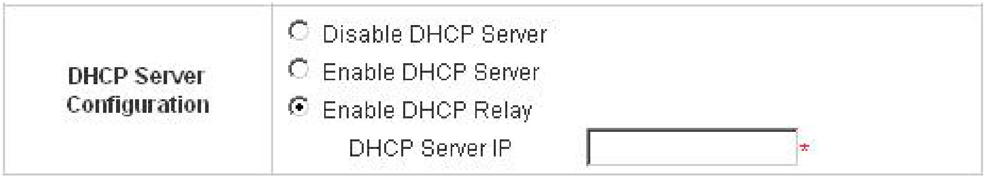


Reserved IP Address List - LAN1 & LAN2

Item	Reserved IP Address	MAC	Description
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

(Total:40) First Prev Next Last

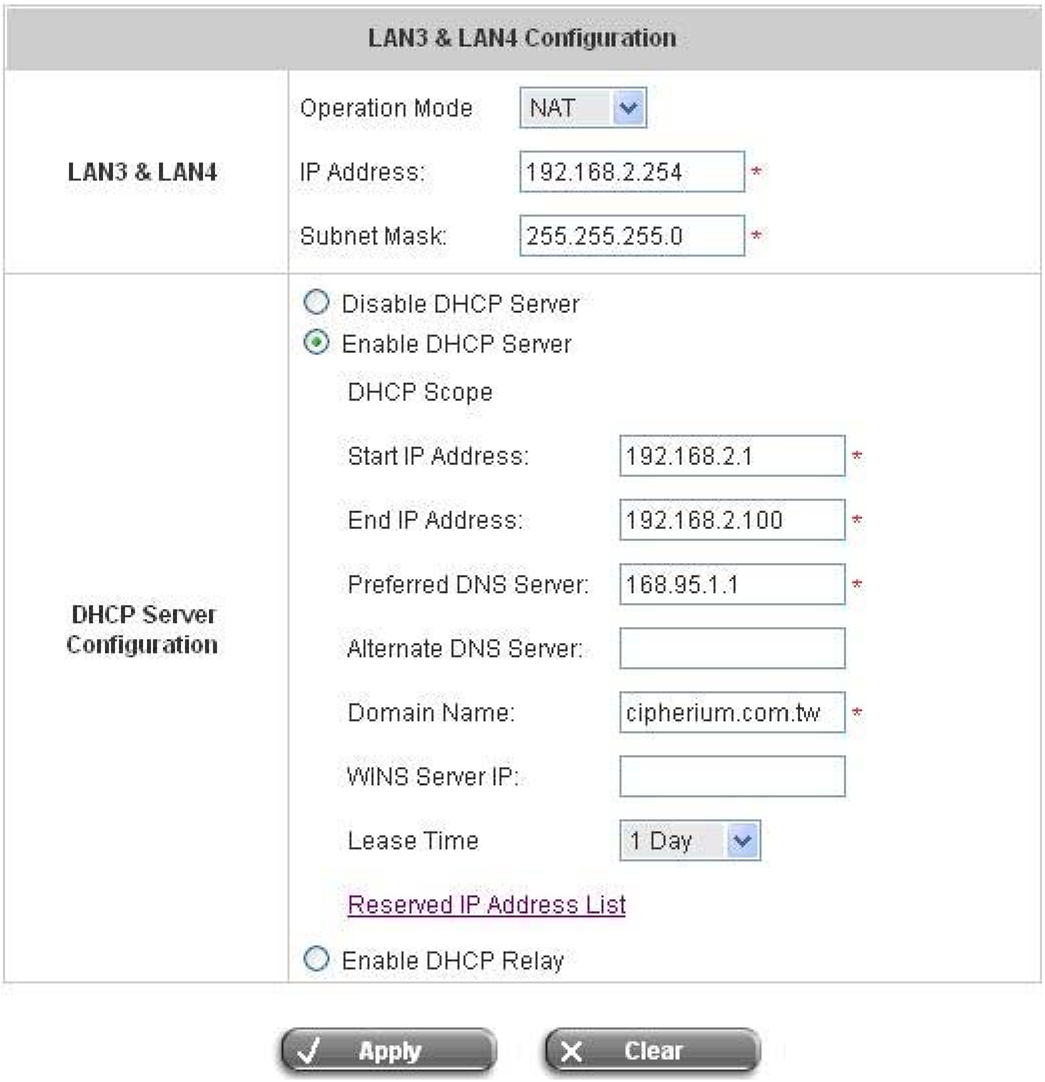
3. **Enable DHCP Relay:** If enabling this function is desired, other DHCP Server IP address must be specified. See the following figure.



DHCP Server Configuration	○ Disable DHCP Server ○ Enable DHCP Server ● Enable DHCP Relay DHCP Server IP ______ *

4.1.5 LAN3 & LAN4 Configuration

In this section, set the related configuration for LAN3/LAN4 port and DHCP server.



LAN3 & LAN4 Configuration

LAN3 & LAN4

Operation Mode: NAT

IP Address: 192.168.2.254 *

Subnet Mask: 255.255.255.0 *

DHCP Server Configuration

○ Disable DHCP Server

● Enable DHCP Server

DHCP Scope

Start IP Address: 192.168.2.1 *

End IP Address: 192.168.2.100 *

Preferred DNS Server: 168.95.1.1 *

Alternate DNS Server:

Domain Name: cipherium.com.tw *

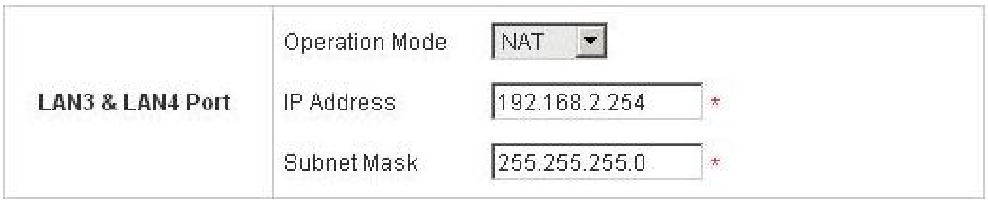
WINS Server IP:

Lease Time: 1 Day

Reserved IP Address List

○ Enable DHCP Relay

- **LAN3 & LAN4 Port**



LAN3 & LAN4 Port

Operation Mode: NAT

IP Address: 192.168.2.254 *

Subnet Mask: 255.255.255.0 *

Operation Mode: Choose one of the two modes, **NAT** mode and **Router** mode, by the requirements.

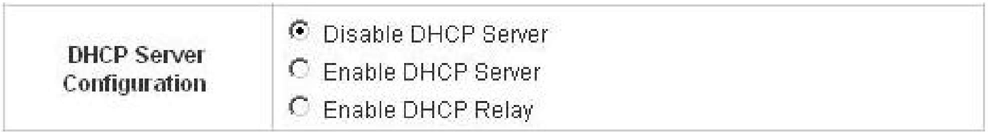
IP Address: Enter the desired IP address for the LAN3 & LAN4 port.

Subnet Mask: Enter the desired subnet mask for the LAN3 & LAN4 port.

