CIPHERIUM Repeater

Administrator's Manual

Version 1.0.1

© 2004 Cipherium Systems Co., Ltd.

Copyright

The intellectual property rights and copyright of this manual belong to Cipherium Systems Co., Ltd. and are protected by the R.O.C. copyright laws and international copyright laws. No part or the manual in its entirety may be transshipped, transmitted, duplicated, distributed, displayed, published, or broadcasted in any form or by any means without the prior written permission of Cipherium Systems Co., Ltd. The trademarks mentioned in the manual belong to the owners of the respective registered companies or organizations.

Please contact Cipherium Systems if you have any questions on copyright:

Tel.: +886-2-2731-6669

Fax: +886-2-2731-7776

E-mail：sales@cipherium.com.tw

© 2004 Cipherium Systems Co., Ltd.

Table of Contents

1. Preface 1

1.1. Brief Introduction of Repeater 1

1.2. Before you Read 2

1.2.1. Audience 2

1.2.2. Document Convention 2

2. Product Description 3

2.1. Package Contents 3

2.2. Front Panel 3

2.3. Hardware Specifications 5

2.4. Technical Specifications 5

2.4.1. Standards 5

2.4.2. Networking 6

2.4.3. Firewall 6

2.4.4. User Management 6

2.4.5. Administration 7

2.4.6. Accounting 7

3. Installation 8

3.1. Installing the Repeater 8

3.1.1. System Requirements 8

3.1.2. Installation Procedure 8

3.1.3. Setting up the PC for the Public LAN and Private LAN 9

3.2. Getting Started 17

3.2.1. System Concept 17

3.2.2. Connecting Network Devices 18

3.2.3. Begin Installation 20

4. Console Interface 27

4.1. Main Menu of Console interface 27

4.2. Utilities for network debugging of Console interface 28

4.3. Change admin password of Console interface 29
4.4. Reload factory default of Console interface 30
4.5. Restart Cipherium Repeater 30

5. Web Management Interface 31

5.1. System Configuration 31
5.1.1. Configuration Wizard 32
5.1.2. System Information.....45
5.1.3. WAN Configuration 47
5.1.4. Authentication Configuration 49
5.1.5. Private Configuration 61
5.2. User Authentication 64
5.2.1 Authentication Policy 64
5.2.2 Group Configuration 75
5.2.3 Black List Configuration 76
5.2.4 Guest User Configuration 78
5.2.5 Roaming Configuration 79
5.2.6 Additional Configuration.....81
5.2.7 On-demand User Configuration.....86
5.3 Group Profile 90
5.3.1 Firewall Profile 91
5.3.2 Specific Route Profiles.....93
5.3.3 Login Schedule Profiles 95
5.4 Network Configuration.....95
5.4.1 Network Address Translate.....95
5.4.2 Privilege List.....98
5.4.3 Monitor IP List 100
5.4.4 Walled Garden List 102
5.4.5 Proxy Server Properties.....103
5.4.6 Dynamic DNS 104
5.5 Utilities.....105
5.5.1 Change Password 105
5.5.2 Backup / Restore Strategy 106

5.5.3 Firmware Upgrade 107
5.5.4 Restart 108
5.6 Status 108
5.6.1 System Status 109
5.6.2 Interface Status 112
5.6.3 Current Users 114
5.6.4 Traffic History 114
5.6.5 DHCP Server Reporting 115
5.6.6 Notify Configuration 116

6 Technical Support 117

7 Appendix - Windows TCP/IP Setup 118

7.3 Check the TCP/IP Setup of Windows 9x/ME 118
7.4 Check the TCP/IP Setup of Windows 2000 122
7.5 Check the TCP/IP Setup of Windows XP 126

Figure Index

Figure 3-1 The Repeater User Public LAN Flow 18
Figure 3-2 Example of Setting up a Small Enterprise Network 19
Figure 3-3 Administrator Login 20
Figure 3-4 Welcome Screen 21
Figure 3-5 Configuration Wizard Screen 22
Figure 3-6 Entering Username and Password 23
Figure 3-7 Successful Login Page 24
Figure 3-8 Logon Fails (not an on-demand user) 25
Figure 3-9 Successfully logon page for on-demand user 25
Figure 3-10 Redeem page 26
Figure 3-11 Remaining hours or data size 26
Figure 4-1 Main Menu of Repeater Console Interface 27
Figure 4-2 Repeater Utility Menu 28
Figure 5-1 Setup Wizard Interface 32
Figure 5-2 Setup Wizard Description 33
Figure 5-3 Change Admin's Password Screen 33
Figure 5-4 Choose the System's Time Zone 34
Figure 5-5 Set System Information 35
Figure 5-6 Select the Connection Type for WAN Port 35
Figure 5-7 Set the Connection Type for WAN Static IP Address 36
Figure 5-8 Select the Connection Type for WAN Dynamic IP Address 37
Figure 5-9 Set WAN PPPoE 37
Figure 5-10 Configure Public LAN 38
Figure 5-11 Set DHCP Server 38
Figure 5-12 Select Public LAN Methods 39
Figure 5-13 Add Local Users 40
Figure 5-14 POP3 Setup Screen 40
Figure 5-15 Radius Setup Screen 41
Figure 5-16 LDAP Setup Screen 41
Figure 5-17 Set Wireless – Access Point Connection 42
Figure 5-18 Configure Wireless port 43

Figure 5-19 Enable DHCP Sever of Wireless Port 43
Figure 5-20 Restart 44
Figure 5-21 System Configuration 45
Figure 5-22 Example of WAN Static IP Mode.....47
Figure 5-23 WAN Dynamic IP Mode 48
Figure 5-24 WAN PPPoE Mode 48
Figure 5-25 Dial on Demand 48
Figure 5-26 Authentication Configuration.....49
Figure 5-27 Example of Public LAN Interface Configuration 49
Figure 5-28 Disable the DHCP Server on Public LAN 51
Figure 5-29 Enable the DHCP Server on Public LAN 51
Figure 5-30 Reserve the IP Address Setting on Public LAN.....52
Figure 5-31 Enable the DHCP Relay on Public LAN 53
Figure 5-32 Example of Wireless Interface Configuration.....53
Figure 5-33 Security setting.....54
Figure 5-34 Advance setting of Wireless 55
Figure 5-35 Wireless Port Configuration(2).....57
Figure 5-36 Disable the DHCP Server on Wireless.....58
Figure 5-37 Enable the DHCP Server on Wireless.....58
Figure 5-38 Reserve the IP Address Setting on Wireless 59
Figure 5-39 Enable the DHCP Relay on Wireless 59
Figure 5-40 WDS Configuration.....60
Figure 5-41 Example of Private LAN Interface 61
Figure 5-42 Disable DHCP Server on Private LAN.....62
Figure 5-43 Enable DHCP Server on Private LAN.....62
Figure 5-44 Reserve IP Address Setting on Private LAN.....63
Figure 5-45 Enable DHCP Relay on Private LAN 64
Figure 5-46 Example of Authentication Policy(1) 64
Figure 5-47 Example of Authentication Policy(2) 65
Figure 5-48 Exception Configuration.....66
Figure 5-49 Local User List.....67
Figure 5-50 Example of Adding User Accounts.....68
Figure 5-51 Added User Accounts Screen 69

Figure 5-52 Example of Editing User Accounts 69
Figure 5-53 Example of Upload User Account Interface 70
Figure 5-54 Example of Download User Account Interface 70
Figure 5-55 POP3 Setup Screen 71
Figure 5-56 RADIUS Setup Screen 72
Figure 5-57 LDAP Setup Screen 73
Figure 5-58 NT Domain Setup Screen 73
Figure 5-59 Layer 2 Authentication 74
Figure 5-60 Group Configuration Screen 75
Figure 5-61 Example of Black List 76
Figure 5-62 Example of Adding User to Black List 77
Figure 5-63 Example of Deleting a User from Black List 78
Figure 5-64 Guest User Configuration Management Interface 78
Figure 5-65 Example of Guest User Management Interface 79
Figure 5-66 Roaming Configuration 80
Figure 5-67 Additional Configuration 81
Figure 5-68 Upload User-defined Login Interface 82
Figure 5-69 HTML Instructions Required for Using User-Defined Interface 83
Figure 5-70 Path of Graphic File in User Login Interface 83
Figure 5-71 Graphic File Description 83
Figure 5-72 Path of Graphic File for User Logout Interface 83
Figure 5-73 Upload User Logout Interface 84
Figure 5-74 HTML Codes Required for User Logout Interface 85
Figure 5-75 POP3 Message 85
Figure 5-76 MAC Address Control Interface 86
Figure 5-77 Receipt Information 86
Figure 5-78 On-demand User Configuration 87
Figure 5-79 On-demand User Page Field and Description 88
Figure 5-80 On-demand User List 88
Figure 5-81 Billing Configuration 88
Figure 5-82 Upload On-demand User 90
Figure 5-83 Example of Firewall Profile 91
Figure 5-84 Select the Group for Applying Firewall Profile Rules 91

Figure 5-85 Example of Edit Filter Rule 92
Figure 5-86 Example of Editing Specific Route Profile 94
Figure 5-87 Example of Guest Login Schedule Management Interface 95
Figure 5-88 Defining the Static Assignment Address Correspondence 96
Figure 5-89 Defining Public Accessible Server 96
Figure 5-90 IP Address and Network Port Redirect 97
Figure 5-91 Privilege IP Address 99
Figure 5-92 Direct Connecting MAC Address 100
Figure 5-93 Monitor IP List 100
Figure 5-94 Monitor IP result 102
Figure 5-95 Defining Walled Garden Server Address 102
Figure 5-96 Proxy List 103
Figure 5-97 Dynamic DNS 104
Figure 5-98 Change Administrator's Account 105
Figure 5-99 Backup and Restore 106
Figure 5-100 Executing the Firmware Upgrade 107
Figure 5-101 Restart 108
Figure 5-102 System Status Example 109
Figure 5-103 System Status Description 109
Figure 5-104 Interface Status Example 112
Figure 5-105 Interface Status Example 113
Figure 5-106 Online User Data 114
Figure 5-107 History Example 114
Figure 5-108 Traffic History Example (2) 115
Figure 5-109 DHCP Server Reporting Example 115
Figure 5-110 Notify Configuration Example 116

FCC CAUTION

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

FCC RF Radiation Exposure Statement: This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

Your device contains a low power transmitter. When device is transmitted it sends out RadioFrequency (RF) signal.

In order to maintain compliance with the FCC RF exposure guidelines, this equipment shouldbe installed and operated with minimum distance 20cm between the radiator and your body.Use only with supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations

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 Repeater

CE0984①

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 EN 300 328-2 V1.**2**.1 (**2001-08**)
- EN 301 489-17 V.1.**2**.1 (**2002-04**)
- EN 50371: 2002
- EN 60950: 2000

IC CAUTION

"To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing."
"Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device."

This Class B digital apparatus complies with Canada RSS-210.
Cet appareil numérique de la classe B est conforme à la norme CNR-210 du Canada

The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment. (DoC)

The term "IC:" before the certification/registration number only signifies that the Industry Canada technical specifications were met.

1. Preface

1.1. Brief Introduction of Repeater

Wireless network breaks through the barrier of traditional thinking, and releases unlimited innovation and implementability, which becomes the working attitude and living environment pursued by people nowadays. In addition, manufacturers try very hard to lower the entry level and thus more consumers are happy to have such technology to get rid of the tangled network cables and limitations. However, the problems accompanying the wireless technology cannot be overlooked. The ways of preventing your neighbors from "borrowing" your wideband or becoming your "Network Neighbor" to enter your computer system anytime are the important topics when upgrading to wireless users. The Cipheriium Repeater is easy to set up and operate, but also has built up gates to filter user's entrance and exit, and thus takes care of both the strictness of management and the convenience of usage. Finally, you can have peace of mind to carry out the wireless construction or implement a wireless studio at home.

Also we integrate a wireless port in Repeater which supports 54Mbps wireless networking standard and is almost five times faster than the widely deployed 802.11b products in homes, enterprises, and public wireless hotspots around the country —802.11b and 802.11g share the same 2.4GHz radio band, so Repeater can also work with existing 11Mbps 802.11b equipment.

Quick Installation • Online Immediately

The installation and setup of the Repeater are easy without changing the present existing network architecture. You can install and login the system within a short time and establish the security mechanism. With the protection by the Repeater, users must be authenticated before logging on to the network, and the administrator can assign a fine-grained priority to each user stratifying the scope and right of using network resources.

Friendly Management and Application Interfaces

The Repeater is not only easy to install, but also has friendly management interface and

operation logic, which allow you to get a hand on it easily. You can use all the functions of the system with a click. A full web-based management interface allows you to operate and manage the system online by browser. At the user end, the login Public LAN is also operated through the browser, and it does not require installing any additional software interface.

Integrating the Existing User Password Database

In general, most organizations use specific database system to centralize and manage user passwords before introducing the wireless network into the organization. The Repeater supports Local, POP3 (+SSL), RADIUS and LDAP external Public LAN mechanisms, and allows you to integrate the current user password database. This system also provides a built-in user database, so that the administrator can create or upload Public LAN data by batch processing.

1.2. Before you Read

1.2.1. Audience

This manual is intended for system or network administrators, therefore we assume that our readers have acquired networking knowledge to a certain extent and are able to complete the setups step by step following the instructions of this manual in order to use the Cipherium System's Repeater for a better manage of network system and user data.

1.2.2. Document Convention

For any caution or warning that require special attention of readers, eye-catching italic font put in box is used as highlight. An example is given below:

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

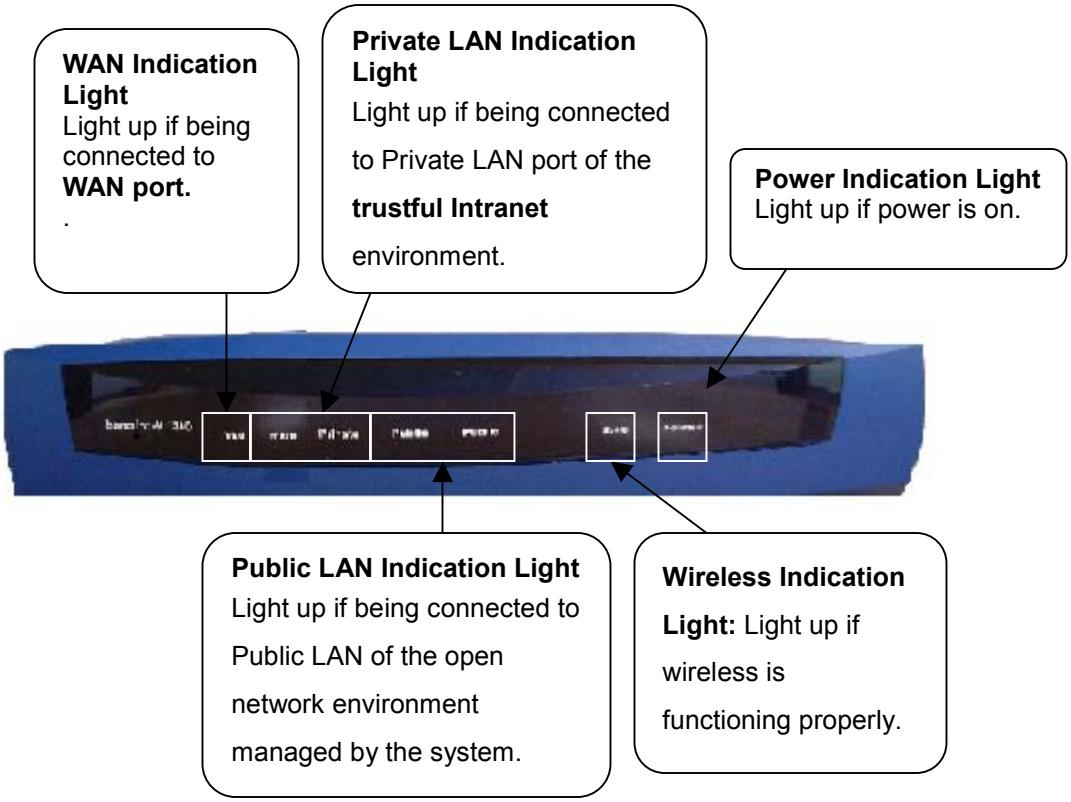
2. Product Description

2.1. Package Contents

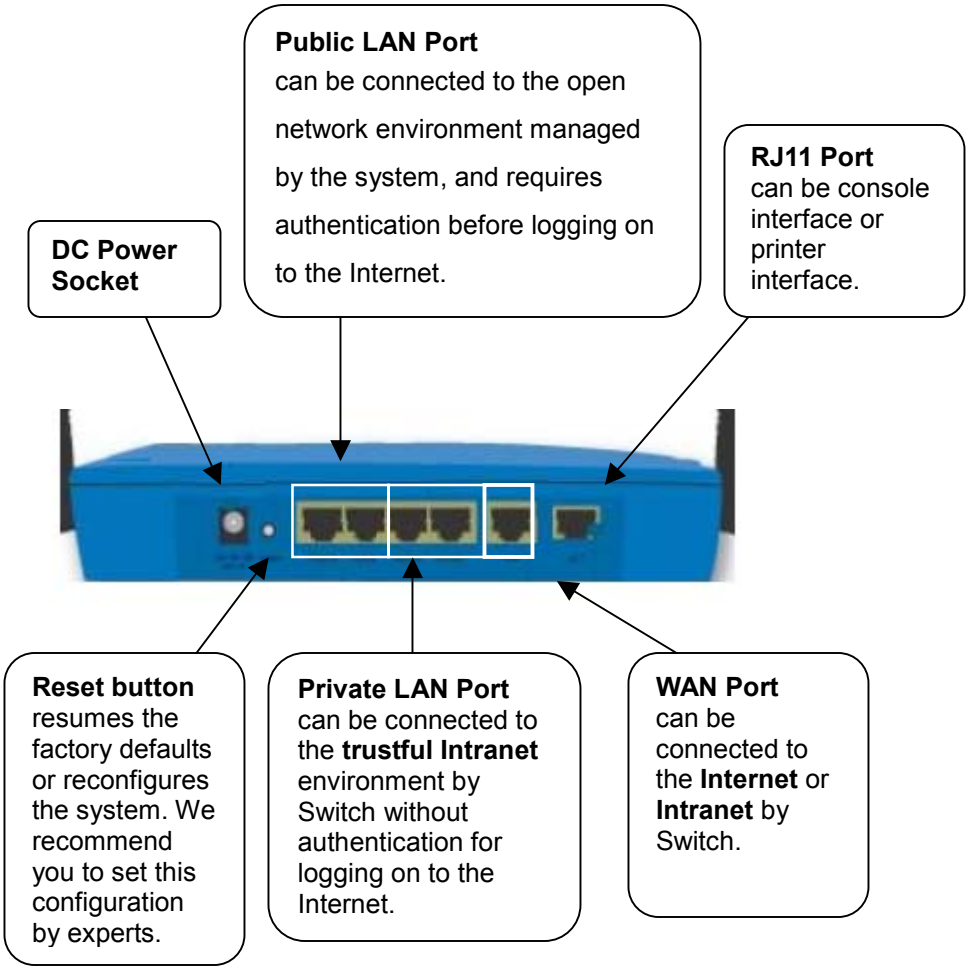
The standard package of the Repeater includes:

- Repeater x 1
- CD-ROM (Administrator's Manual and Quick Installation Guide) x 1
- Power adaptor x 1
- Ethernet cable x 1
- console cable x 1
- Wall-mount

2.2. Front Panel



(Back Side)



WAN Port

The WAN port is connected to a network which is not managed by the Repeater 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.