- **DHCP Server Configuration**

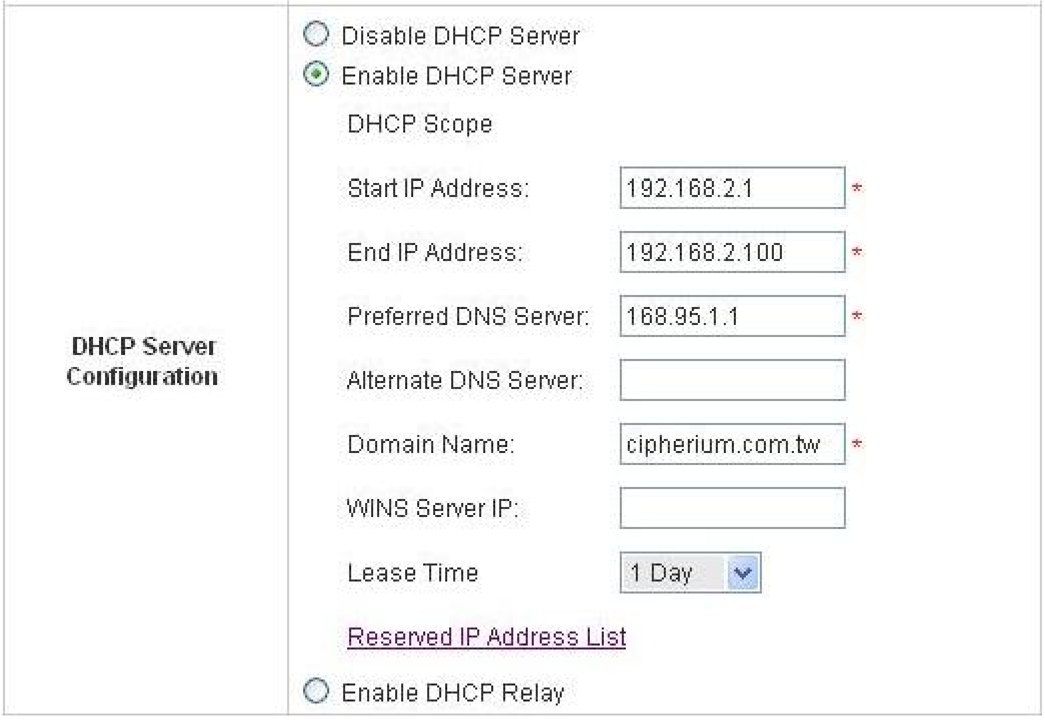
There are three methods to set the DHCP server: **Disable DHCP Server**, **Enable DHCP Server** and **Enable DHCP Relay**.

1. **Disable DHCP Server:** Disable DHCP Server function.



DHCP Server Configuration	● Disable DHCP Server ○ Enable DHCP Server ○ Enable DHCP Relay

2. **Enable DHCP Server:** Choose **"Enable DHCP Sever"** function and set the appropriate configuration for the DHCP server. The fields with red asterisks are required to be filled in.



DHCP Server Configuration

○ Disable DHCP Server
● Enable DHCP Server
DHCP Scope

Start IP Address:	192.168.2.1	*
End IP Address:	192.168.2.100	*
Preferred DNS Server:	168.95.1.1	*
Alternate DNS Server:		
Domain Name:	cipherium.com.tw	*
WINS Server IP:		
Lease Time	1 Day	

Reserved IP Address List

○ Enable DHCP Relay

DHCP Scope: Enter the **"Start IP Address"** and the **"End IP Address"** of this DHCP block. These fields define the IP address range that will be assigned to the Private LAN clients.

Preferred DNS Server: The primary DNS server for the DHCP.

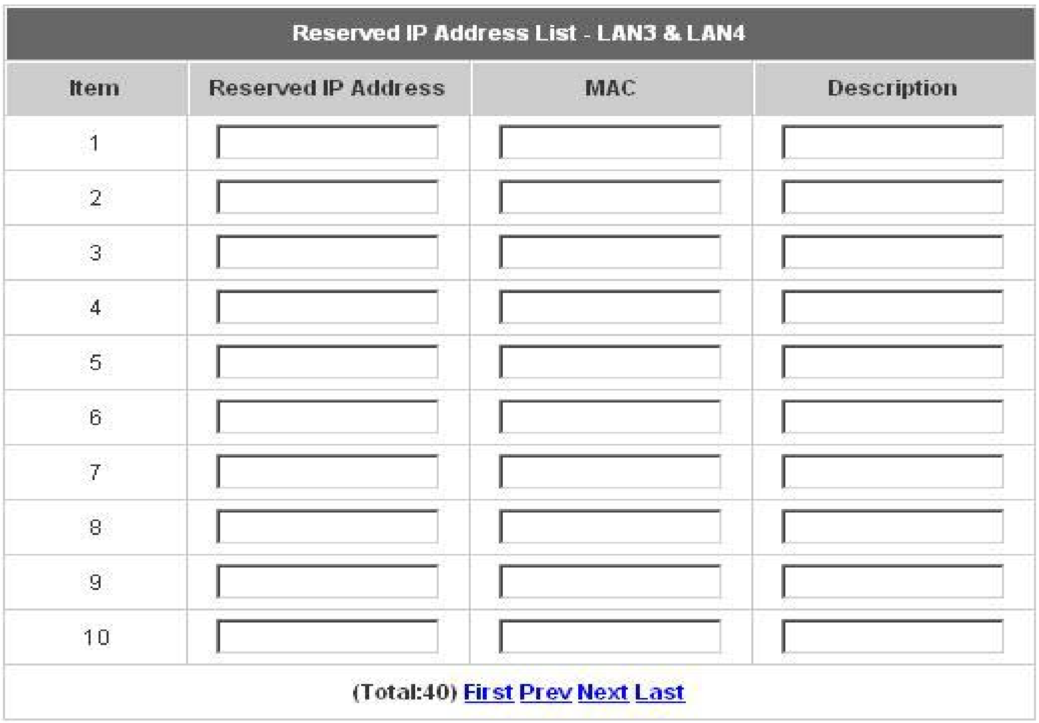
Alternate DNS Server: The substitute DNS server for the DHCP.

Domain Name: Enter the domain name.

WINS IP Address: Enter the IP address of WINS.

Lease Time: Choose the time to update the DHCP.

Reserved IP Address List: For reserved IP address settings in detail, please click the hyperlink of ***Reserved IP Address***. If using the **Reserved IP Address List** function for IP address outside the DHCP range is desired, click the **Reserved IP Address List** on the management interface. The setup of the Reserved IP Address List as shown in the following figure will appear. Enter the related Reserved IP Address, MAC, and some description (not mandatory). Click ***Apply*** to complete the setup.

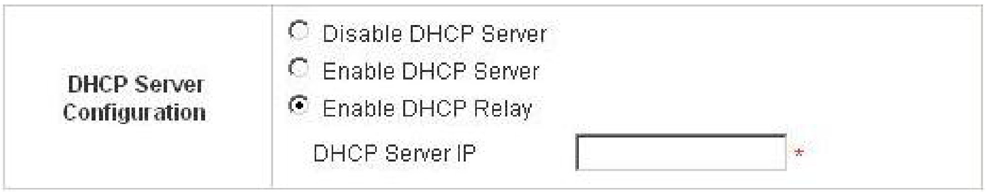


Reserved IP Address List - LAN3 & LAN4

Item	Reserved IP Address	MAC	Description
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

(Total:40) First Prev Next Last

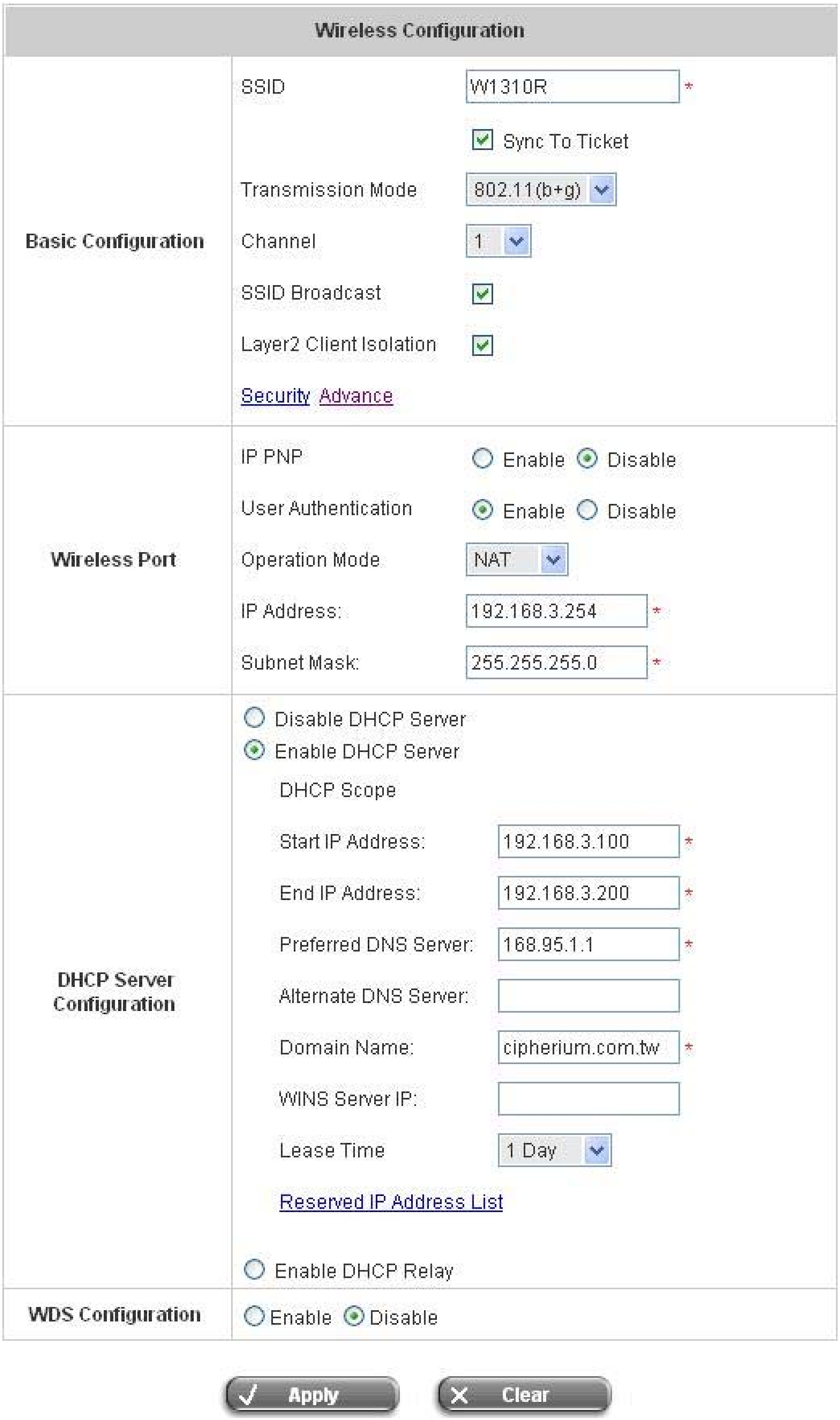
3. **Enable DHCP Relay:** If enabling this function is desired, other DHCP Server IP address must be specified. See the following figure.



DHCP Server Configuration	○ Disable DHCP Server ○ Enable DHCP Server ● Enable DHCP Relay DHCP Server IP ▭ *

4.1.6 Wireless Configuration

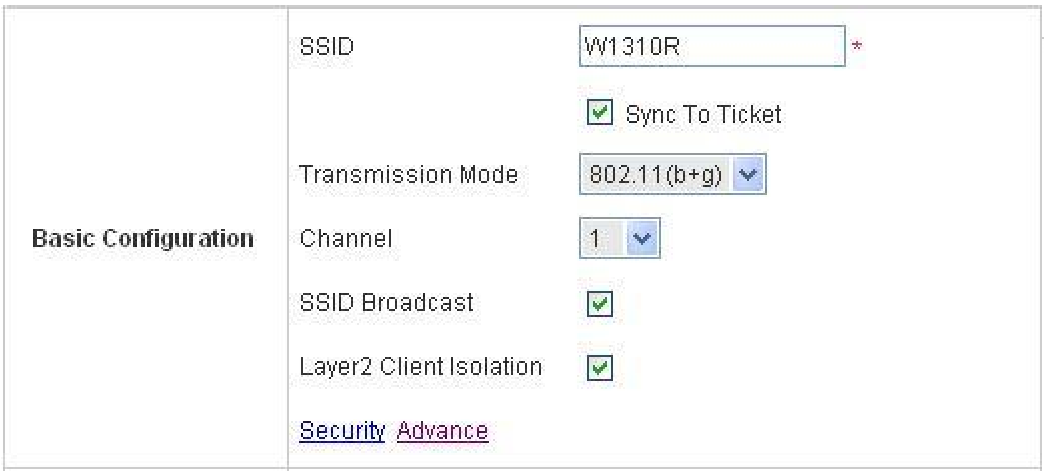
This section is for setting related configurations for the wireless port.



Wireless Configuration

Basic Configuration	SSID	W1310R *
		☑ Sync To Ticket
	Transmission Mode	802.11(b+g)
	Channel	1
	SSID Broadcast	☑
	Layer2 Client Isolation	☑
	Security Advance	
Wireless Port	IP PNP	○ Enable ● Disable
	User Authentication	● Enable ○ Disable
	Operation Mode	NAT
	IP Address:	192.168.3.254 *
	Subnet Mask:	255.255.255.0 *
DHCP Server Configuration	○ Disable DHCP Server	
	● Enable DHCP Server	
	DHCP Scope	
	Start IP Address:	192.168.3.100 *
	End IP Address:	192.168.3.200 *
	Preferred DNS Server:	168.95.1.1 *
	Alternate DNS Server:	
	Domain Name:	cipherium.com.tw *
	WINS Server IP:	
	Lease Time	1 Day
	Reserved IP Address List	
	○ Enable DHCP Relay	
WDS Configuration	○ Enable ● Disable	

- **Wireless Configuration**



Basic Configuration	SSID	W1310R *
		☑ Sync To Ticket
	Transmission Mode	802.11(b+g)
	Channel	1
	SSID Broadcast	☑
	Layer2 Client Isolation	☑
	Security Advance	

SSID: The SSID is the unique name shared among all devices in a wireless network. The SSID must be the same for all devices in the wireless network. It is case sensitive, must not exceed 32 characters and may be any character on the keyboard. Administrators can give a new name in this field or use the default name.