Public LAN Port

The Public LAN port is used to connect to the desired network for management or WLAN, and all users connected to the Public LAN must login successfully before using the network resources.

Private LAN Port

The Private LAN port is used to connect to the trustful network or Ethernet. In other words, the computer or user connected to the Repeater from Private LAN does not require login to use the network resources. This port can be used to connect to a server such as File Server or a DataBase Server, etc.

DC Power Socket

It is used to connect the power supply.

RJ11 Port

There have 2 functions but can't be used at the same time.

1. Connect to a specific printer for on-demand user to print out tickets.
2. If you need to set the Administrator's Password, you can connect a PC to this port used as a Console Serial Port, and use terminal connection program (such as the super terminal and the parameter is 9600, 8, N, 1, None flow control) to change the Administrator's Password.

2.3. Hardware Specifications

- Dimensions: 14.9cm(W) x 4.7cm(H) x 24.8cm(L)
- Weight: 470g
- Power: DC12V/1A 5.5Φ
- Operating Temperature: 5-45˚C
- 5 Fast Ethernet RJ 45 Connectors
- 1 RJ11 Ports
- Supports 10/100Mbps Full / Half Duplex Transfer Speed

2.4. Technical Specifications

2.4.1. Standards

- Supports IEEE 802.1x

- Supports IEEE 802.11g

2.4.2. 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
- Supports roaming across networks

2.4.3. Firewall

- Provides Several DoS protection mechanisms
- Customizable packet filtering rules
- Customizable walled garden (free surfing area)

2.4.4. User Management

- Supports at least 500 on-line users concurrently
- Supports Local, POP3 (+SSL), RADIUS, and LDAP Public LAN mechanisms
- Supports two or more Public LAN mechanisms simultaneously
- Can choose MAC address locking for built-in user database
- Can set the time for the user to login to the system
- Can set the user's idle time
- Can specify the connection to MAC address without Public LAN

- Can specify the connection to IP address without Public LAN
- Permits or refuses all connections when the WAN interface fails
- Supports web-based login
- Provides several friendly logout methods
- Supports RADIUS accounting protocol to generate the billing record on RADIUS server.

2.4.5. 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

2.4.6. Accounting

- Supports built-in user database and RADIUS accounting

3. Installation

3.1. Installing the Repeater

3.1.1. System Requirements

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

3.1.2. Installation Procedure

Follow the following steps to install the Repeater:

1. Make sure the power of the Repeater is turned off.

2. Connect the WAN port.

Use the network cable of the 10/100BaseT to connect to the Repeater and the network not managed by the Repeater system such as the ATU-Router of ADSL, port of Cable Modem, or the Switch or Hub on the LAN of a company.

3. Connect the port. (Optional)

Use the network cable of the 10/100BaseT to connect to the Repeater and the network not managed by the Repeater system such as the ATU-Router of ADSL, port of Cable Modem, or the Switch or Hub on the LAN of a company.

4. Connect the Public LAN.

The Public LAN is used to connect the desired network for management or WLAN, and all users connected to the Public LAN must login successfully before using the network resources. Use the network cable of the 10/100BaseT to connect to the Switch or Hub of the Public LAN, and then use the network cable of the 10/100BaseT to connect to the Administrator's PC. If it is necessary to connect the PC or wireless AP directly to the Public LAN, then we need to

use the cross over line.

Warning: *Public LAN cannot connect to Layer 3 device.*

5. Connect the Private LAN port.

The Private LAN port is used to connect the trustful network or Ethernet. In other words, the computer connected to the Repeater from Private LAN does not require login to use the network resources. This port can be used to connect to a server such as File Server or a DataBase Server, etc. Use the network cable of the 10/100BaseT to connect to the Switch or Hub of the Private LAN, and then use the network cable of the 10/100BaseT to connect to the Administrator's PC. If it is necessary to connect the PC or wireless AP directly to the Private LAN, then we need to use the cross over line.

6. Turn on the power.

Plug the bundled power supply connector into the socket.

7. Check the LED indication light.

After the power is on, the power indication light should be lit. The WAN and indication lights should be lit when the WAN and ports are properly connected to the network equipment. The corresponding indication lights also should be lit when the Public LAN and Private LAN ports are properly connected.

3.1.3. Setting up the PC for the Public LAN and Private LAN

After the Repeater is installed, the following must be set up for the Public LAN and Private LAN sections:

- TCP/IP Network Setup
- Internet Connection Setup

3.1.3.1. TCP/IP Network Setup

- If the operating system of your PC is Windows 95/98/ME/2000/XP, then you just need to keep the default setting (without any change) to directly start/restart the system.

- During the process of starting the system, the Repeater with DHCP function will automatically assign an appropriate IP address (and related information) to each PC.

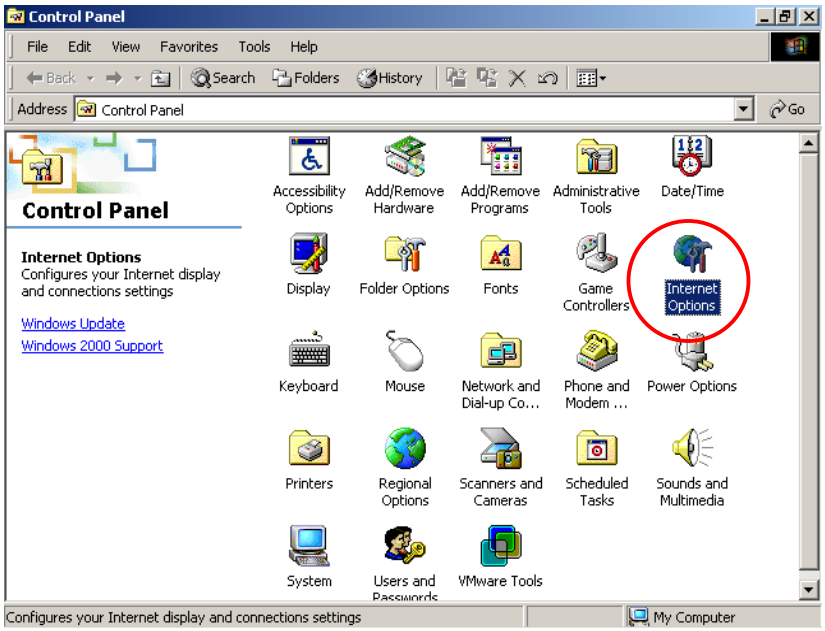
- For the Windows operating systems other than those for servers, the default setting of the TCP/IP will treat the PC as the DHCP client, and such function is called "obtain an IP address automatically".

- If you want to use the static IP in the Public LAN or Private LAN section or check the TCP/IP setup, please refer to Appendix - Windows TCP/IP Setup.

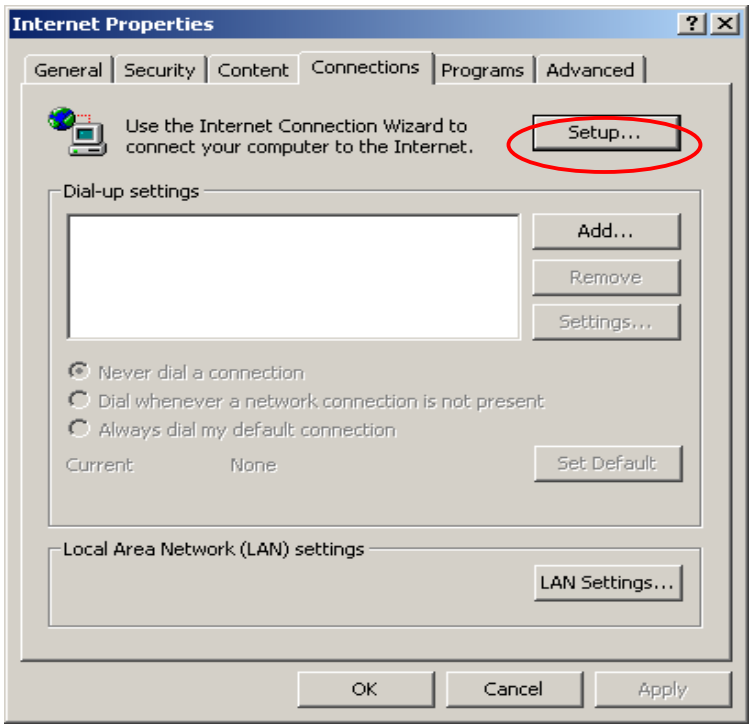
3.1.3.2. Internet Connection Setup

Windows 9x/2000

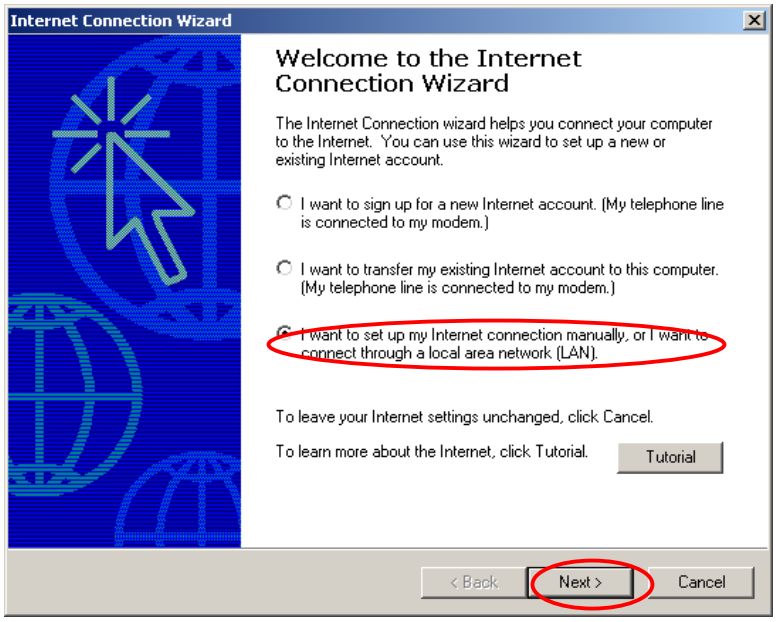
1. Choose **Start - Console – Internet Options**.



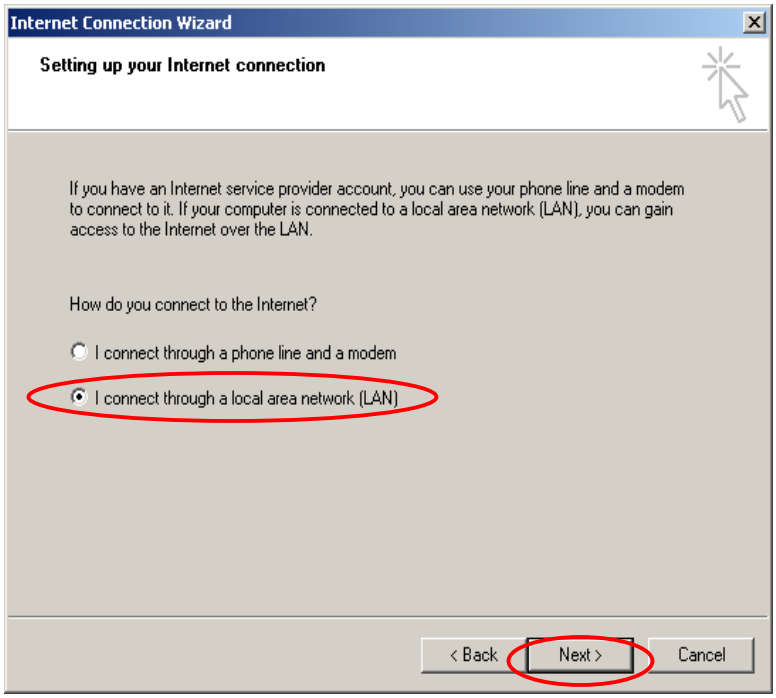
2. Choose the **"Connections"** Icon, and then click **"Setup"**.



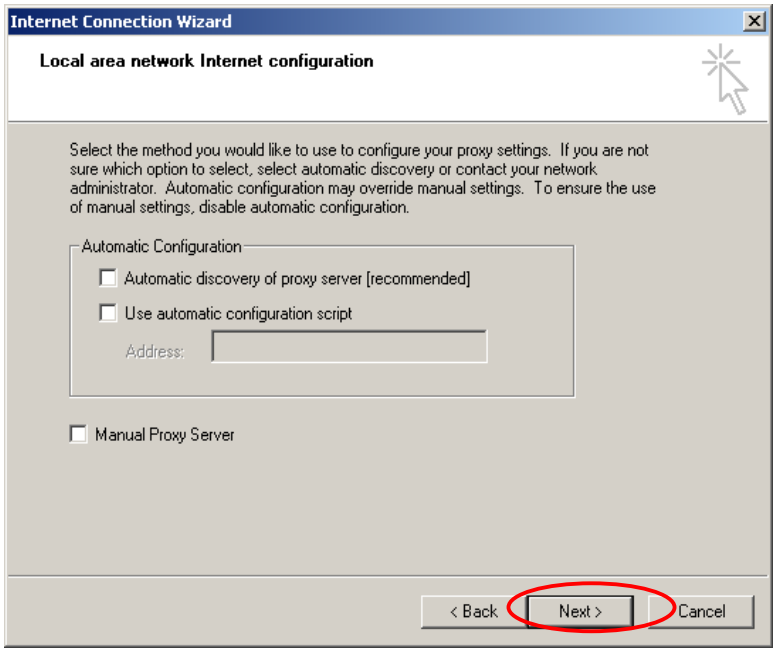
3. Choose **"I want to set up my Internet connection manually, or I want to connect through a local Area network (LAN)",** and then click **"Next"**.



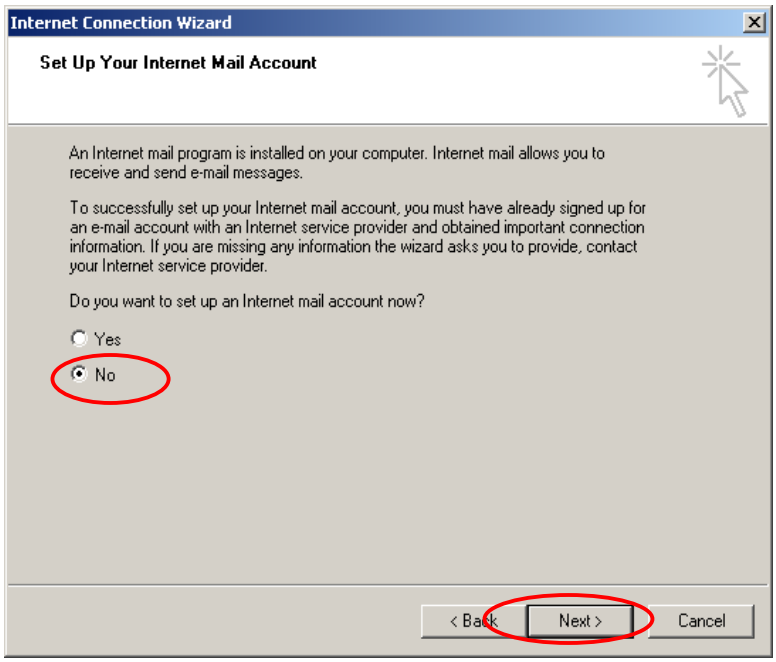
4. Choose **"I connect through a local area network (LAN)"** and click **"Next"**.



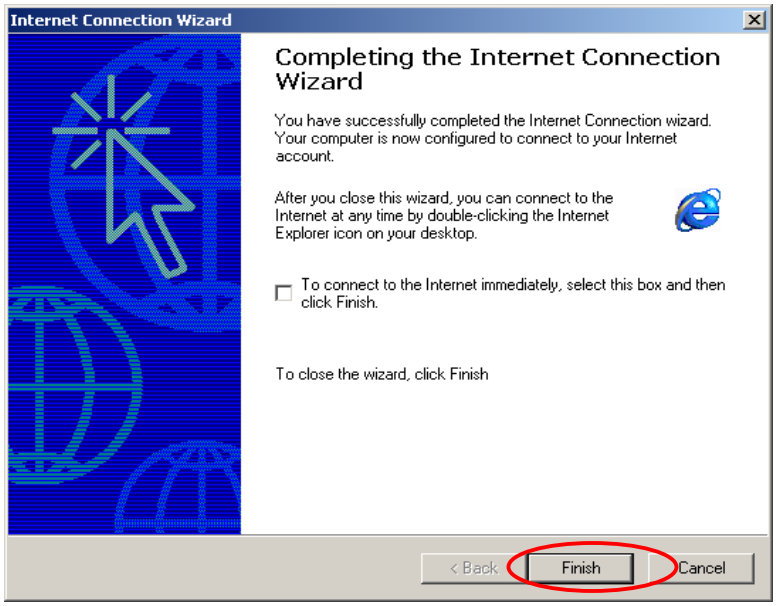
5. **Do not choose** any option in the following LAN window for Internet configuration.