Sync to Ticket: Synchronize the SSID of ticket with this system.

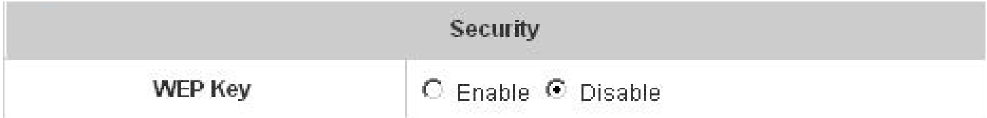
Channel: Select the appropriate channel from the list to correspond to the network settings; for example, 1 to 11 channels are suitable for the North America area. All points in the wireless network must use the same channel in order to make sure correct connection.

Transmission Mode: There are 2 modes to select from, **802.11b** (2.4G, 1~11Mbps) and **802.11 (b+g)** (2.4G, 1~11Mbps and 2.4G, 54Mbps).

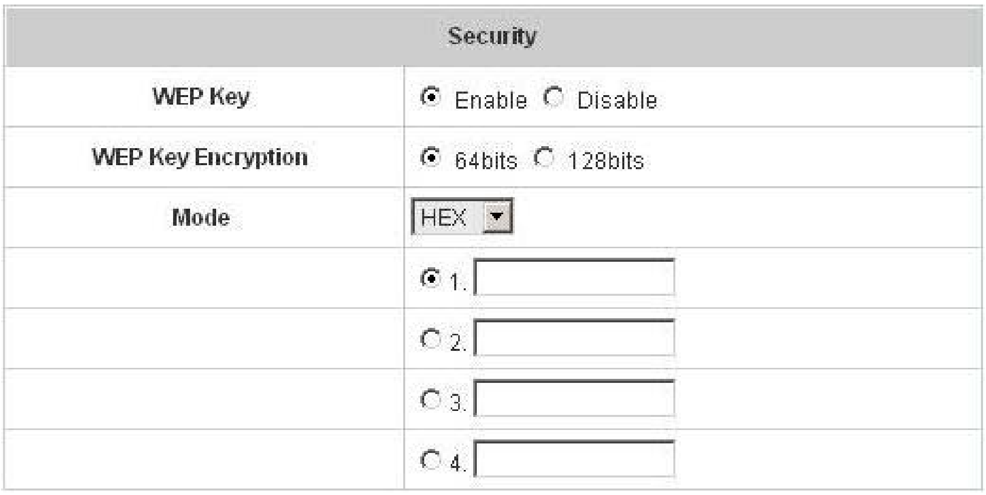
SSID Broadcast: Select to enable the SSID broadcast in the network. When configuring the network, this function may be enabled but should be disabled when configuration is finished. Since when SSID Broadcast is enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to the network.

Layer2 Client Isolation: This function can be enabled to isolate any client from each other.

Security: For security settings in detail, please click the hyperlink ***Security*** to go into the **Security** page. Choose **"Enable"** to configure the setting.



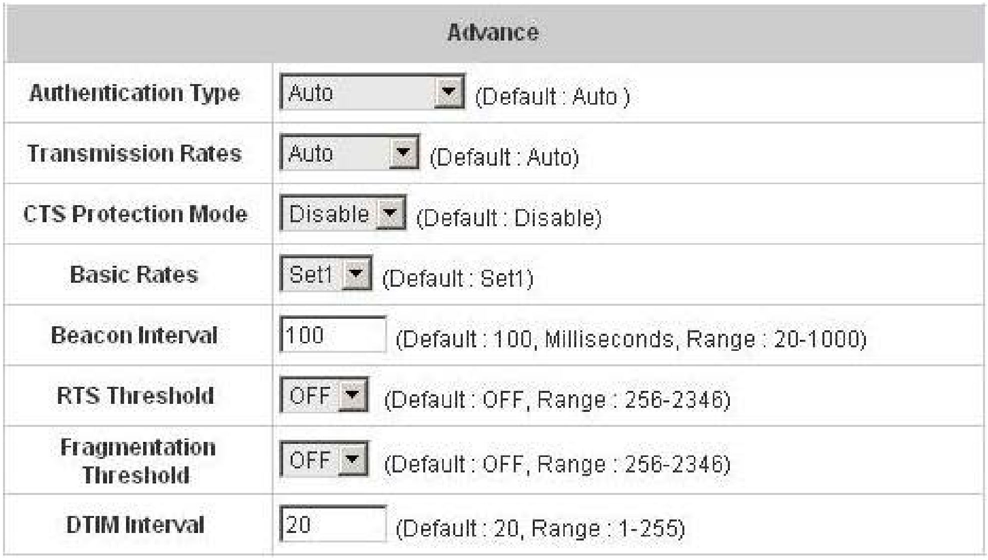
Security	
WEP Key	○ Enable ● Disable



Security	
WEP Key	● Enable ○ Disable
WEP Key Encryption	● 64bits ○ 128bits
Mode	HEX
	● 1.
	○ 2.
	○ 3.
	○ 4.

1. **WEP Key: W**ired **E**quivalent **P**rivacy. If using this function is desired, please choose **"Enable"**.
2. **WEP Key Encryption**: This is a data privacy mechanism based on a 64-bit or 128-bits shared key algorithm.
3. **Mode:** There are two types of encryption, **HEX** and **ASCII**. After selecting one of them, please enter the related information in the blanks below.

Advance: For advance settings in detail, please click the hyperlink ***Advance*** to go into the **Advance** page.

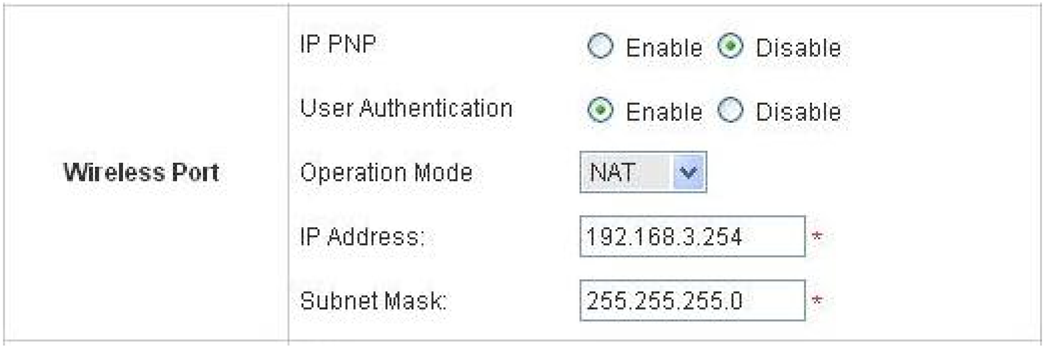


Advance	
Authentication Type	Auto (Default : Auto)
Transmission Rates	Auto (Default : Auto)
CTS Protection Mode	Disable (Default : Disable)
Basic Rates	Set1 (Default : Set1)
Beacon Interval	100 (Default : 100, Milliseconds, Range : 20-1000)
RTS Threshold	OFF (Default : OFF, Range : 256-2346)
Fragmentation Threshold	OFF (Default : OFF, Range : 256-2346)
DTIM Interval	20 (Default : 20, Range : 1-255)