6. When the system asks **"Do you want to set up an Internet mail account now?"**, choose **"No"**.

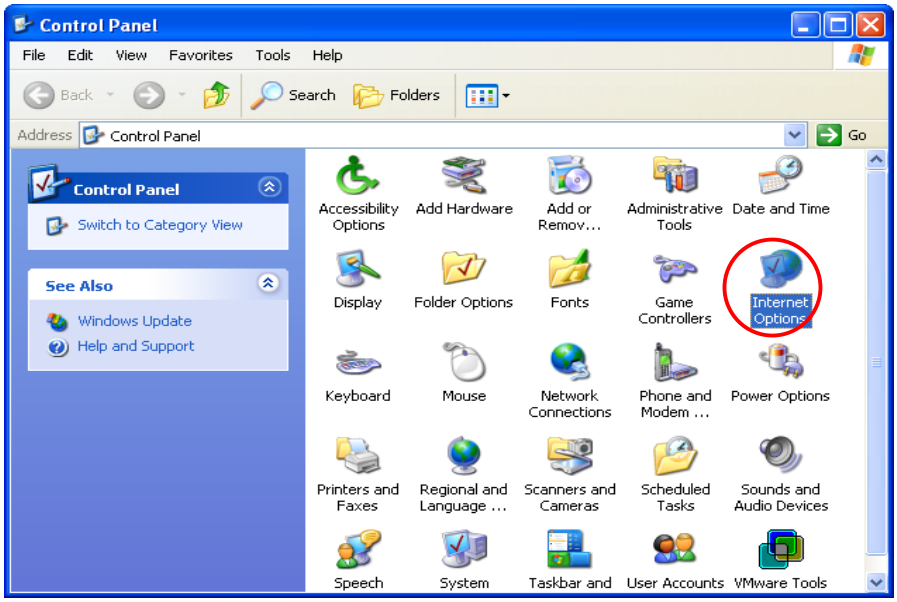


7. Click **"Finish"** to exit the Internet Connection Wizard. Now, you have completed the setup.

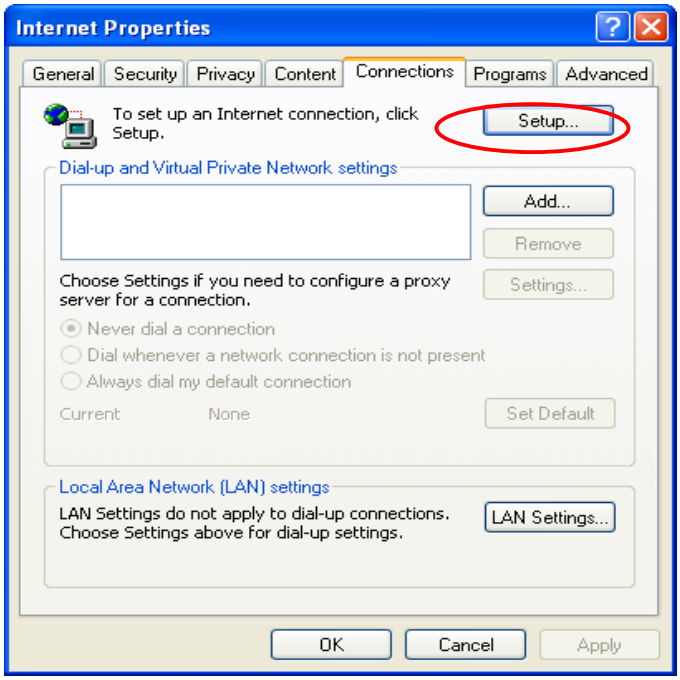


Windows XP

1. Choose **Start - Console – Internet Option**.

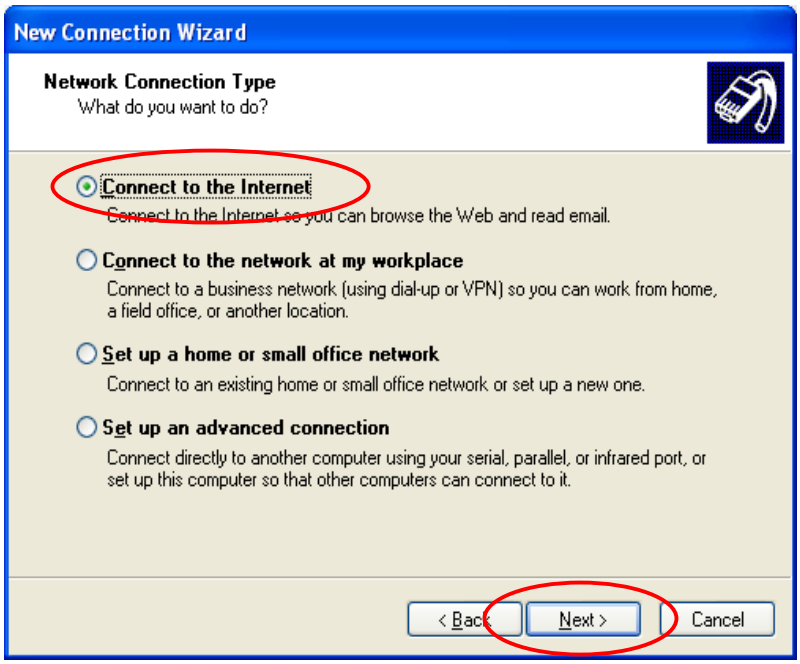


2. Choose the **"Connections"** icon, and then click **"Setup"**.

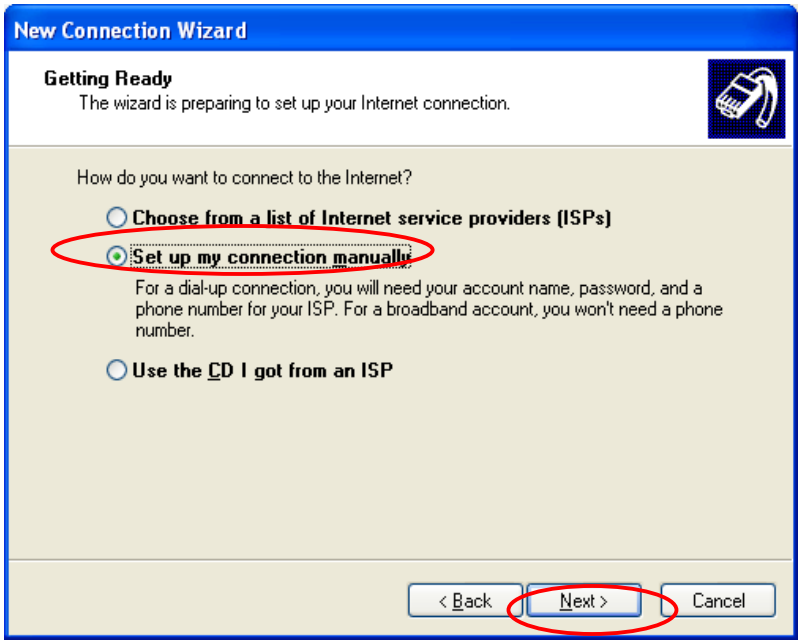


3. Press **"Next"** when the new connection wizard appears on the screen.

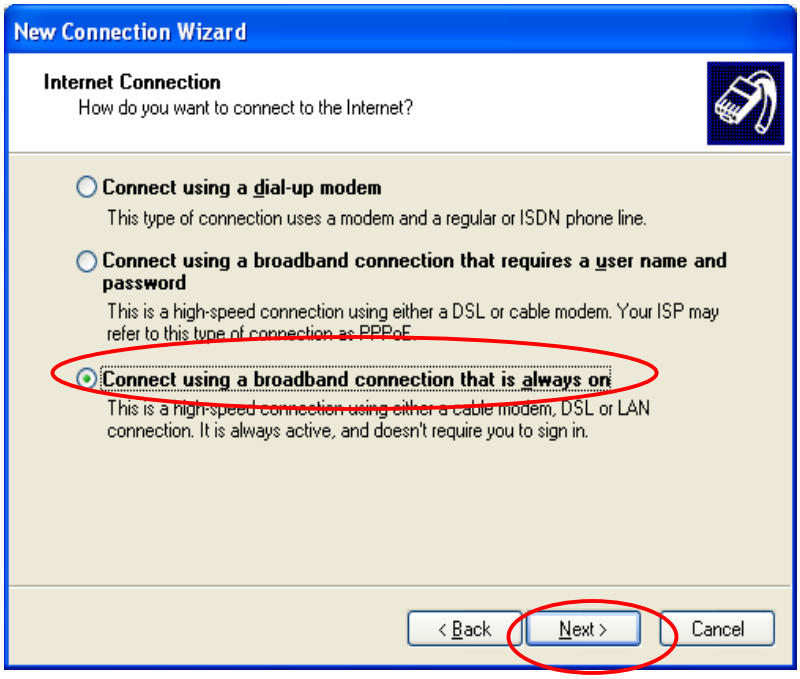
4. Choose **"Connect to the Internet"** and then click **"Next"**.



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



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



7. Click "**Finish**" to exit the Connection Wizard. Now, you have completed the setup.

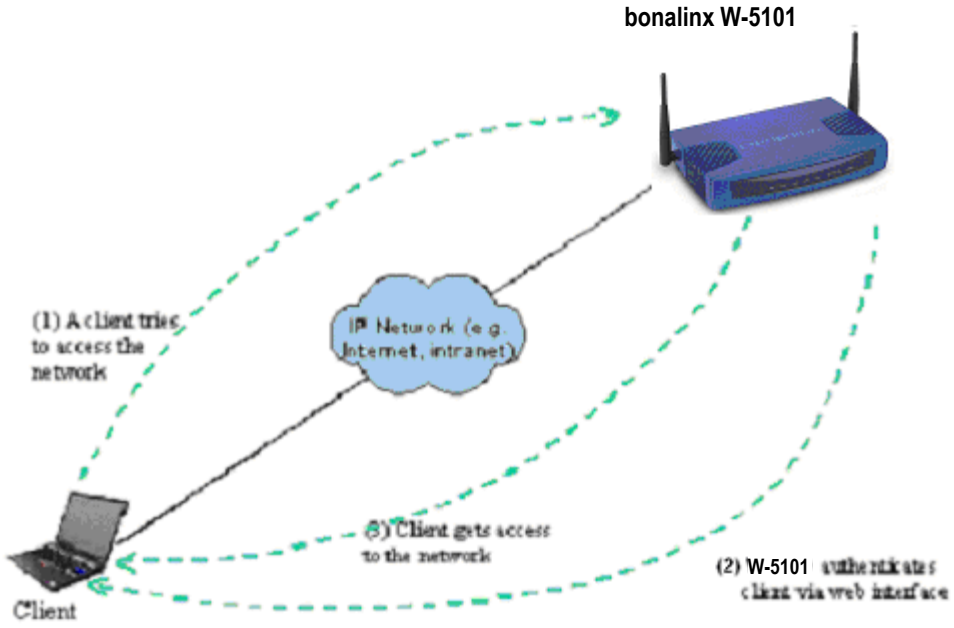
3.2. Getting Started

3.2.1. System Concept

The Repeater is responsible for controlling all network data passing through the system. The users under the managed network must be authenticated in order to obtain the right to access the network beyond the managed network. The Public LAN mechanism at the user's end is provided via the Repeater server, and the SSL encryption is used to protect the webpage. When a user at Public LAN is requesting, the Repeater server software will check the Public LAN database at the rear end to confirm the user's access right. The Public LAN database can be the local database of the Repeater or any external database that the Repeater supports. If the user is not an authorized user, the Repeater will refuse the user's request for the access. In the meantime, the Repeater will also continue blocking the user from accessing the network. If the user is an authorized user, then the Repeater will authorize the user with an appropriate

access right, so that the user can use the network. The concept of the operation of the whole Public LAN procedure is shown in the following figure.

Figure 3-1 The Repeater User Public LAN Flow



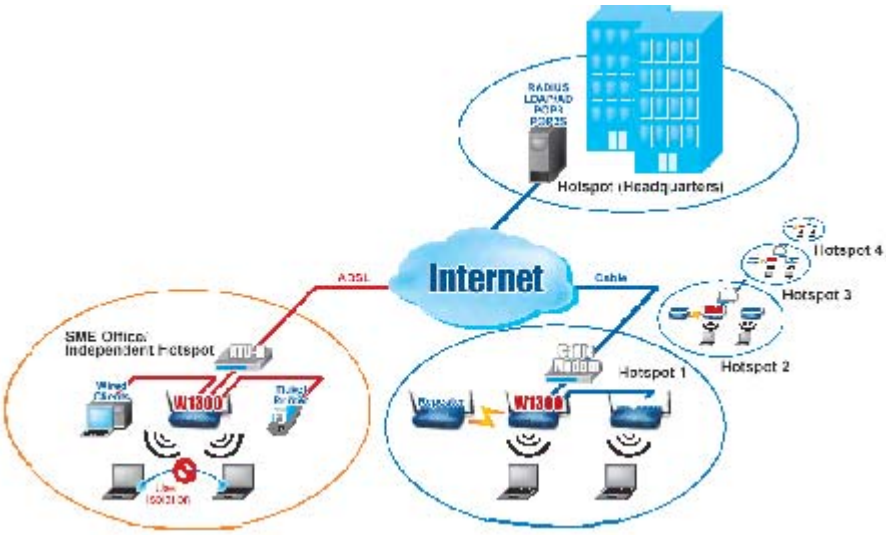
If the online user remains idle without using the network for a time exceeding a predetermined time on the Repeater or the online user logs out of the system, the Repeater will exit the working stage of such user, and terminate the user's access right for the network.

In the system, the Repeater is responsible for authorization and management functions. The user account information is stored in the Repeater database, or other specified external Public LAN databases. The process of authenticating the user's identity is executed via the SSL encrypted webpage. Using the web interface can ensure that the system is compatible to most desktop devices and palm computers.

3.2.2. Connecting Network Devices

Figure 3-2 provides a simple example of setting up a small enterprise network.

Figure 3-2 Example of Setting up a Small Enterprise Network



In **Figure 3-2**, the Repeater is set to control a part of the company's intranet. The whole managed network includes cable network users and wireless network users.

In the beginning, any user located at the managed network is unable to access the network resource without permission. If you want to have the access right to access the network beyond the managed network, you must open an Internet browser such as the Internet Explorer to connect to any website. When the browser attempts to connect to a website, the Repeater will force the browser to redirect to the user login webpage. The user must enter a username and password for Public LAN. After the identity is authenticated successfully, the user will gain proper access right defined on the Repeater. Please refer to **Figure 3-1** for the user Public LAN flow.

3.2.3. Begin Installation

After the Repeater is connected to network devices, you can start setting the Repeater to control your network environment. In the following sections, we will guide you step by step to set up a system composed of individual Repeater.

3.2.3.1. Entering the Web Management Interface

1. Opening Browser

After the Repeater is installed and the foregoing setup is completed, use the network cable of the 10/100BaseT to connect to the Private LAN port, please open the browser (such as Microsoft IE). On the website, enter the administrator's URL such as https://192.168.2.254. IF you can't get the login screen, this may because you have set your network to obtain an IP address automatically from Private LAN port and this IP address does not belong in the same subnet as this URL, please specify an IP address such as **192.168.2.xx** in your network then do it again.

2. Keying in the Administrator's Username and Password

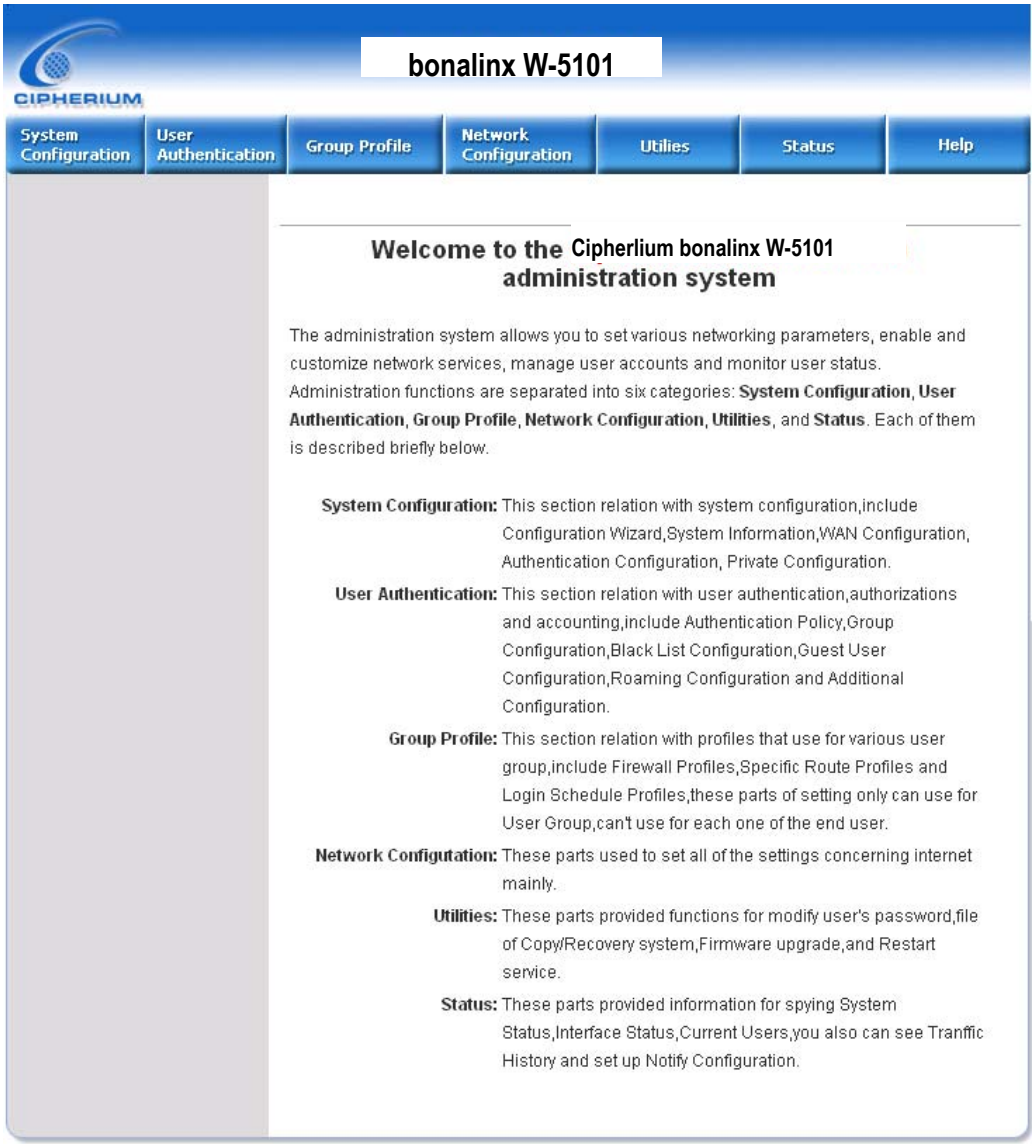
In the opened webpage, you will see the login screen as shown in **Figure 3-3.** Please key in "**admin**" in the Username column, and then "**admin**" in the Password column. Click "**Enter**" to login.