1. **Authentication Type:** The default value is **Auto**. When **"Auto"** is selected, it will auto-detect to authenticate by **Shared Key** type or **Open System** type. **Shared Key** is used such that both the sender and the recipient share a WEP key for authentication. **Open Key** is that the sender and the recipient do not share a WEP key for authentication. All points on the network must use the same authentication type.
2. **Transmission Rates:** The default value is **Auto**. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of this particular wireless network. Select from a range of transmission speeds or keep the default setting, **Auto**, to make the Access Point use the fastest possible data rate automatically.

3. **CTS Protection Mode:** The default value is **Disable**. When enabled, a protection mechanism will ensure that the 802.11b devices can connect to Access Point and not be affected by many other 802.11g devices existing at the same time. However, the performance of this 802.11g devices may decrease.
4. **Basic Rate:** The basic rate offers three options, **All**, **Set1** and **Set2** and the default value is **Set1**. Depending on the wireless mode selected, W1310R will deliver a pre-defined data rate. Select **"All"** to activate all transmission rates to be compatible with the majority of the devices.
5. **Beacon Interval:** Enter a value between 20 and 1000 msec. The default value is 100 milliseconds. The entered time means how often the signal transmission occurs between the access point and the wireless network.
6. **RTS Threshold: R**eady **T**o **S**end threshold. The range is from 256 to 2346 and the default is **OFF**. The administrator could set the value which is the time to wait before sending another packet. It is recommended that the value remains in the range of 256 to 2346.
7. **Fragmentation Threshold:** The range is from 256 to 2346 and the default is **OFF**. The value specifies the maximum size of packet allowed before data is fragmented into multiple packets. It should be remained in the range of 256 to 2346. A smaller value results smaller packets but with a larger numbers of packets in transmission.
8. **DTIM Interval:** This function indicates the interval of the **D**elivery **T**raffic **I**ndication **M**essage (DTIM). DTIM is a countdown function to inform clients to listen to broadcast and multicast messages. When an Access Point has buffered broadcast or multicast message from an associated client, it sends the next DTIM at this interval rate (from 1~255), the client will hear the beacons.

- **Wireless Configuration**



Wireless Port	IP PNP	○ Enable ● Disable
	User Authentication	● Enable ○ Disable
	Operation Mode	NAT
	IP Address:	192.168.3.254 *
	Subnet Mask:	255.255.255.0 *

IP PNP: Use any IP address to connect to the system. Regardless of what the IP address at the users end is, they can still be authenticated through W1310R and access the network.

User Authentication: If **"User Authentication"** is disabled, **"Specific Route Profile"** needs to be specified for the users to access Internet.

Operation Mode: Choose one of the two modes, **NAT** mode and **Router** mode, by the requirements.

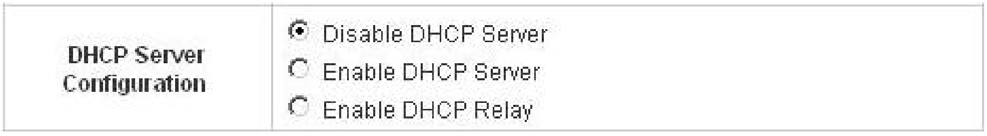
IP Address: Enter desired IP address for the wireless port.

Subnet Mask: Enter desired subnet mask for the wireless port.

- **DHCP Server Configuration**

There are three methods to set the DHCP server: **Disable DHCP Server**, **Enable DHCP Server** and **Enable DHCP Relay**.

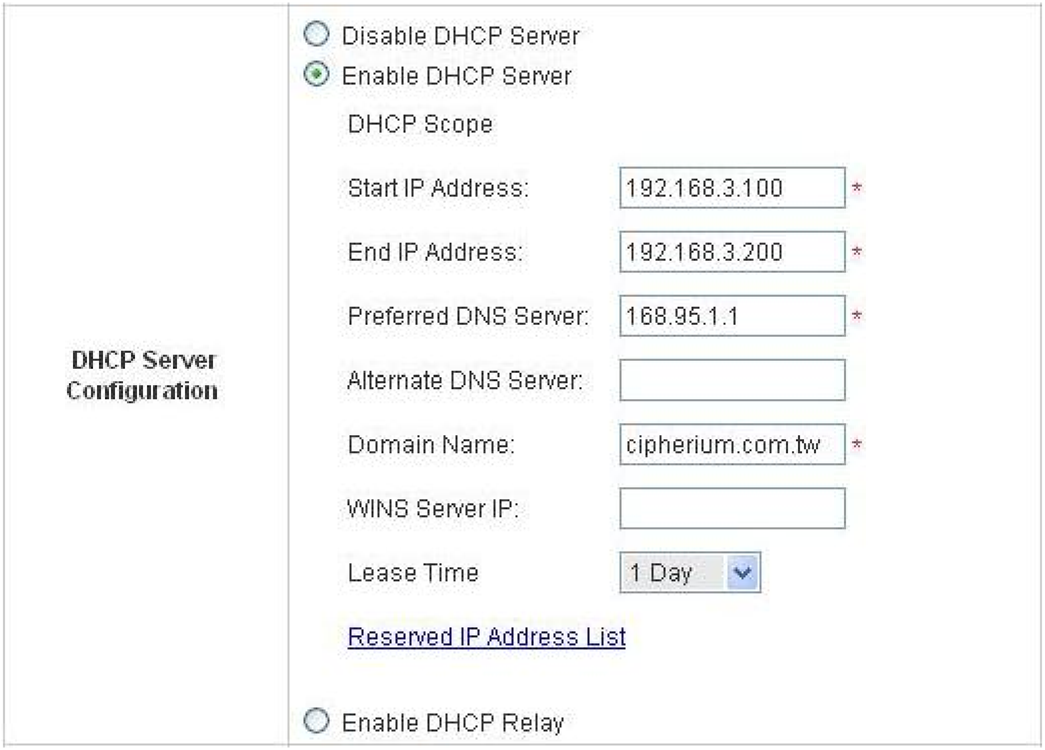
1. **Disable DHCP Server:** Disable the DHCP Server function.



DHCP Server Configuration

● Disable DHCP Server
○ Enable DHCP Server
○ Enable DHCP Relay

2. **Enable DHCP Server:** Choose **"Enable DHCP Sever"** function and set the appropriate configuration for the DHCP server. The fields with red asterisks are required to be filled in.