Figure 3-3 Administrator Login

3. System Setup

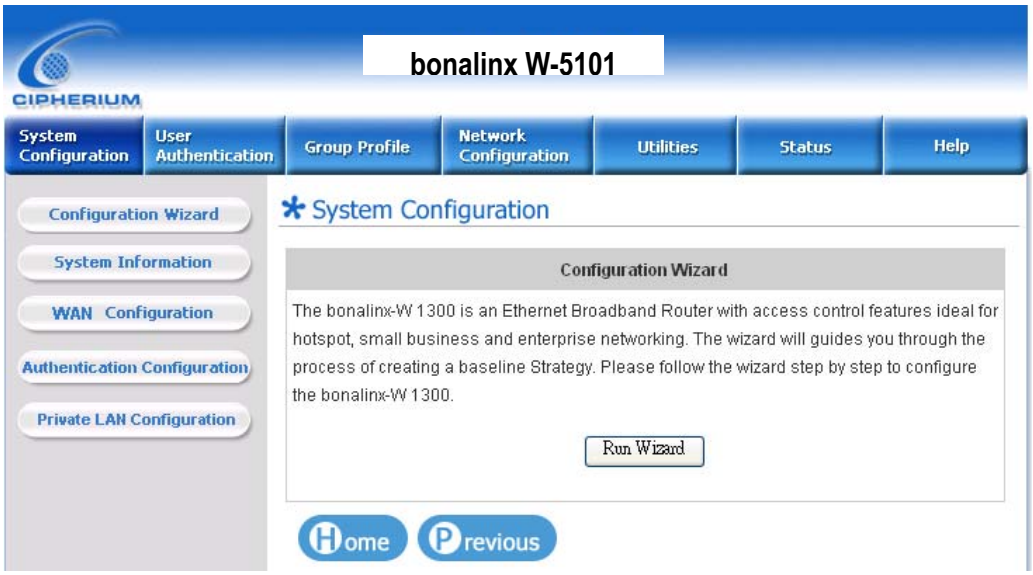
After successfully logging on to the Repeater and entering into the web management interface, you can run the installation wizard to help you complete the setup.

Figure 3-4 Welcome Screen



Click **System Configuration > Configuration Wizard** and the configuration wizard will appear on the screen as shown in **Figure 3-5.**

Figure 3-5 Configuration Wizard Screen



Click **"Run Wizard"** and the configuration wizard will guide you through the seven steps to complete the setup.

Please refer to Chapter 5.1.1 "**Configuration Wizard**" for the detailed description.

.

3.2.3.2. Accessing External Network from Network Section Managed by System

If all the steps are set properly so far, we can further connect the Repeater to the managed network to experience the controlled network access environment. First, connect a user-end device to the network at the Repeater Public LAN, and set the dynamic access network. After the network address is obtained at the user end, open an Internet browser, and link to any website. Then, the default login webpage will appear in the Internet browser.

Figure 3-6 Entering Username and Password

Key in the created username and password in this interface. And then click on the **"Enter"** button (for both standard user and on-demand user).

Figure 3-7 Successful Login Page

After this user login successfully, you have just completed the setup of the Repeater and allowed it to provide you with a managed network environment. This user can also browse the webpage on the Internet.

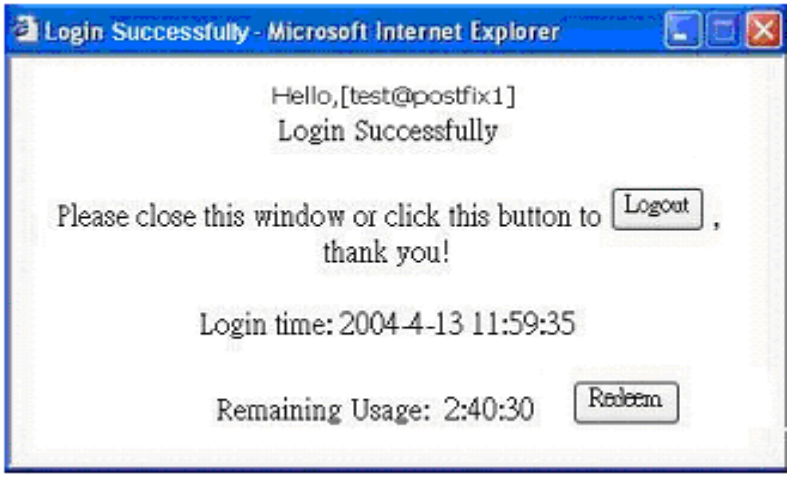
Nevertheless, if you are not a on-demand user, please do not click on "**Remaining**", because

the following error window will appear.

Figure 3-8 Logon Fails (not an on-demand user)

The following is the successful login page for on-demand user. There is an extra function, the "Redeem" button, that user can add credit in the current account if the remaining usage is considered to be insufficient.

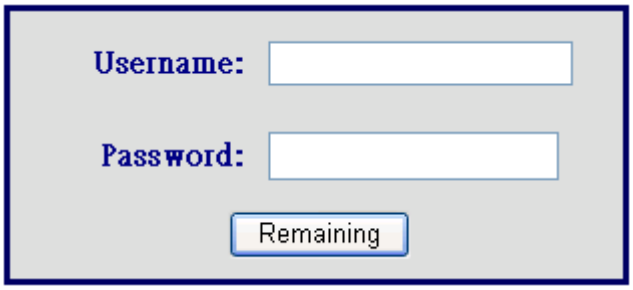
Figure 3-9 Successfully logon page for on-demand user



Attention: The maximum session time/data transfer is 24305 days/2003Mbyte. If the redeem amount exceeds this number, the system will automatically reject the redeem process.

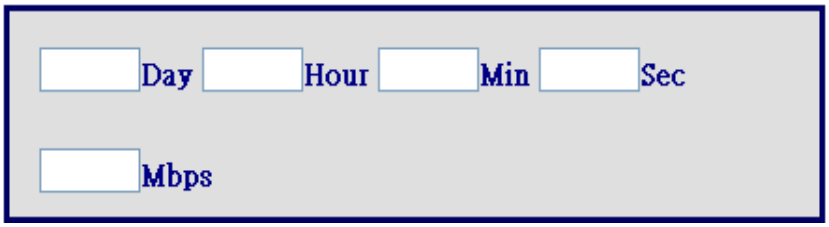
After user has paid the redeem cost at counter, he/she will get another username and password, by key in this information in the appropriate window, the system will merge the two accounts and put together the available usage.

Figure 3-10 Redeem page



This window will show the remaining hours or data size for user's online access.

Figure 3-11 Remaining hours or data size



4. Console Interface

The interface of Repeater provides two types of function,

A. The Repeater provides a RJ11 interface for the administrator to handle different problems and situations occurred during operation. To link to the **RJ11** interface of the Repeater, you need a modem cable. The terminal simulation program that you use, such as the super terminal, should be set to the parameter value of **9600,8,n,1**.

The main console is a basic interface using interactive dialog boxes. Please use the arrow keys on the keyboard to browse the menu and press the "**Enter**" key to select specific menus and confirm entered value.

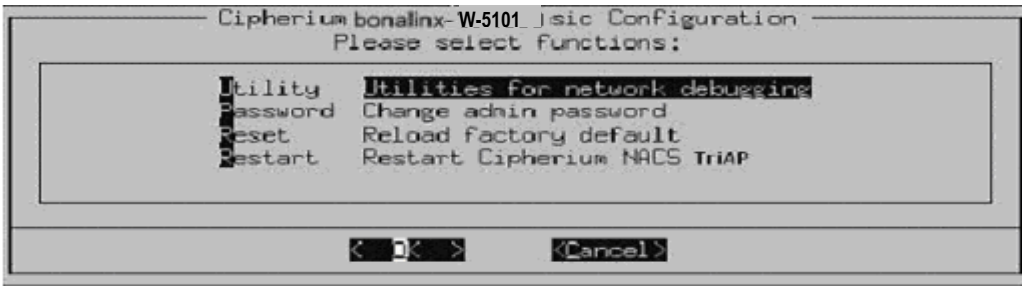
B. It also can be as a printer interface that connects to specific thermal line ticket printer.

Warning: *These two functions can't be used at the same time.*

4.1. Main Menu of Console interface

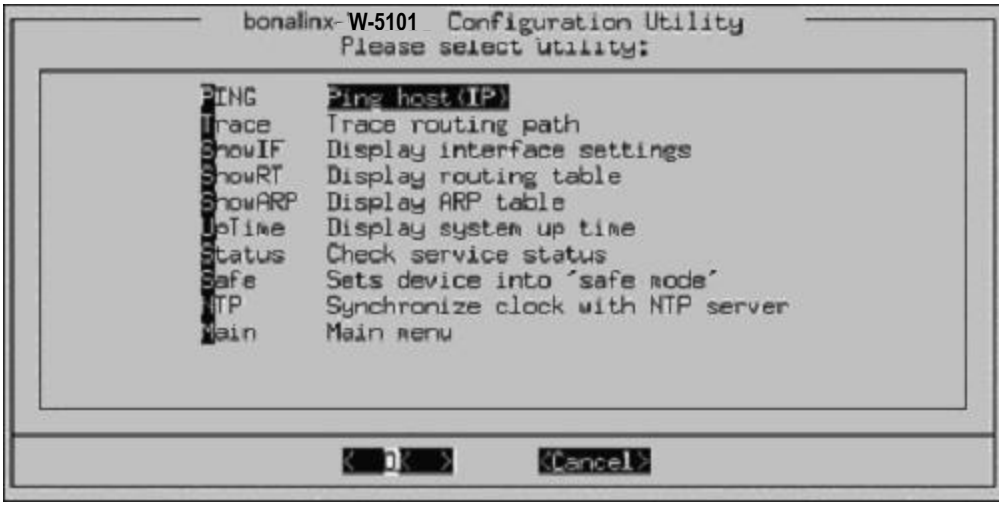
Once you properly connect to the serial port of the Repeater, the console welcome screen will appear automatically. If the welcome screen does not appear in the terminal simulation program automatically, please try to press the "**Down**" arrow key, so that the terminal simulation program will send some commands to the serial port of the Repeater, and the welcome screen or the main menu will appear again. If you are still unable to see the welcome screen or the main menu of the console, please check if the connection of your cables and the setup of the terminal simulation program are correct.

Figure 4-1 Main Menu of Repeater Console Interface



4.2. Utilities for network debugging of Console interface

Figure 4-2 Repeater Utility Menu



The Repeater console interface provides several utilities to assist the Administrator to control the system conditions and debugging. The utilities are described as following:

1. Ping host (IP): By sending ICMP echo request, the online condition with specific target can be tested.

2. Trace routing path: Trace and inquire the routing path to a specific target.

3. Display interface settings: It displays the information of each network interface setting including the MAC address, IP address, and netmask.

4. Display the routing table: The internal routing table of the Repeater is displayed to assist the confirmation of successful setup of another Static Route on Repeater.

5. Display ARP table: The internal ARP table of the Repeater is displayed.

6. Display system live time: The system live time (time for system being turn on) of the Repeater is displayed.

7. Check service status: The current execution status of each service on the Repeater is checked.

8. Set device into "**safe mode**": If administrator is unable to use Web Management Interface on the browser while Repeater unexplicitly fails. Administrator can choose this utility and set Repeater into safe mode, then administrator can management this device with browser again.

9. Synchronize clock with NTP server: Immediately check and correct the clock through the NTP protocol and network time server. Since the Repeater does not support manual setup for its internal clock, therefore we must reset the internal clock through the NTP.

4.3. Change admin password of Console interface

Besides supporting the use of console management interface through the connection of null modem, the Repeater also supports the SSH online connection for the setup. When using a null modem to connect to the Repeater console, we do not need to enter administrator's password to enter the console management interface.

When SSH is used to connect the Repeater, the username is "**admin"** and the default password is also "**admin".** This set is the same as those for the Web management interface. You can use this option to change the Repeater administrator's password. Even if you forgot the password and are unable to login the console management interface of the Repeater from the Web or the remote end of the SSH, you can still use the null modem to connect to the console management interface of the Repeater and set the administrator's password again.

Caution: *Although it does not require a password for the connection via the serial port, the same management interface can be accessed via SSH. Therefore we recommend you to*

immediately change the Repeater Admin username and password after you login the system for the first time.

4.4. Reload factory default of Console interface

It will reset the system configuration to factory defaults.

4.5. Restart Cipherium Repeater

It will restart the Repeater.

5. Web Management Interface

This section gives a complete description on the setup of Repeater. **Table 5-1** shows all options and functions of the Repeater and may facilitate your operation on Repeater.

Table 5-1 Functions List

Option	**System Configuration**	**User Authentication**	**Group Profile**	**Network Configuration**	**Utilities**	**Status**
Function	Configuration Wizard	Authentication Policy	Firewall Profiles	Network Address Translate	Change Password	System Status
	System Information	Group Configuration	Specific Route Profiles	Privilege List	Backup / Restore Strategy	Interface Status
	WAN Configuration	Black List Configuration	Login Schedule Profiles	Walled Garden List	Firmware Upgrade	Current Users
	Authentiction Configuration(include auth. Port & wireless port)	Guest User Configuration		Proxy Server Properties	Restart	Traffic History
	Private Configuration	Roaming Configuration				DHCP reporting
		Addition Configuration				Notify Configuration
		On-demand User configuration				

5.1. System Configuration

This option provides the following detailed functions to further set up your system, these

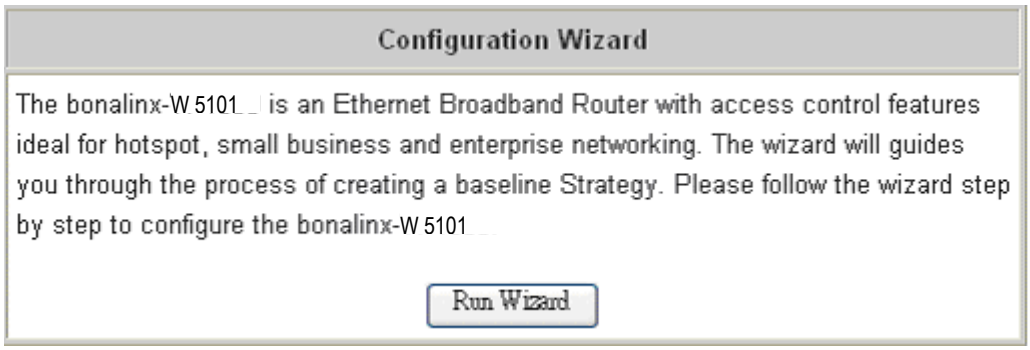
functions include: **Configuration Wizard, System Information, WAN Configuration, Authentication Configuration, and Private LAN Configuration.** Please refer to the explicit setup if you need more information.

5.1.1. Configuration Wizard

The Wizard will guide you through the setup of Repeater1200. All you need is to follow the procedures and instructions given by the Wizard, step by step, fill in the required set values. And, then restart Repeater to activate the setting.

Please click the "**Run Wizard**" button on the Setup Wizard interface as shown in **Figure 5-1** to start the system setup.

Figure 5-1 Setup Wizard Interface



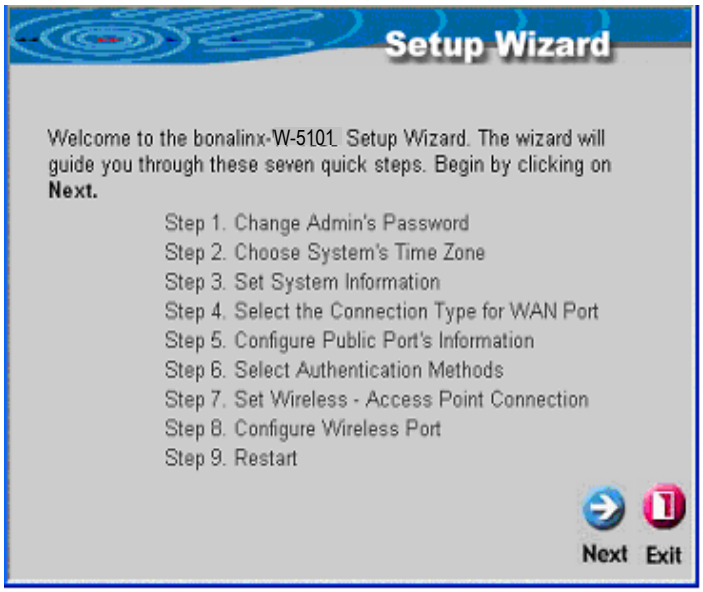
The Setup Wizard Interface as shown in **Figure 5-2** describes the installation procedure, and there are 9 procedures as listed below:

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

9. Restart

After a brief check-over of the whole process, click "**Next**" to continue, or "**Exit**" to exit the Setup Wizard.

Figure 5-2 Setup Wizard Description



1. Change Admin's Password

Please change the admin's password as shown in **Figure 5-3.**

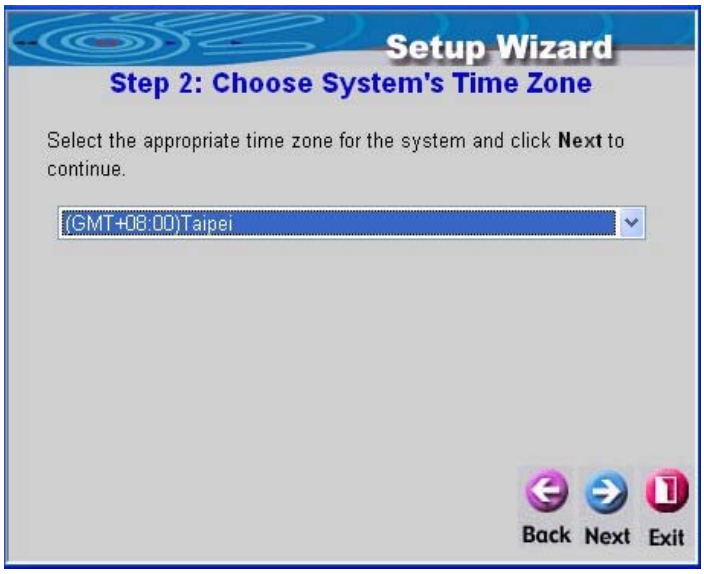
Click **"Next"** to continue or "**Exit**" to exit.

Figure 5-3 Change Admin's Password Screen

2. Choose the System's Time Zone

Choose your system's time zone as shown in **Figure 5-4**. Click **"Next"** to continue or "**Exit**" to exit.

Figure 5-4 Choose the System's Time Zone



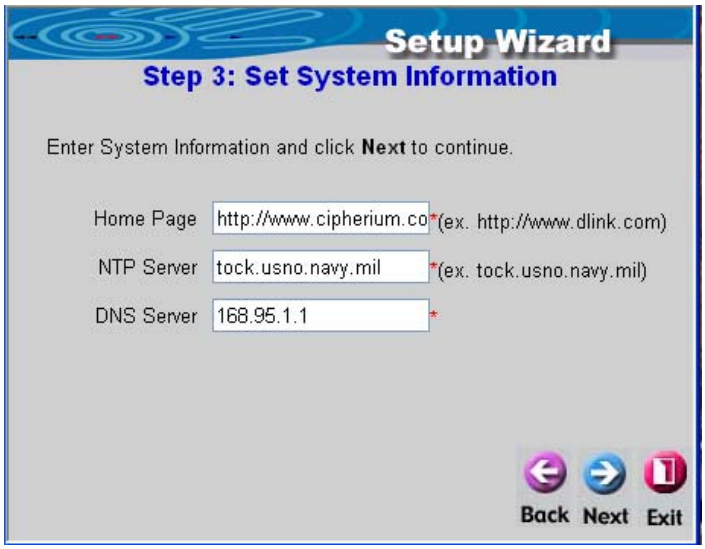
3. Set System Information

After logging on successfully, you will see fields for Home Page, NTP Server, and DNS server .

- **Succeed Page:** It will direct you to the website after a user logs on. You can enter the website of your company or any major entry website.
- **Time Server:** Please enter the website of the timer server.
- **DNS Server:** Please enter the DNS server that provides service on the network.

Click **"Next"** to continue or "**Exit**" to exit.

Figure 5-5 Set System Information



4. Select Connection Type for WAN Port

To select the connection type for WAN PORT, you can choose any of the following three types as shown in **Figure 5-6**:

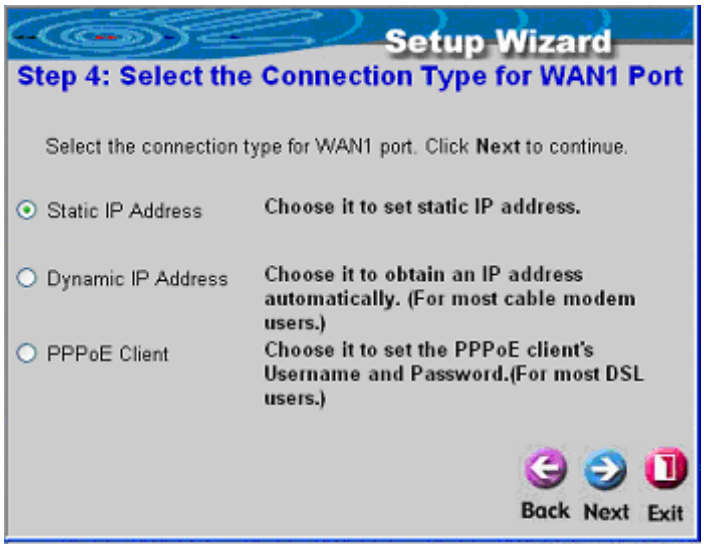
• For static IP address, please select **Static IP Address**. (**Figure5-7**)

• For dynamic IP address, please select the **Dynamic IP Address** (**Figure 5-8**).

• For xDSL and using PPPoE to connect to Internet, please select **PPPoE Client** (**Figure 5-9, Figure 5-10**).

Click "**Next**" to go to the next stage.

Figure 5-6 Select the Connection Type for WAN Port



• For **static IP address**

After you select **Static IP Address**, please enter the IP, Netmask, and Gateway of WAN PORT as shown in **Figure 5-7.**

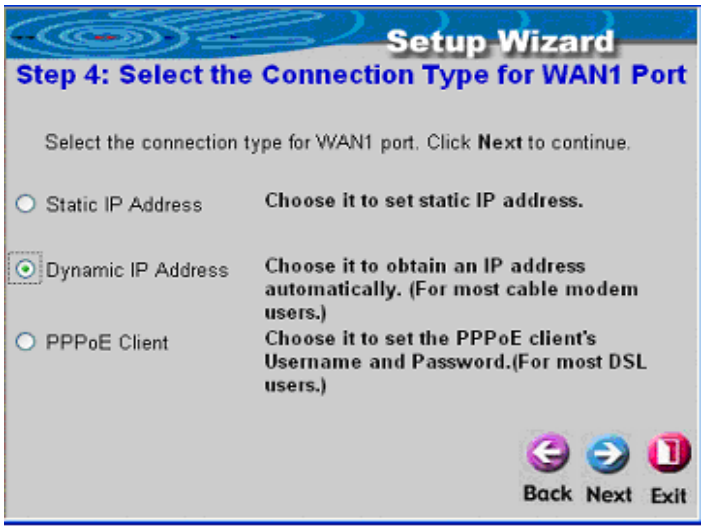
Click **"Next"** to continue or "**Exit**" to exit.

Figure 5-7 Set the Connection Type for WAN Static IP Address

• For **dynamic IP address**

After you select **Dynamic IP Address** as shown in **Figure 5-8**, click **"Next"** to continue or "**Exit**" to exit.

Figure 5-8 Select the Connection Type for WAN Dynamic IP Address



• For **PPPoE**

After you select **PPPoE**, enter the username and password of the PPPoE as shown in **Figure 5-9**. Click **"Next"** to continue or "**Exit**" to exit.

Figure 5-9 Set WAN PPPoE

5. Configure Public LAN

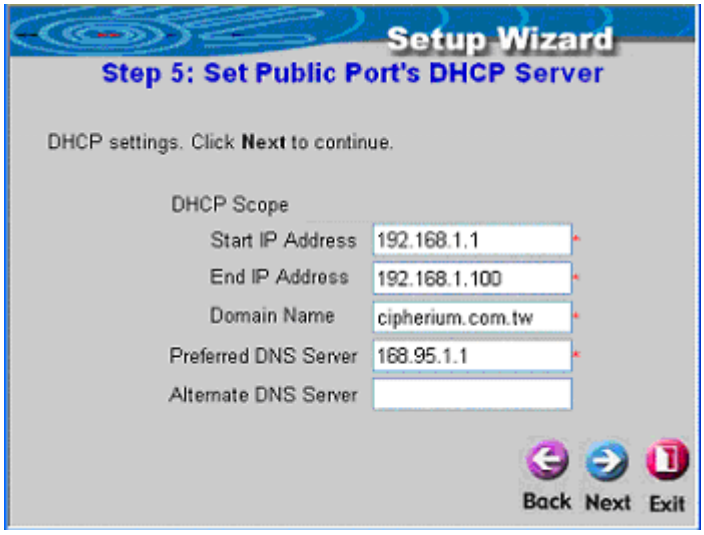
This procedure sets the related information of the Public LAN as shown in **Figure 5-10**. Please enter IP and Subnet Mask, and determine to Enable or Disable the DHCP.

Figure 5-10 Configure Public LAN

Click **"Next"** to continue or **"Exit"** to exit.

• If you choose to enable the DHCP, please refer to **Figure 5-11.**

Figure 5-11 Set DHCP Server



Related information for enabling the DHCP Server includes DHCP Start IP Address, DHCP End IP Address, Domain Name, Primary DNS IP Address, and Secondary DNS IP address. Fillling in the correspondent values, click **"Next"** to continue or **"Exit"** to exit.

6. Select Public LAN Methods

The Public LAN method sets the user's information and authenticates the user's account. You can set the Postfix Name to an easily identified name such as "**Local User**". The system provides 4 Public LAN mechanisms as described below:

•Local User, please refer to **Figure 5-13**.

•POP3 User, please refer to **Figure 5-14.**

•RADIUS User, please refer to **Figure 5-15.**

•LDAP User, please refer to **Figure 5-16.**

Figure 5-12 Select Public LAN Methods

• If you select **Local User**, please enter the Postfix Name. After this setup is completed, click **"Next"** to continue or **"Exit"** to exit.

If you want to continue to add Local users, enter the Username, Password, and MAC (not compulsory), and then click "**ADD**" to complete the procedure as shown in **Figure 5-13.**

Ex: Uername:test, Password:test

Figure 5-13 Add Local Users

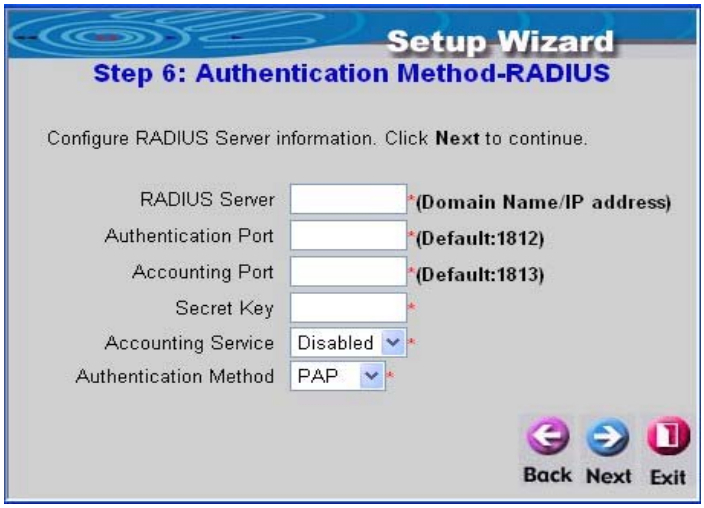
• If you select **POP3 User,** please enter the Server IP and Server Port of POP3 and determine whether or not to enable SSL function as shown in **Figure 5-14.**

Figure 5-14 POP3 Setup Screen

• If you select **RADIUS User**, please enter the related settings for the RADIUS Server, including Server IP, Public LAN, Accounting Port, Secret Key, Accounting Service, and

Public LAN Method as shown in **Figure 5-15.** After this setup is completed, click "**Next**" to continue or "**Exit**" to exit.

Figure 5-15 Radius Setup Screen



• If you select **LDAP User**, please enter the information for Server IP, Server Port, and Base DN as shown in **Figure 5-16**. After this setup is completed, click **"Next"** to continue or **"Exit"** to exit.

Figure 5-16 LDAP Setup Screen

7. Set Wireless – Access Point Connection

Please enter **SSID** name and select a **channel** and the **AP mode**, then click **next.**

Figure 5-17 Set Wireless – Access Point Connection

Caution: This device can support Channel 1-13. When using in other plcace as Taiwan, USA, Channel 12, 13 will be disabled by software and only Channel 1-11 are applicable.

8. Configure Wireless port's information

This procedure sets the related information of the Wireless port as shown in **Figure 5-18**. Please enter IP and Subnet Mask, and determine to Enable or Disable the DHCP.

Figure 5-18 Configure Wireless port

• If you select to enable the DHCP, please refer to **Figure 5-19**.

Figure 5-19 Enable DHCP Sever of Wireless Port

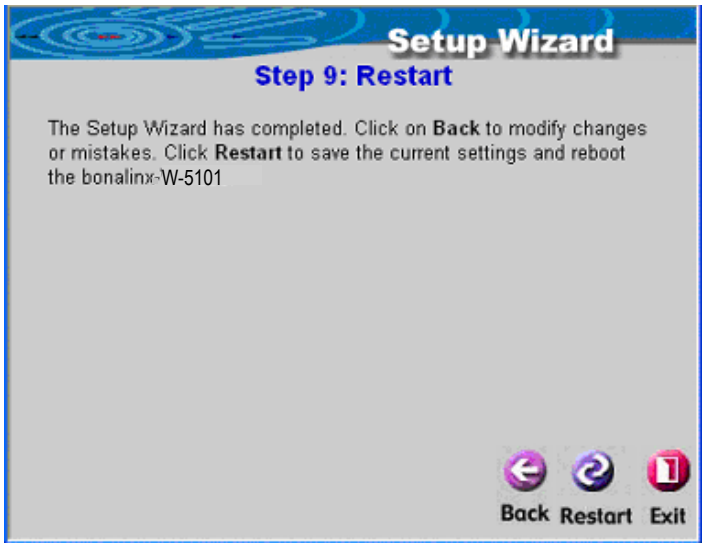
Related information for enabling the DHCP Server includes DHCP Start IP Address, DHCP End IP Address, Domain Name, Primary DNS IP Address, and Secondary DNS IP address.

After this setup is completed, click **"Next"** to continue or **"Exit"** to exit.

9. Restart

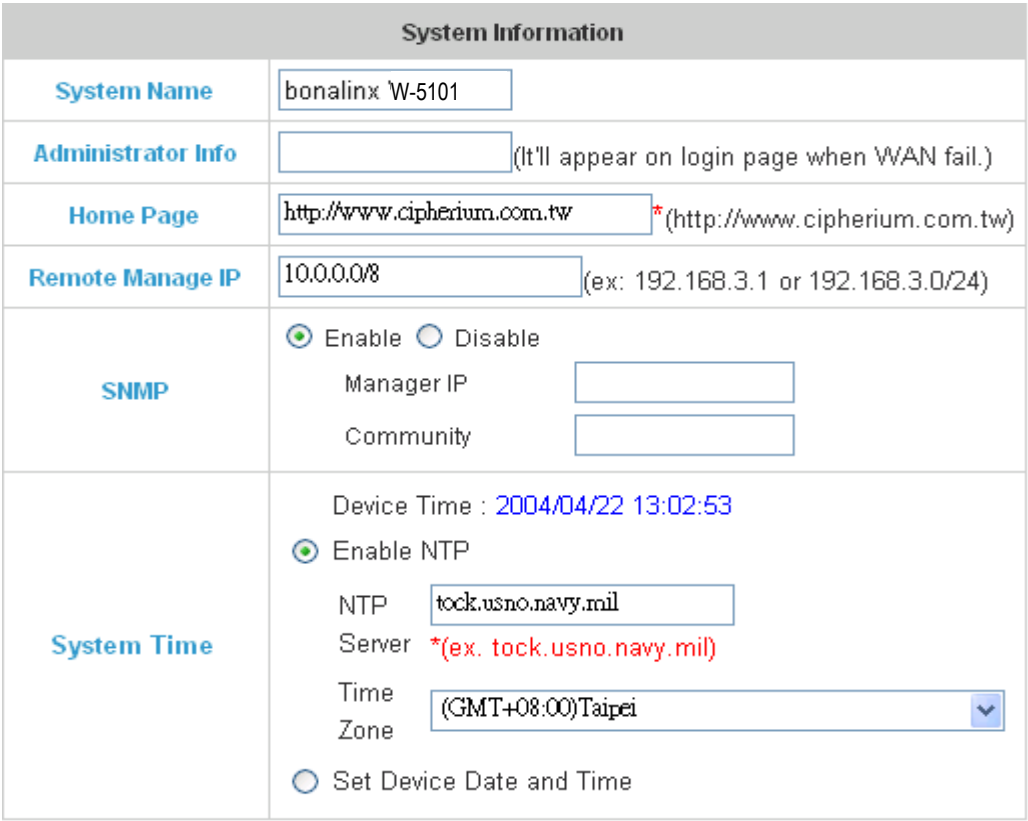
If you are sure that your setup is correct, please click the **"Restart"** button to restart and complete the setup procedures. If you do not want to keep the previous setups, please click "**Exit**". It will invalidate the previous setups.

Figure 5-20 Restart



5.1.2. System Information

Figure 5-21 System Configuration



> ***Caution***: *Click on "apply" button will automatically use the current setting without restart the bonalinx W-5101. The on-line users will nonethelessly be disconnected because of the information update.*

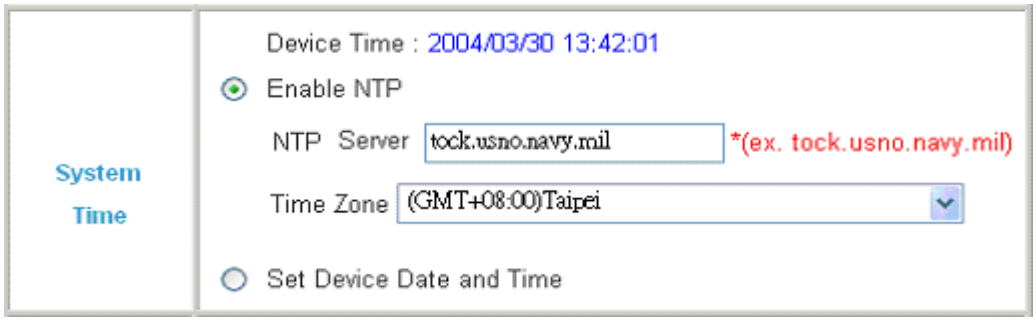
System Name: The name is Repeater system, and the default is "Repeater".

Administrator Info: It lets the Administrator enter the related information such as administrator's name, telephone number, and e-mail. If a user connects to the Repeater and the WAN Port has a connection problem, the user login screen will show the data entered in these columns on screen.

Home Page: You can enter the website of the Web Server. When a user logs on, the user will be linked to this home page automatically. The home page is usually set to the website of the company such as http://www.cipherium.com.tw. No matter which webpage the user wants to link, the user will be redirected to the set website here.

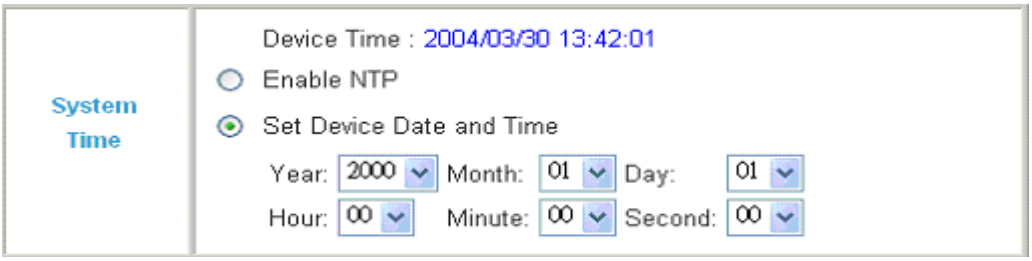
Remote Manage IP: You can set up the system to connect the WAN Port to a website that controls the functions of Repeater, such website could be 10.2.3.0/24. It means that as long as you are at the IP address of 10.2.3.0/24, you can execute the functions to control Repeater. Another example is 10.0.0.3, as long as you are at the IP address of 10.0.0.3, you can execute the function by connecting to the WAN port of Repeater and manage the functions of Repeater.

SNMP: Repeater supports SNMP v2 read only data access. The Administrator can specify the IP address and the SNMP community name to determine the target of the management information base (MIB) exported from the Repeater.



System Time: The Repeater supports NTP communication protocol to correct the network time. Please specify the IP address of a server on the system configuration interface. (Universal Time is Greenwich Mean Time, GMT).

Time Zone: Set up the time zone for Repeater, and the default is GMT+08:00.