DHCP Server Configuration

○ Disable DHCP Server
● Enable DHCP Server

DHCP Scope

Start IP Address:	192.168.3.100 *
End IP Address:	192.168.3.200 *
Preferred DNS Server:	168.95.1.1 *
Alternate DNS Server:	
Domain Name:	cipherium.com.tw *
WINS Server IP:	
Lease Time	1 Day

Reserved IP Address List

○ Enable DHCP Relay

DHCP Scope: Enter the **"Start IP Address"** and the **"End IP Address"** of this DHCP block. These fields define the IP address range that will be assigned to the Wireless LAN clients.

Preferred DNS Server: The primary DNS server for the DHCP.

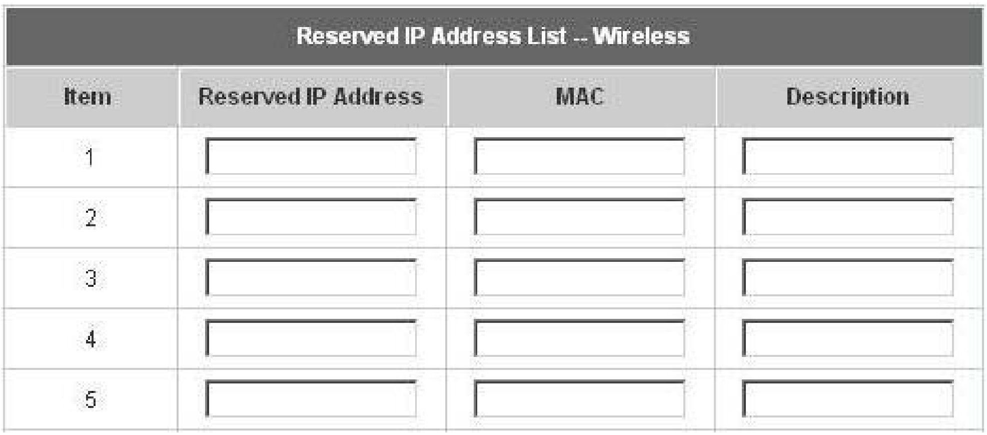
Alternate DNS Server: The substitute DNS server for the DHCP.

Domain Name: Enter the domain name.

WINS IP Address: Enter the IP address of WINS.

Lease Time: Choose the time to change the DHCP.

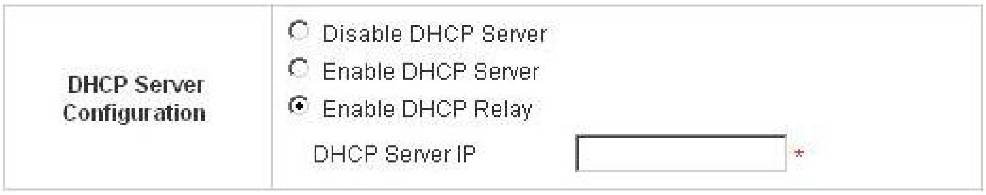
Reserved IP Address List: For reserved IP address settings in detail, please click the hyperlink of ***Reserved IP Address***. If using the **Reserved IP Address List** function for IP address outside the DHCP range is desired, click on the **Reserved IP Address List** on the management interface. The setup of the Reserved IP Address List as shown in the following figure will appear. Enter the related Reserved IP Address, MAC, and some description (not mandatory). Click ***Apply*** to complete the setup.



Reserved IP Address List -- Wireless

Item	Reserved IP Address	MAC	Description
1			
2			
3			
4			
5			

3. **Enable DHCP Relay:** If enabling this function is desired, other DHCP Server IP address must be specified. See the following figure.

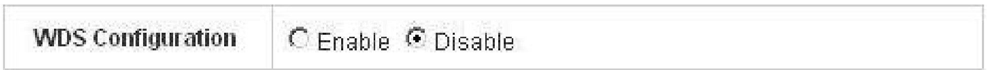


DHCP Server Configuration

○ Disable DHCP Server
○ Enable DHCP Server
● Enable DHCP Relay
DHCP Server IP *

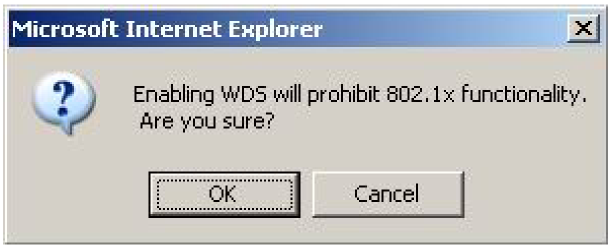
- **WDS configuration**

This function can extend the range of accessing the network. It has to work with a repeater. A repeater is a peripheral device supporting W1310R to extend the wireless access by receiving requests from APs or clients and passing the requests to W1310R to obtain authentication.



WDS Configuration ○ Enable ● Disable

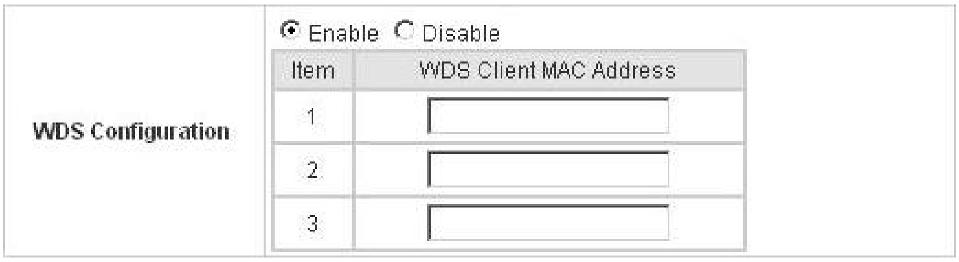
When "Enable" is clicked, there will be a warning box showing up.



Microsoft Internet Explorer

Enabling WDS will prohibit 802.1x functionality.
Are you sure?

If this function is enabled, please enter the MAC address of repeater in the blanks. A maximum of three repeaters are supported.