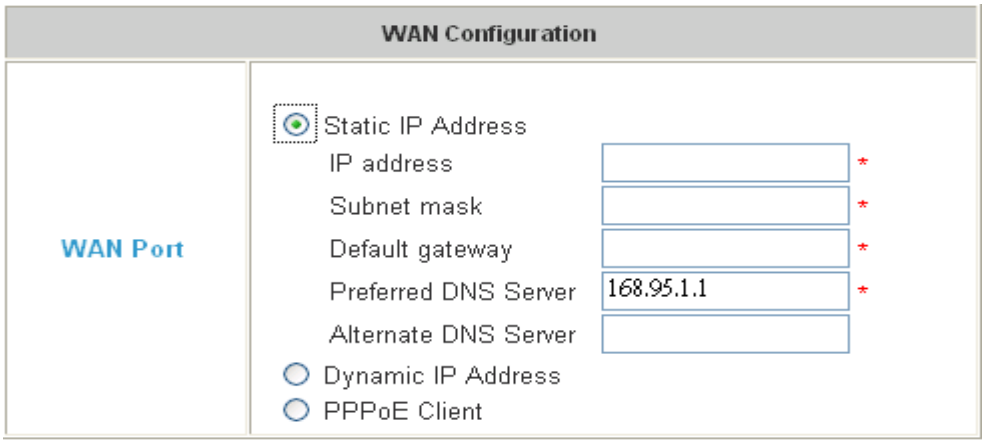
Set Device Date and Time: Set up the current time for the Repeater.

5.1.3. WAN Configuration

There are 3 methods of obtaining IP from the WAN Port: Static IP Address, Dynamic IP Address, and PPPoE.

1. **Static IP Address**: Manually specify the IP address of the WAN Port, which is applicable for the network environment that the IP address cannot be obtained from WAN Port automatically.

Figure 5-22 Example of WAN Static IP Mode



2. **Dynamic IP Address**: It is applicable for the network environment of WAN Port to obtain automatically the IP address, through a DHCP Server constructed in the network of the WAN Port.

Figure 5-23 WAN Dynamic IP Mode

WAN Configuration	
WAN Port	○ Static IP Address ◉ Dynamic IP Address ○ PPPoE Client

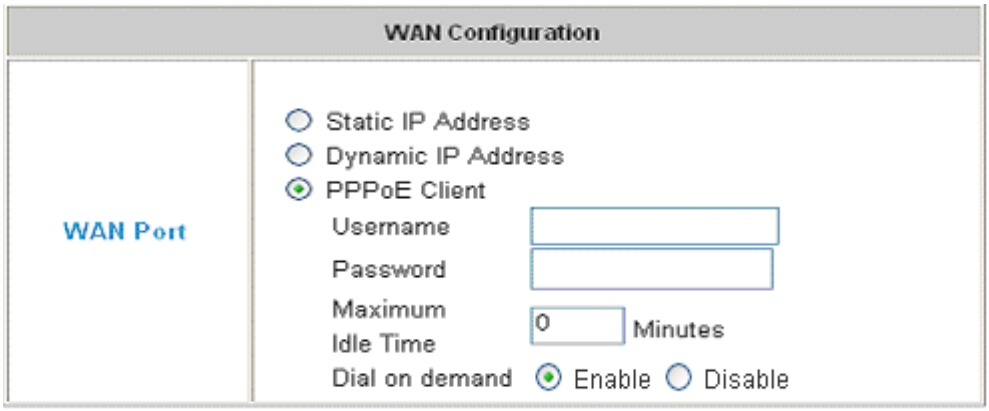
3. **PPPoE:** If WAN Port uses the network environment connected by PPPoE, please select PPPoE, and set the username and password.

Figure 5-24 WAN PPPoE Mode

WAN Configuration	
WAN Port	○ Static IP Address ○ Dynamic IP Address ◉ PPPoE Client Username [ ] Password [ ] Dial on demand ○ Enable ◉ Disable

3.1 Dial on Demand: When the **Dial on Demand** function is enabled under PPPoE, the system will automatically disconnect the user after an idle time as specified here.

Figure 5-25 Dial on Demand



5.1.4. Authentication Configuration

Repeater have two ports require of authentication , one is **General Public LAN** , the other is **Wireless port.**

Figure 5-26 Authentication Configuration

1. Public LAN

Figure 5-27 Example of Public LAN Interface Configuration

Public Port	
Public Port	Enable IP PNP ☐ Enable User Authentication ☐ Specific Route Profile: 3:Policy Route 3 Operation Mode: NAT IP Address: 192.168.1.254 * Subnet Mask: 255.255.255.0 *
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: Lease Time: 1 Day Reserved IP Address List ○ Enable DHCP Relay

- **IP PNP**: At the user end, you can use any IP address to connect to the machine at the Public LAN section; no matter what the IP address at the user end is, you can obtain the Public LAN from Repeater and access the network resources properly, suppose you had used static IP address and specified IP address, Subnet Mask, Default Gateway and DNS.
- **User Public LAN**: You can choose to Enable or Disable user Public LAN, if you enable user authentication, you have to define Specific Route Profile to user .
- **Specific Route Profile:** To define specific route for user to access internet.
- **Operation Mode:** It provides two modes: NAT Mode and ROUTER Mode.
- **IP Address:** Enter your desired IP address for setup.
- **Subnet Mask:** Enter your desired Subnet Mask for setup.

Related Setup for DHCP Server of Public LAN:

DHCP Server has three choices: Disable DHCP Server, Enable DHCP Server, and Enable DHCP Relay.

(1) Disable DHCP Server: Disable the function of DHCP Server.

Figure 5-28 Disable the DHCP Server on Public LAN

DHCP Server Configuration	◉ Disable DHCP Server ○ Enable DHCP Server ○ Enable DHCP Relay

(2) Enable DHCP Server: Enable the functions of DHCP Server. Appropriate setup is needed for the standard enabling of DHCP server, and the setup information for DHCP Server includes DHCP Scope Start IP Address, End IP Address, Preferred DNS Server, Alternate DNS Server, Domain Name, WINS Serve, and Reserved IP Address List.

Figure 5-29 Enable the DHCP Server on Public LAN

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: ciphcrium.com.tw * WINS Server: Lease Time: 1 Day Reserved IP Address List ○ Enable DHCP Relay

If you want to use the **Reserved IP Address List** function, please click the hyperlink of 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. Please enter the related Reserved IP Address, MAC, and description (not compulsory) on the management interface. After the information is keyed, click **"Apply"** to complete the setup.

Figure 5-30 Reserve the IP Address Setting on Public LAN

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

(Total:40) First Previous Next Last

(3) Enable DHCP Relay：If you want to enable the **DHCP Relay mode,** you must specify

other DHCP Server IP Address.

Figure 5-31 Enable the DHCP Relay on Public LAN

DHCP Server Configuration	○ Disable DHCP Server ○ Enable DHCP Server ◉ Enable DHCP Relay DHCP Server IP [ ] *

2. Wireless Port

Figure 5-32 Example of Wireless Interface Configuration

Wireless Port	
Wireless Configuration	SSID [W 5101] Auto Channel Selection ☑ Channel [1] Transmission Mode [Mixed] SSID Broadcast ☑ Layer2 Client Isolation ☑ Security Advance
Wireless Port	Enable IP PNP ☐ Enable User Authentication ☑ Operation Mode [NAT] IP Address [192.168.3.254] * Subnet Mask [255.255.255.0] *
DHCP Server Configuration	◉ Disable DHCP Server ○ Enable DHCP Server ○ Enable DHCP Relay

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 keyboard character.

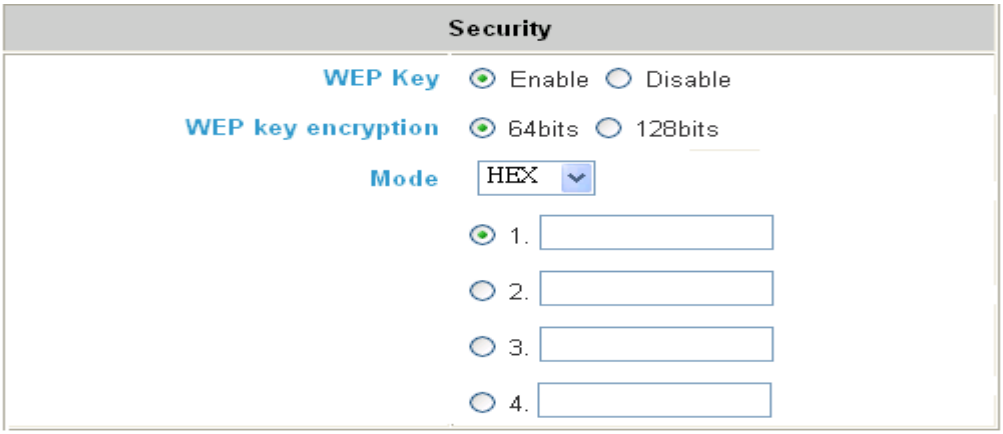
Auto Channel Select: The system will automatically select the appropriate channel.

Chanel : Select the appropriate channel from the list to correspond with your network settings, between 1 and 11 (in North America). All points in your wireless network must use the same channel in order to make sure its correct functioning.

Transmission Mode : There are 3 mode you can select**, 11b-only** (2.4G,1~11Mbps)**, 11g-only** (2.4G,54Mbps) and **Mix mode**(b and g)

SSID broadcast: Allows the SSID to be broadcast on your network. You may want to enable this function while configuring your network, but make sure to disable it when you finished. With this enabled, someone could easily obtain the SSID information with site survey software and get unauthorized access to your network. Click **Enable** to broadcast. Click **Disable** to increase network security and prevent the SSID from being seen on networked

Figure 5-33 Security setting



WEP Key(**W**ired **E**quivalent **P**rivacy)A data privacy mechanism based on a 64-bit, 128-bit, or 256-bit shared key algorithm, If you do not wish to utilize WEP encryption, make sure the **Disabled** is selected.

Mode : There are two types that you can select , **HEX** and **ASCII.**

Advance setting in detail: Please click the hyperlink of **Advance.**

Figure 5-34 Advance setting of Wireless

Advance	
Authenticaiton Type	Auto (Default : Auto)
Transmission Rates	Auto (Default : Auto)
CTS Protection Mode	Disable (Default : Disable)
Basic Rates	Default (Default : Default)
Beacon Interval	100 (Default : 100, Milliseconds, Range : 20-1000)
RTS Threshold	2346 (Default : 2346, Range : 256-2346)
Fragmentation Threshold	2346 (Default : 2346, Range : 256-2346)
DTIM Interval	3 (Default : 3, Range : 1-255)

Authntication Type: The default is set to **Auto**, where it auto-detects for **Shared Key** or **Open System.** Shared Key is when both the sender and the recipient share a WEP key for authentication. Open Key is when the sender and the recipient do not share a WEP key for authentication. All points on your network must use the same authentication type.

Transmission Rates: The default setting is **Auto**. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can keep the default setting, **Auto**, to have the Access Point automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Access Point and a wireless client.

CTS Protection Mode: The default value is set to **Disabled**. When set to **Auto,** a protection mechanism will ensure that your Wireless-B devices will connect to Access Point when many

Wireless-G devices are present. However, performance of your Wireless-G devices may decrease.

Basic Rates: The SNMP screen allows you to customize the Simple Network Management. The default value is set to **Default**. Depending on the wireless mode you have selected, a default set of supported data rates will be selected. The default setting will ensure maximum compatibility with all devices. You may also choose to enable all data rates by selecting **ALL**. For compatibility with former Wireless-B devices, select 1-2Mbps.

Antenna select: The default value is set to **Diversity**. In Diversity mode, both antennas will be enabled. Otherwise, you can have wireless transmission operating only on the **Left** or **Right** antenna.

Beacon Interval: This value indicates the frequency interval of the beacon.The default value is 100. Enter a value between 20 and 1000 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Access Point to synchronize the wireless network.

RTS Threshold: This value should remain at its default setting of 2346.Should you encounter inconsistent data flow, only minor reductions are recommended.

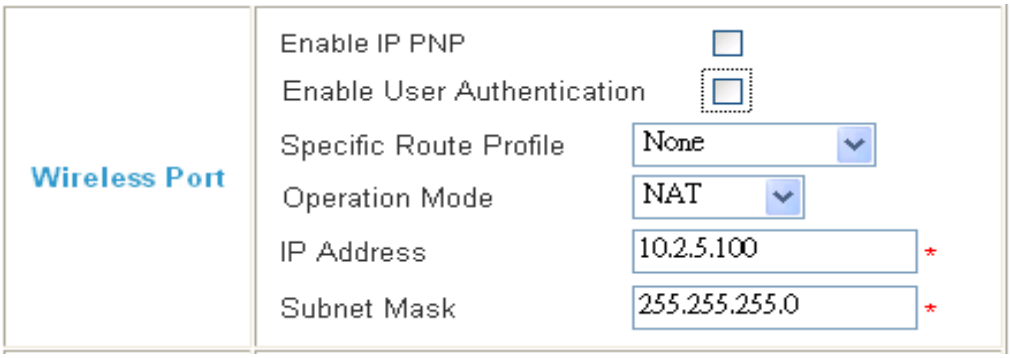
Fragmentation Threshold: This value specifies the maximum size for a packet before data is fragmented into multiple packets. It should remain at its default setting of 2346. A smaller setting means smaller packets, which will create more packets for each transmission. Only minor reductions of this value are recommended.

DTIM Interval: . The default value is 3. This value, between 1 and 255 milliseconds, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Access Point Clients may hear the beacons and informed to receive the broadcast and multicast messages.

Layer2 Client Isolation: You can enable this function to isolate two different domains or just Disable from system default.

EX:10.2.3.4 can't see 10.2.4.4

Figure 5-35 Wireless Port Configuration(2)



IP PNP: At the user end, you can use any IP address to connect to the machine at the Public LAN section; no matter what the IP address at the user end is, you can obtain the Public LAN from Repeater and access the network resources properly, suppose you used static IP address and specified IP address, Subnet Mask, Default Gateway and DNS.

User Public LAN: You can choose to Enable or Disable user Public LAN, if you enable user authentication, you have to define Specific Route Profile to user.

Specific Route Profile: To define specific route for user to access network.

Operation Mode: It provides two modes: NAT Mode and ROUTER Mode.

IP Address: Enter your desired IP address for setup.

Subnet Mask: Enter your desired Subnet Mask for setup.

Related Setup for DHCP Server of Public LAN. DHCP Server has three choices: Disable

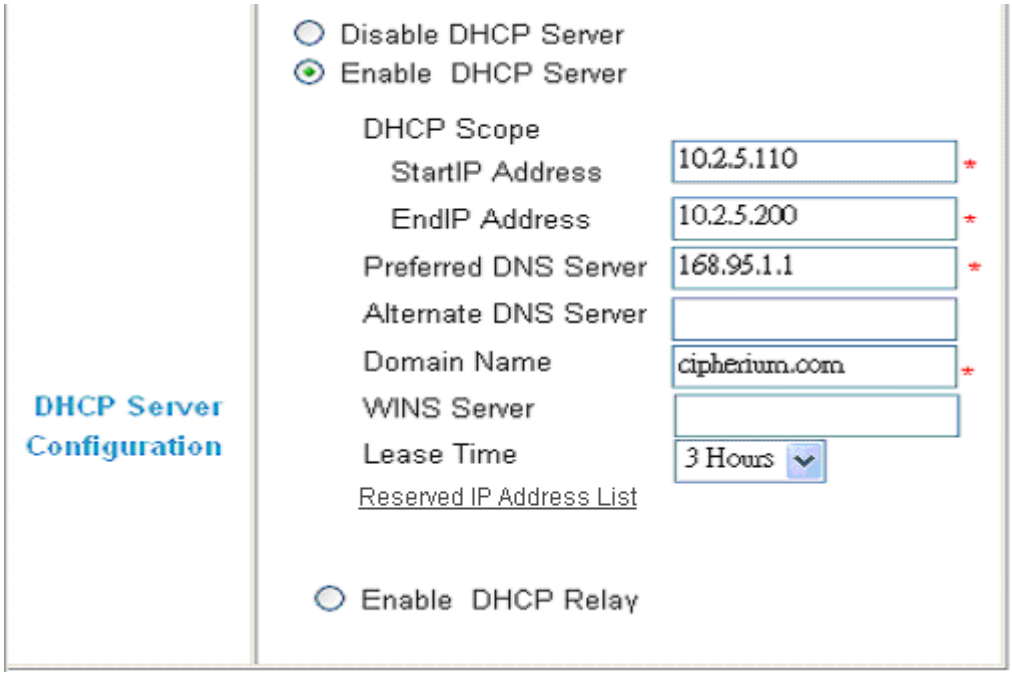
DHCP Server, Enable DHCP Server, AND Enable DHCP Relay

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

Figure 5-36 Disable the DHCP Server on Wireless

2. **Enable DHCP Server:** Enable the functions of the DHCP Server. Appropriate setup is needed for the normal enabling of the DHCP server, and the setup information includes DHCP Scope Start IP Address, End IP Address, Preferred DNS Server, Alternate DNS Server, Domain Name, WINS Serve, and Reserved IP Address List.

Figure 5-37 Enable the DHCP Server on Wireless



If you want to use the **Reserved IP Address List** function, please click the hyperlink of 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. Please enter the related Reserved IP Address, MAC, and description (not compulsory) on the management interface. After the information is keyed, click **"Apply"** to complete the setup.

Figure 5-38 Reserve the IP Address Setting on Wireless

Reserved IP Address List -- Wireless			
Item	Reserved IP Address	MAC	Description
1	10.2.3.22	11:11:11:11:11:11	ffdsfds
2			
3			
4			
5			
6			
7			
8			
9			
10			

(Total:40) First Previous Next Last

3. **Enable DHCP Relay**：If you want to enable the **DHCP Relay mode,** you must specify other DHCP Server IP Address.

Figure 5-39 Enable the DHCP Relay on Wireless

DHCP Server Configuration	○ Disable DHCP Server ○ Enable DHCP Server ◉ Enable DHCP Relay DHCP Server IP [ ] *

WDS Configuration: provides a possibility to extend the Network access. The W-5101

is acting as a Repeater, receiving access request from AP or clients and pass the request to Repeater to obtain authentication.

Figure 5-40 WDS Configuration

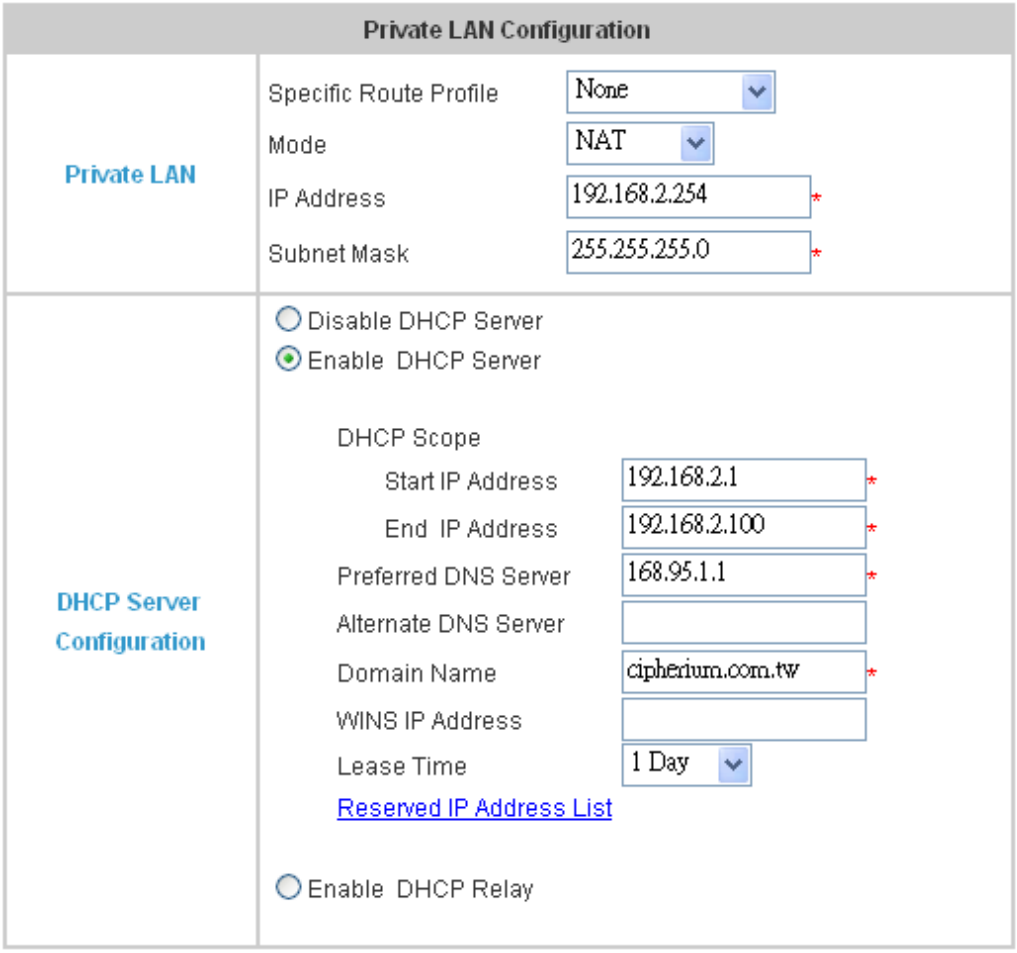
WDS Configuration	Enable Disable Item | MAC Address 1 2 3

W-5101 MAC address: the MAC address of W-5101. W-5101 is a peripheral device supporting Repeater to extend the wireless access. A maximum of three W-5101 is possible for the extension.

5.1.5. Private Configuration

Set up the Specific Route Profile rule, execution mode, IP address, and Subnet Mask of Private LAN Port as shown in the following figure.

Figure 5-41 Example of Private LAN Interface



Specific Route Profile: From the pull-down menu, select your desired Specific Route Profile rule or select **"None"**.

Mode: It provides two modes: NAT Mode and ROUTER Mode.

NAT Mode: All IP addresses externally connected through the Private LAN Port (these IP address must belong to the same subnet as the Private LAN Port) will be converted into the IP address of the WAN Port by the Repeater and connected to the outside

network.

Router Mode：All IP addresses externally connected through the Private LAN Port use its own IP address for external connections. Then, the Repeater acts like a Router.

IP Address: Enter your desired IP address for the setup.

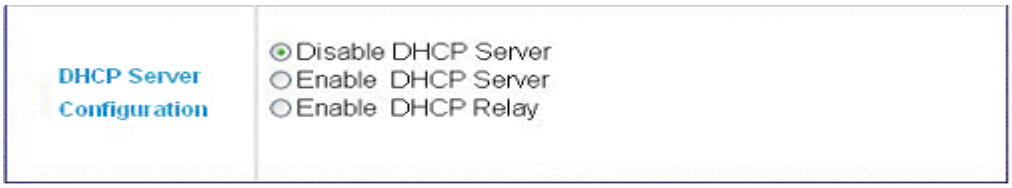
Subnet Mask: Enter your desired Subnet Mask for the setup.

Related Setup for DHCP Server of Private LAN Port:

DHCP Server provides three choices: **Disable DHCP Server, Enable DHCP Server**, and **Enable DHCP Relay.**

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

Figure 5-42 Disable DHCP Server on Private LAN



2. Enable DHCP Server: If you enable the DHCP Server function, it is necessary to have appropriate setups to properly enable the DHCP server. The setup related data includes DHCP Scope Start IP Address, End IP Address, Preferred DNS Server, Alternate DNS Server, Domain Name, WINS Serve, and Reserved IP Address List.

Figure 5-43 Enable DHCP Server on Private LAN

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 IP Address: Lease Time: 1 Day Reserved IP Address List ○ Enable DHCP Relay

If you want to use the **Reserved IP Address List** function, please click the hyperlink of 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. Please enter the related Reserved IP Address, MAC, and some description (not compulsory) on the management interface. After the information is keyed in, click **"Apply"** to complete the setup.

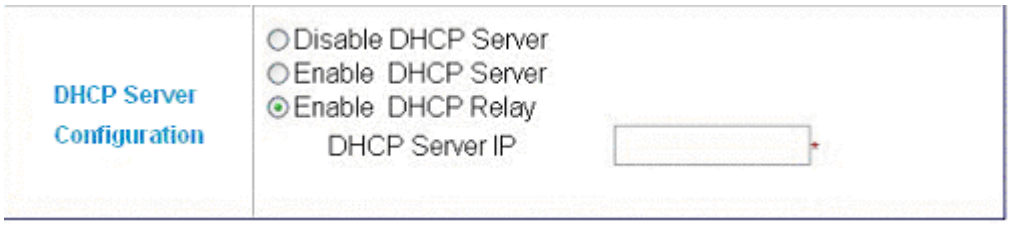
Figure 5-44 Reserve IP Address Setting on Private LAN

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

(Total:40) First Previous Next Last

3. **Enable DHCP Relay:** Enable the DHCP Relay mode. If you want to set up this mode, it is necessary to specify another DHCP Server IP address.

Figure 5-45 Enable DHCP Relay on Private LAN



5.2. User Authentication

This option provides to Administrator the advanced system set up according to the following detailed items including **Authentication Policies**, **Group Configuration**, **Black List Configuration**, **Guest User Configuration**, **Roaming Configuration**, **Additional Configuration** and **On-demand User configuration**.

5.2.1 Authentication Policy

The Repeater provides a simple interface simplifying the complicated management setup, and the system provides a total of 5 management setups. Administrator can adopt different Authetication methods according to each management setup. Each management setup has at most 20 management rules to go with the group configuration, so that the management on general users is once more diversified and flexible. Administrator can select the desired management set up through the pull-down menu. In addition, a layer 2 Authentication is also possible.

Figure 5-46 Example of Authentication Policy(1)

Preferred Authentication Policies	
Authentication Policy	1:postfix1
Authentication Policies Configuration	
Authentication Policy	3:postfix3 Prefered Authentication Method: ☐
Policy Name	postfix3 *(It's postfix name)
Policy Status	○ Enable ◉ Disable

Preferred Authentication Method: This Authentication method is put to be the Preference.

Authentication Policy: It is the preferred Authentication group.

Authentication Methods Configuration: Authentication method setup.

Authentication Policy: The system provides 5 policy groups for your choice. Select the desired control group from the pull-down menu.

Preferred Authentication Method: After selecting the item, it means that the selected setup control group as shown above is the preferred Authentication method.

Policy Name: In the postfix of this management setup, the Repeater system will control the priority according to the following postfix when the user logs in the system.

Policy Status: You can select Enable (default) or Disable. If you select Disable, then such postfix will be disabled.

Warning: *Policy Name cannot use those words : GRIC, MAC, IP*

Figure 5-47 Example of Authentication Policy(2)

Black List Profile	None
Authentication Server	Local POP3 RADIUS LDAP NT Domain Local Users List Assign to Group: 1:Group1 Exception Configuration Enable Disable

Black List Profile: To select a blacklist profile.

Authentication Server: Provides 5 Authentication Methods: Local, POP3, RADIUS, LDAP, and NT Domain.

Assign to Group: Assign a group to the control group from the pull-down menu.

Exception Configuration: It permits Exception Configuration: It permits to exclude certain accounts as shown in the following figure from being limited by restrictions above.

Figure 5-48 Exception Configuration

Authentication Server

Exception Configuration Enable Disable

If	Attribute	Logic	Value	Group
1		equal to		1:Group1
2		equal to		1:Group1
3		equal to		1:Group1
4		equal to		1:Group1
5		equal to		1:Group1

(Total:20) First Previous Next Last

Attribute: After the Public LAN, the Repeater will obtain the user's attributes related

to authenticated server. Administrator can use certain attributes as the management rule for the setup.

Logic: It has **equal to, not equal to, larger than, smaller than,** and **include** for your choice.

Value: Please fill in a desired value to be evaluated to the Attribute by Logic.

Group: It specifies a user group for all users matching the management equation.

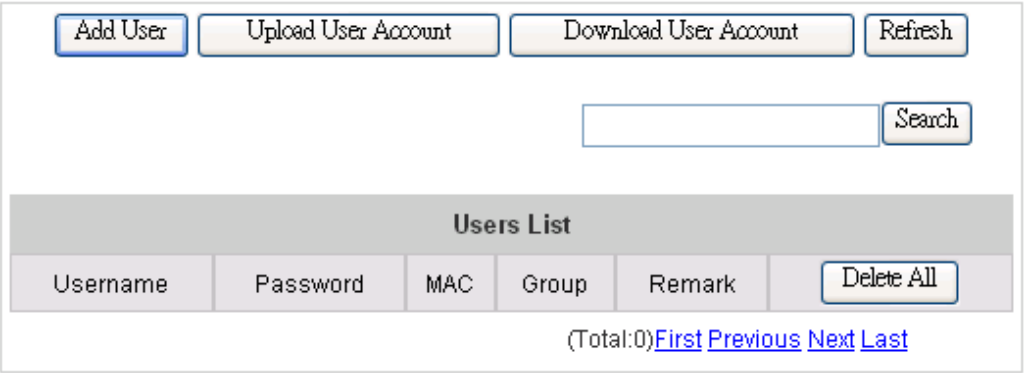
Default Group: If a user who does not match any management equation logins, the priority of this default group will be applied.

Five Authentication Methods:

1. Local

The user's account information is stored in Repeater. If you need to manage the user's account, please click the hyperlink **Local Users List** on the Authentication Server interface to enter the Account Management Interface**.**

Figure 5-49 Local User List



User List: It provides a complete list of existing user accounts as shown in **Figure 5-49**, includes information such as Username, Password, MAC, Group, and Remark.

The Administrator can delete or search user information in this management interface. You can also use the "**Delete All"** function key to delete all user accounts. If you want to edit the

content of individual user account, please directly click the hyperlink of the desired user account to enter the **Edit Account** Interface. Click the "**Refresh"** button to show the most updated data.

Add User: Click "**Add Users"** on the **User List** to enter the **Add User** interface, and key in your desired information such as new username, password (compulsory), MAC, an Remark (not compulsory). Then, click on the **"Apply"** button to complete the insertion. (**Figure 5-50** and **Figure 5-51**)

Edit Account: Click the desired username that you want to modify from the **User List** to enter the User Account Interface, and then key in your desired information such as username and password (compulsory), MAC, and Remark (optional). Then, click **"Submit"** to complete the modification. (**Figure 5-52**)

Upload User Account: Click "**Upload User Accounts"** to enter the Upload User Accounts interface. Click the browser button to select the text file for the user account. Then click **"Submit"** to complete the upload. The format of the uploading file is text file, and each line represents a User Account, **Format→Username, Password, MAC,Remark** each parameter is separated by a comma, and no space is allowed between MAC Remark but the comma is still needed. **(Figure 5-53**)

Download User Account: Click **"Download User Accounts"** in the **User List** to enter the Download User Accounts interface, and the system will directly list all created user accounts, and show a hyperlink for the download at the bottom of the screen. Move the cursor of the mouse to such hyperlink and press the right button of the mouse to save as new file. Then, you can list the user accounts and load them into your computer. (**Figure 5-54**)

Figure 5-50 Example of Adding User Accounts

Add User					
Item	Username	Password	MAC (XX:XX:XX:XX:XX:XX)	Group	Remark
1				None	
2				None	
3				None	
4				None	
5				None	
6				None	
7				None	
8				None	
9				None	
10				None	

Figure 5-51 Added User Accounts Screen

User **'Roson'** has been added!
User **'Gavin'** has been added!
User **'Lisa'** has been added!
User **'Hans'** has been added!

Figure 5-52 Example of Editing User Accounts

Figure 5-53 Example of Upload User Account Interface

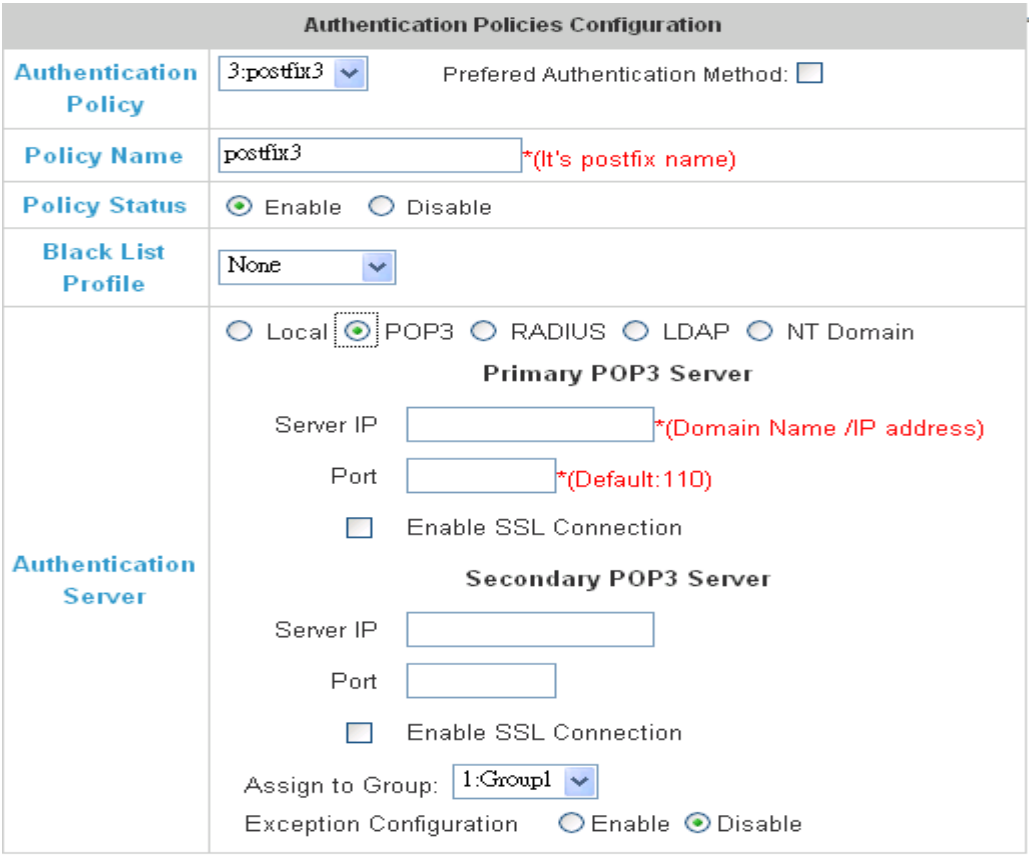
Note: The format of each line is "ID,Password,MAC,Group,Remark" without the quotes. There must be no space between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. When adding user accounts by uploading a file, existing accounts in the embedded database that are also defined in the data file will be replaced by the new ones.

Figure 5-54 Example of Download User Account Interface

2. POP3

If POP3 is used for the Public LAN, you just need to set the Public LAN mechanism to POP3. The setup for primary server or secondary server is available. Enter the IP address or domain name of the Primary POP3 Server and its Primary POP3 Server port. Such setup will be enabled immediately after you click the "**Apply**" button. (It is not compulsory to set up the Secondary POP3 Server).

Figure 5-55 POP3 Setup Screen



Enable SSL Connection: if you select this option, POP3 Protocol will do the Authentication.

3. RADIUS

The RADIUS server sets the external Authentication for user accounts. The setup for primary server or secondary server is available, and such setup will be enabled immediately.

802.1X Public LAN: Select to enable 802.1X as needed. Click the hyperlink "**Edit**" to enter the edit interface of the 802.1X.

Server IP: Key in the location of the RADIUS server by its IP Address or Domain Name.

Authentication Port: It is the Authentication port for RADIUS server.

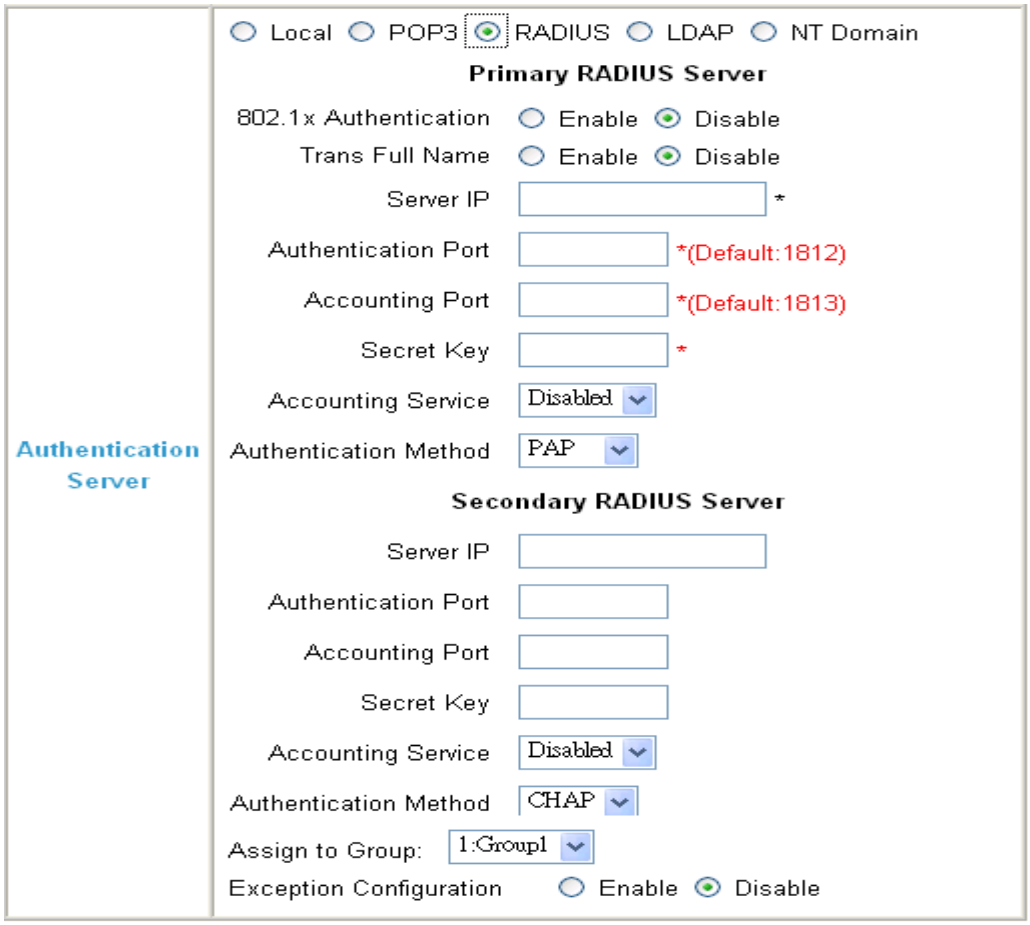
Accounting Port: It is the port reading the accounting information.