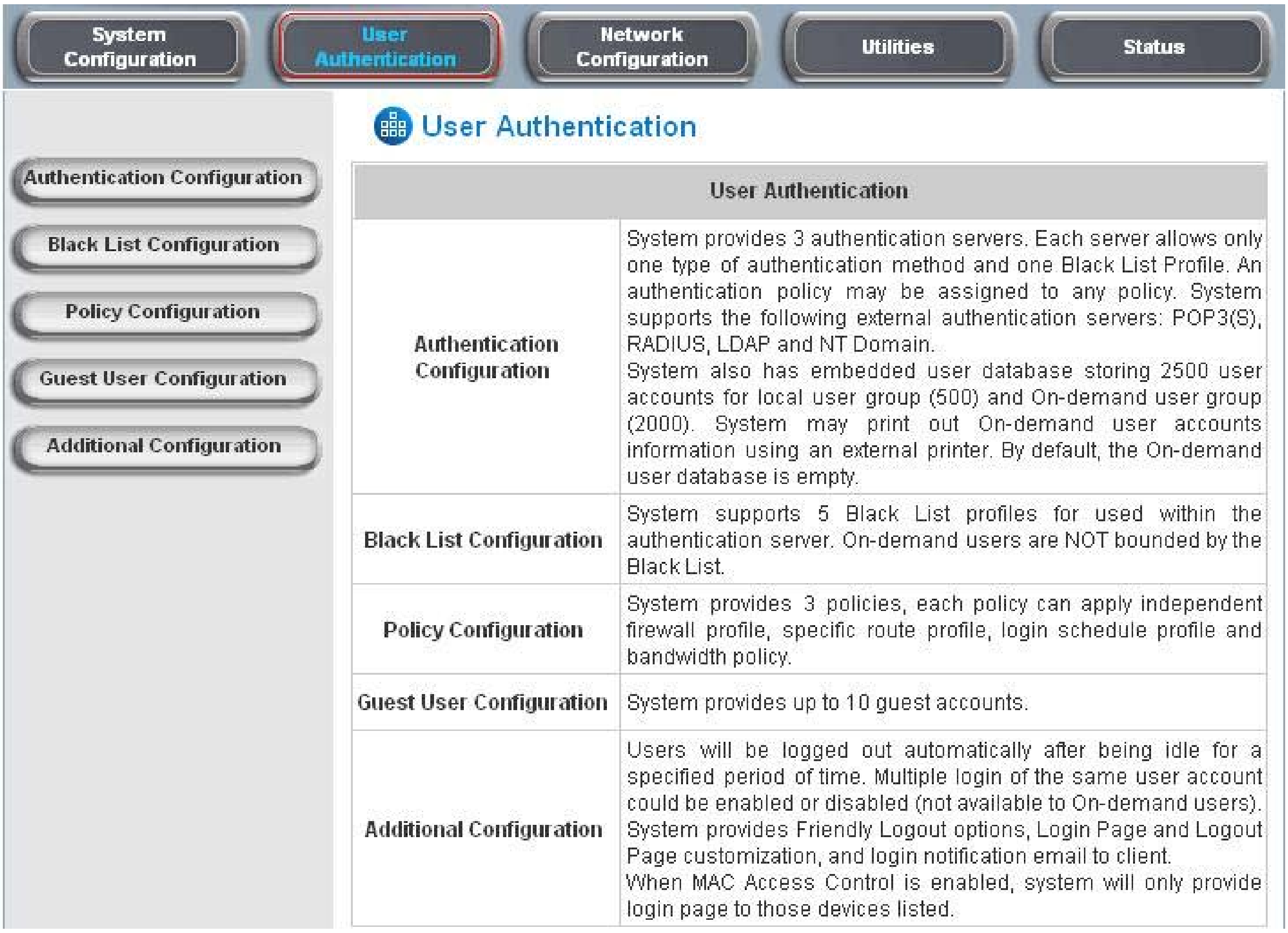
WDS Configuration

● Enable ○ Disable

Item	WDS Client MAC Address
1	
2	
3	

4.2 User Authentication

This section includes the following functions: **Authentication Configuration**, **Black List Configuration**, **Policy Configuration**, **Guest User Configuration** and **Additional Configuration**.

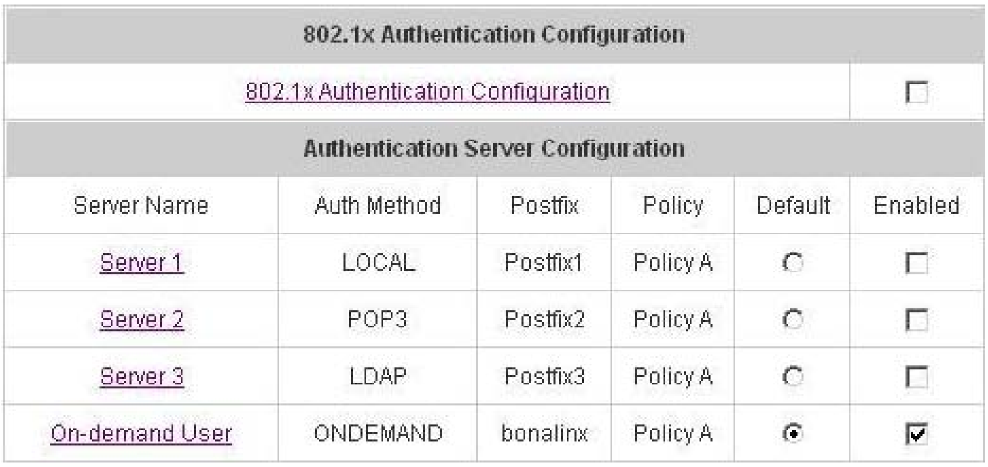


User Authentication

User Authentication	
Authentication Configuration	System provides 3 authentication servers. Each server allows only one type of authentication method and one Black List Profile. An authentication policy may be assigned to any policy. System supports the following external authentication servers: POP3(S), RADIUS, LDAP and NT Domain. System also has embedded user database storing 2500 user accounts for local user group (500) and On-demand user group (2000). System may print out On-demand user accounts information using an external printer. By default, the On-demand user database is empty.
Black List Configuration	System supports 5 Black List profiles for used within the authentication server. On-demand users are NOT bounded by the Black List.
Policy Configuration	System provides 3 policies, each policy can apply independent firewall profile, specific route profile, login schedule profile and bandwidth policy.
Guest User Configuration	System provides up to 10 guest accounts.
Additional Configuration	Users will be logged out automatically after being idle for a specified period of time. Multiple login of the same user account could be enabled or disabled (not available to On-demand users). System provides Friendly Logout options, Login Page and Logout Page customization, and login notification email to client. When MAC Access Control is enabled, system will only provide login page to those devices listed.

4.2.1 Authentication Configuration

This function is to configure the settings for 802.1x authentication, authentication server, and on-demand user authentication.



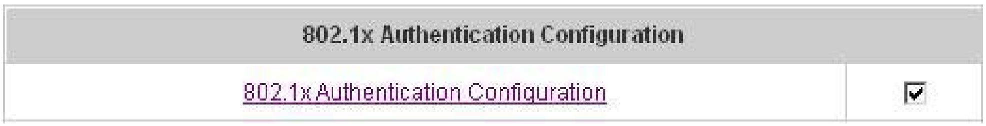
802.1x Authentication Configuration

802.1x Authentication Configuration	□

Authentication Server Configuration

Server Name	Auth Method	Postfix	Policy	Default	Enabled
Server 1	LOCAL	Postfix1	Policy A	○	□
Server 2	POP3	Postfix2	Policy A	○	□
Server 3	LDAP	Postfix3	Policy A	○	□
On-demand User	ONDEMAND	bonalinx	Policy A	●	☑

- **802.1x Authentication Configuration**

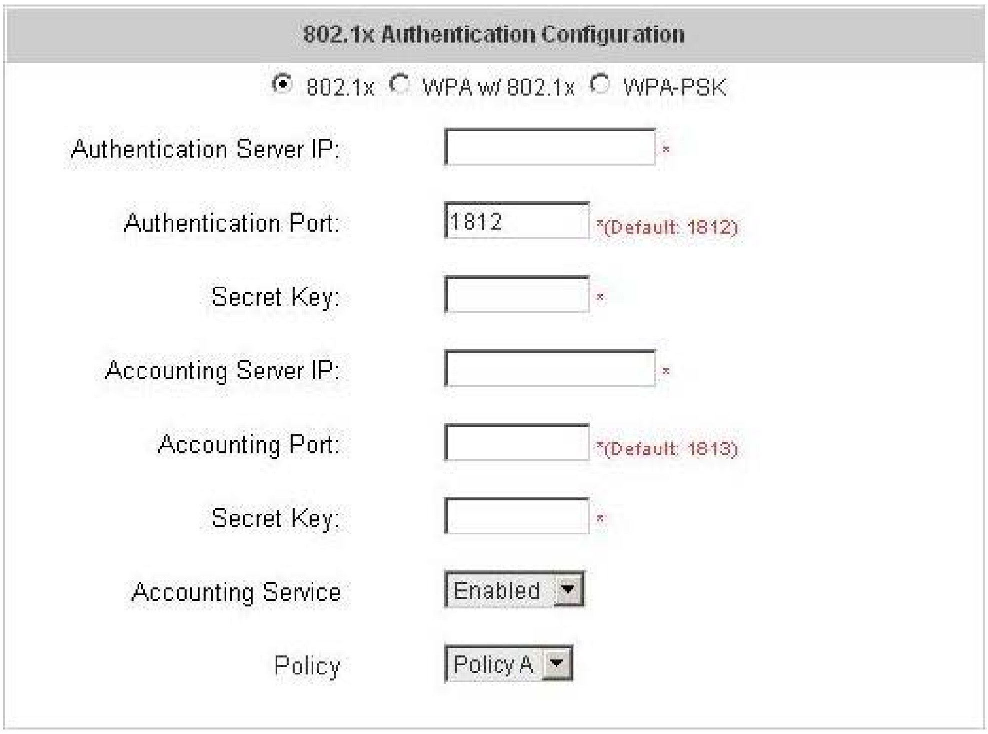


802.1x Authentication Configuration

802.1x Authentication Configuration	☑

There are two kinds of 802.1x authentication methods and one encryption mechanism: **802.1x**, **WPA w/ 802.1x** and **WPA-PSK**. Click the hyperlink ***802.1x Authentication Configuration*** to set the related configurations. After completing and clicking ***Apply*** to save the settings, go back to the previous page to check the item box next to ***802.1x Authentication Configuration*** to enable this function. When using 802.1x authentications, the RADIUS attributes such as idle timeout or session timeout have no effect.

1. **802.1x:** Enable the 802.1x authentication method. The fields with red asterisks are required to be filled in.



802.1x Authentication Configuration

● 802.1x ○ WPA w/ 802.1x ○ WPA-PSK

Authentication Server IP:	*
Authentication Port:	1812 *(Default: 1812)
Secret Key:	*
Accounting Server IP:	*
Accounting Port:	*(Default: 1813)
Secret Key:	*
Accounting Service	Enabled ▼
Policy	Policy A ▼

Authentication Server IP: The IP address or domain name of the Authentication server.

Authentication Port: The port of the authentication server. The default value is 1812.

Secret Key: The secret key of the authentication sever for encryption and decryption.

Accounting Server IP: The IP address or domain name of the accounting server.

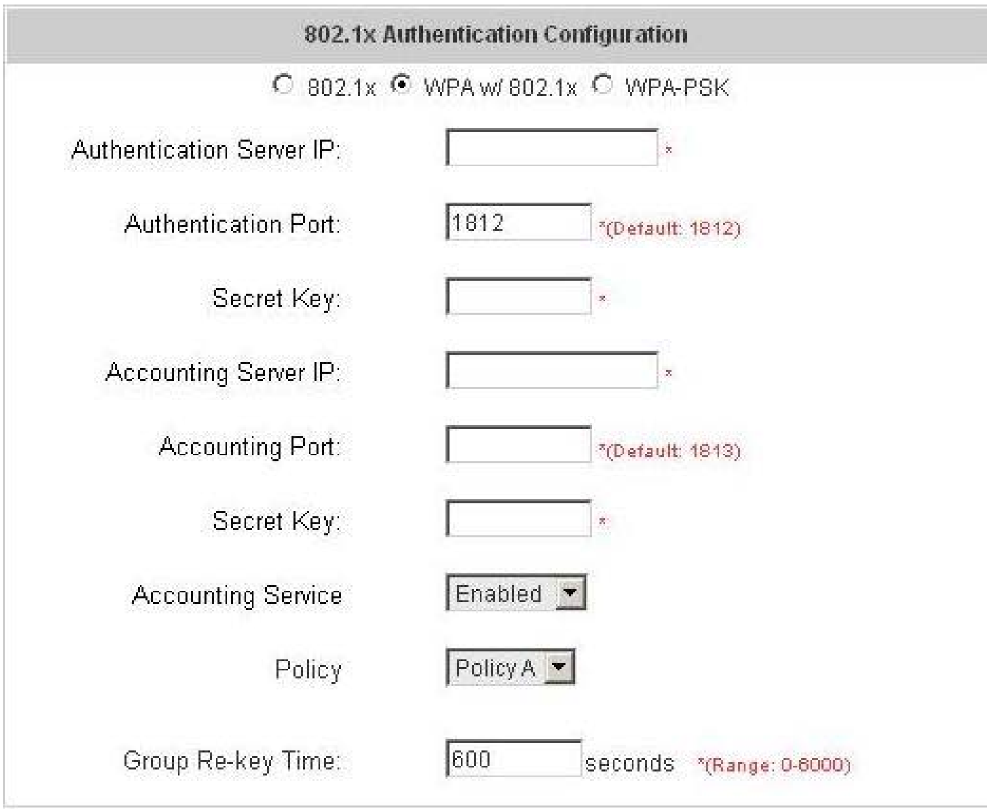
Account Port: The port of the accounting server. The default value is 1813.

Secret Key: The secret key of the accounting sever for encryption and decryption.

Accounting Service: Enable or disable accounting service.

Policy: There are three policies to select from.

2. **WPA x/802.1x:** Enable the supported WPA-Enterprise, Wireless Protection Access with 802.1x.



802.1x Authentication Configuration

○ 802.1x ● WPA w/ 802.1x ○ WPA-PSK

Authentication Server IP: *

Authentication Port: 1812 *(Default: 1812)

Secret Key: *

Accounting Server IP: *

Accounting Port: *(Default: 1813)

Secret Key: *

Accounting Service: Enabled

Policy: Policy A

Group Re-key Time: 600 seconds *(Range: 0-6000)

Authentication Server IP: The IP address or domain name of the Authentication server.

Authentication Port: The port of the authentication server. The default value is 1812.

Secret Key: The secret key of the authentication sever for encryption and decryption.

Accounting Server IP: The IP address or domain name of the accounting server.

Account Port: The port of the accounting server. The default value is 1813.

Secret Key: The secret key of the accounting sever for encryption and decryption.

Accounting Service: Enable or disable accounting service.

Policy: There are three policies to select from.

Group Re-key Time: Time interval for re-keying broadcast/multicast keys in seconds. The maximum is 6000 sec.