Secret Key: It is used for encryption and decryption.

Accounting Service: Select to enable Accounting Service as needed.

Authentication Method: CHAP and PAP are for your choice.

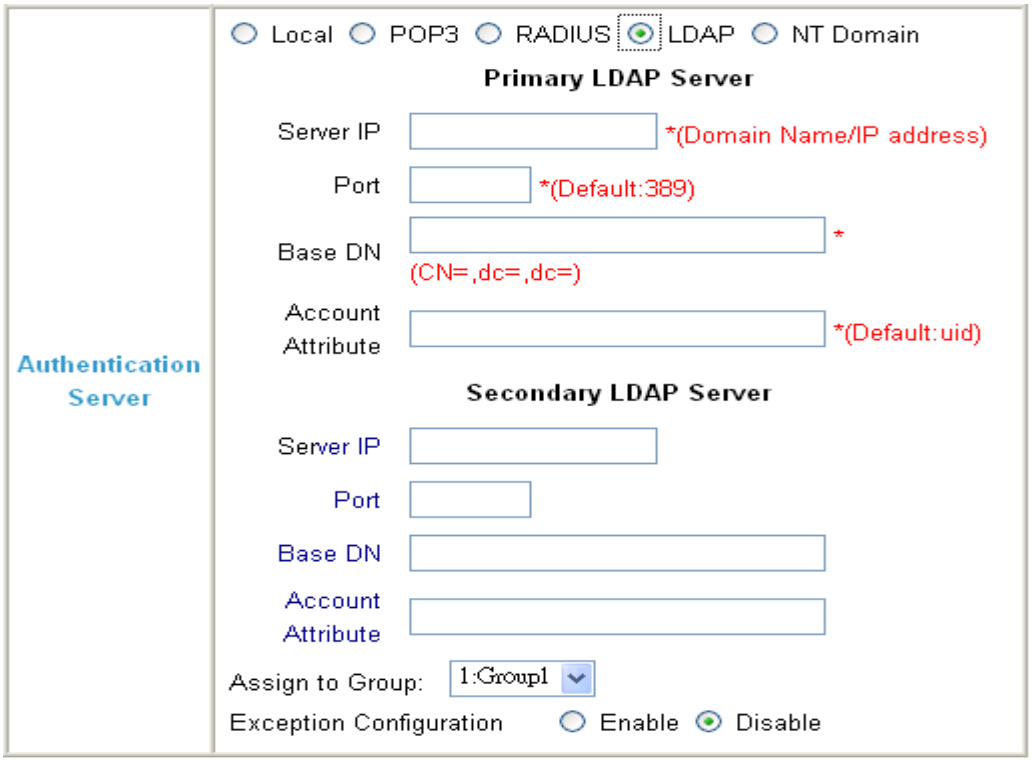
Figure 5-56 RADIUS Setup Screen



4. LDAP

You can select primary server or secondary server as the LDAP server for Public LAN. If you select the LDAP Authentication method, it is necessary to key in the IP Address **(Domain Name), Port number, Base DN Data** of **LDAP Server.** After you confirm the data, please click **"Apply".**

Figure 5-57 LDAP Setup Screen



5. NT Domain

You just need to key in the **IP address** of the **Domain Controller Server** and determine whether or not to enable the Transparent Login function to use the NT Domain server for Authentication.

Figure 5-58 NT Domain Setup Screen

Authentication Server	○ Local ○ POP3 ○ RADIUS ○ LDAP ◉ NT Domain **Domain Controller** Server IP address [ ] * Transparent Login ○ Enable ◉ Disable Assign to Group: 1:Group1 Exception Configuration ○ Enable ◉ Disable

Transparent Login: It sets up whether or not to login the Repeater after a user logins the Windows Domain.

Caution: *1. At present, it only supports win2000 domain controller.*

2. If you want to use NT Domain Autheneication, Please make sure:

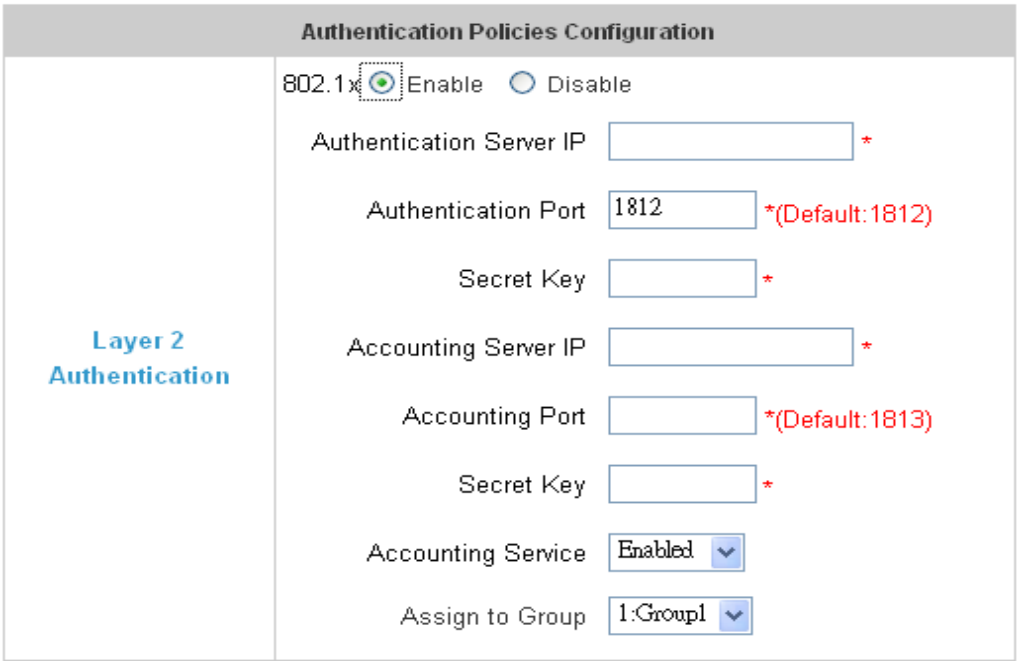
2.1 WAN port Preferred DNS Server IP address is Domain Controller Server IP address

2.2 Walled Garden List has also keyed in Domain Controller Server IP address.

2.3. Policy Name is your complete Domain Name

Layer 2 Authentication: enable/disable so called 802.1x authentication (Please refer to technical handbook for a better picture of this function). Some information are required, such as **Authentication Server IP**, **Authentication Port**, **Secret key** for authentication, **Accounting Service IP**, **Accounting Service Port**, **Secret key** for accounting service, Administrator may also **enable/disable the accounting service** and **assign the Authentication to a group**.

Figure 5-59 Layer 2 Authentication

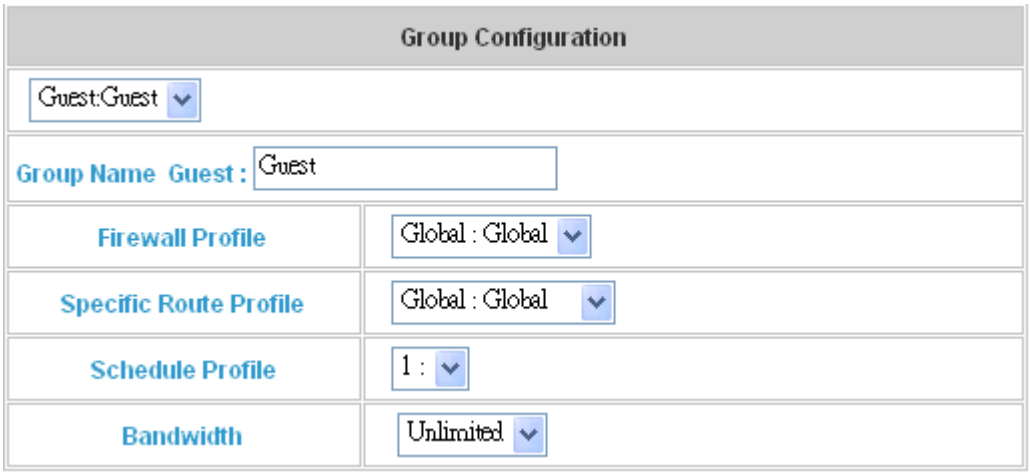


***Caution**: We do not suggest Administrator to enable this function, unless in extreme circumstances. If Administrator enables the layer 2 authentication, all settings at Layer 3, Local, RADIUS, POP3, LDAP, External, will all be OVERRULED and ERASED.*

5.2.2 Group Configuration

In the Repeater system, there are Guest and 5 other user groups for Administrator to manage the firewall profile, route profile and online connection speed in order to control the users. Administrator can use the pull-down menu to select the desired route profile, combining the firewall profile and the route profile with bandwidth control.

Figure 5-60 Group Configuration Screen



Group Name 1: Named this Group.

Firewall Profile: The firewall profile that goes with the system.

Specific Route Profile: The route profile that goes with the system.

Schedule Profile: It sets up the schedule that goes with the logging in system.

Bandwidth: The bandwidth that goes with the system.

5.2.3 Black List Configuration

The Repeater provides a black list function for the system. Administrator can add, delete, or edit a specific black list. Each black list has at most 40 users. If a user logs into the system and such user is on the black list, then the access will be blocked. Administrator can use the pull-down menu to select the desired black list.

Figure 5-61 Example of Black List

Black List Configuration		
Select Black List : 1:Blacklist1		
Name	Blacklist1	
User	Remark	Delete

(Total:0) First Prev Next Last

Add User to List

If you click the hyperlink of **"Add User to List",** the **Add Black List** will appear.

Figure 5-62 Example of Adding User to Black List

Add Users to Blacklist : Blacklist1		
No	Username	Remark
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

After you enter the ID of a user in the black list, click **"Apply"**.

For example, if you successfully add the user b1 into the black list, the system will display a notice to Administrator.

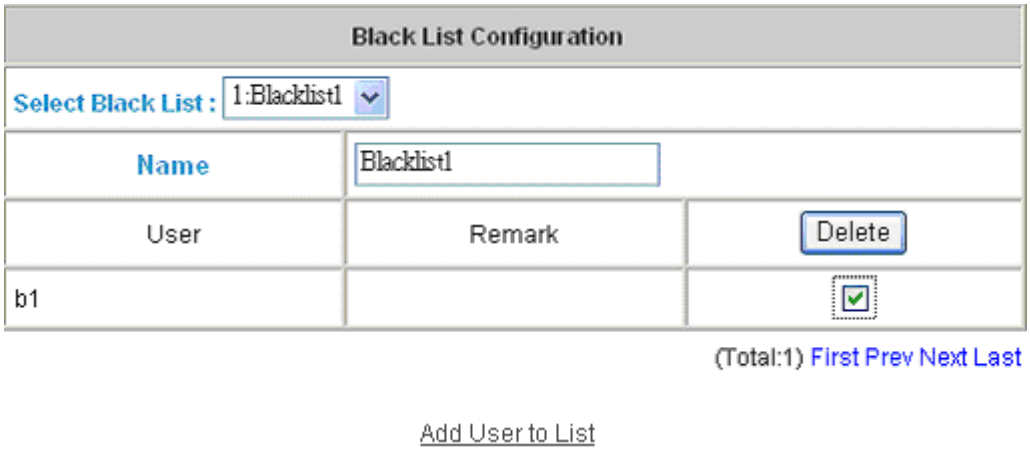
User 'b1' has been added!

After clicking **"Previous",** you will return to the **Black List Configuration**.

If you want to delete a user from the black list, select the delete check box and then click the **"Delete"** button.

Caution: After you delete a user, no message or request of confirmation will appear.

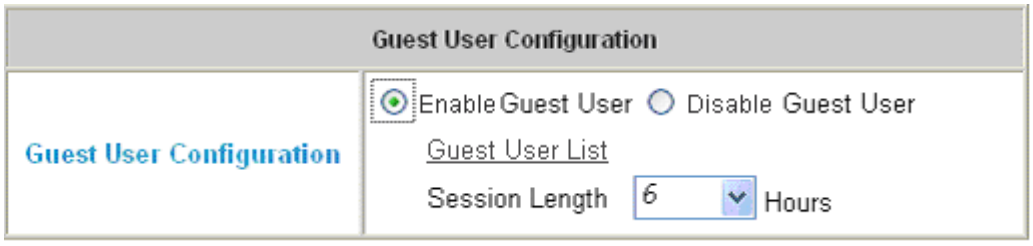
Figure 5-63 Example of Deleting a User from Black List



5.2.4 Guest User Configuration

When you select **Active Guest User**, you can open the **Guest User Configuration** as shown in the following figure.

Figure 5-64 Guest User Configuration Management Interface



Guest User List: The Repeater provides 10 groups for the Guest User List. If you wish to open a certain Guest User List, you just need to key in the corresponding Password in the password column, and then click "**Apply**" to complete the setup for the Guest User Configuration as shown in **Figure 5-65.**

Session Length: It restricts the session used by the Guest User List. The default session length is set to 6 hours , and the limit range is from 1 to 12 hours. After you select the Active Guest User, it is necessary to click "**Apply**" to enable this function.

Figure 5-65 Example of Guest User Management Interface

Guest Users List		
Item	Username	Password
1	guest1	
2	guest2	
3	guest3	
4	guest4	
5	guest5	
6	guest6	
7	guest7	
8	guest8	
9	guest9	
10	guest10	

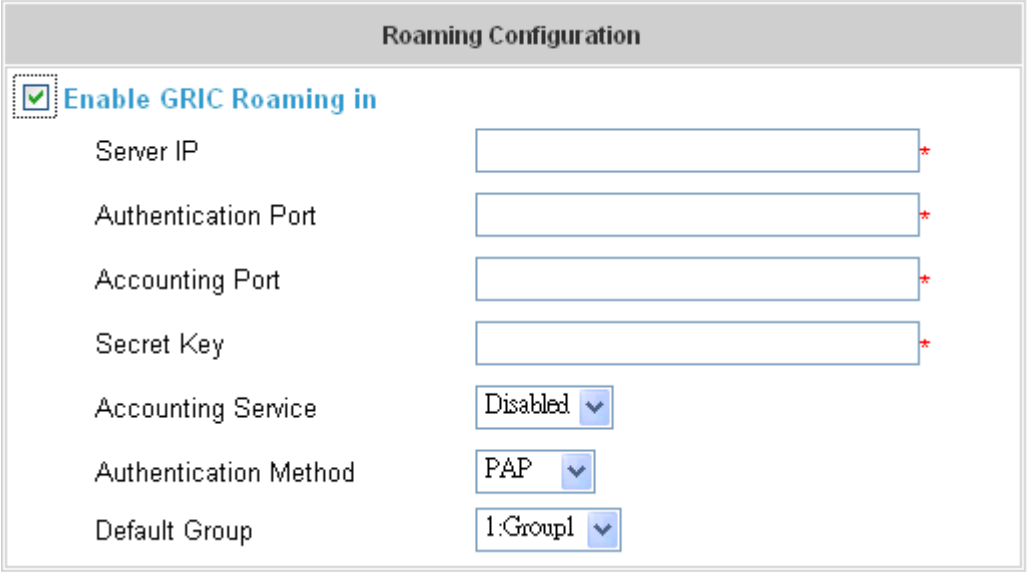
5.2.5 Roaming Configuration

The system provides Repeater and GRIC Server for roaming, and you only need to set up the related parameter in this page to enable the user of the GRIC Server to use the Repeater. These settings will be effective immediately after you click the "**Apply"** button.

The GRIC user will be able to use the webpage **gric.shtml**, and is provided with username,

password, IP, and MAC, so that the Repeater will provide the Authentication and authorization functions.

Figure 5-66 Roaming Configuration



Below is a GRIC example:

Repeater Authentication Port IP address: 192.168.1.254

Username: xyz, and his **IP address**: 192.168.1.100

Password: xyz

MAC address: 01:23:45:67:89:ab

The gric.shtml example should look like this:

https://192.168.1.254/loginpages/gric.shtml?uname=xyz&uip=192.168.1.100&upwd=xyz&umac=01:23:45:67:89:ab

User can also use browser to key in GRIC\username or username@GRIC on ID field and user's password at the login webpage of Public LAN.

5.2.6 Additional Configuration

Figure 5-67 Additional Configuration

Additional Configuration	
User Control	Logout Timer : 10 Min(s) (1 - 1440) Multiple Login : ☐
Friendly	☐ Login 12 Hours ☐ Logout ☐ User Friendlly Credit Reminder
Internet Connection Detection	⦿ Enable ○ Disable URL(or IP):
Upload File	Upload Login Page Upload Logout Page
POP3 Message	Edit Mail Message
Enhance User Authenticate	⦿ Enable ○ Disable Permit MAC Address List

User Control: It applies the rules for general users.

Logout Timer：If a user has idled and not used the network for a while, the system will automatically log out the user. Such logout time can be set in the range of 1~1440, and the default logout time is 10 minutes.

Multiple Login：After you have selected this function, the user with the same ID can log in from several computers.

Friendly： **Login:** After you select this function, the login page will automatically obtain the username and password from previous login. The login page will be dismissed and user no longer needs to enter username and password to login. The username and password for login will be saved for **12 hours.**

Logout: When a user login, a small window will appear and show the user's information and provide you with a logout button for the logout. If you choose to

enable the friendly logout, when you close such window, it will pop out a confirmation window asking if user really wants to logout. If you do not select this option, closing the window will not log out the user.

User Friendly Credit Reminder: For On-Demand Users who have paied before they access internet, they can check how much time left from the login window, and if they only have 10 mintues left, the screen will show some message as below "**You only have 10 minutes left, if you still want to access internet, please check counterjumper** "

Internet connection detection: Repeater detects if the Internet connection is functioning properly by dropping direct packet to the predetermined URL (or IP address).

URL or IP address: this predetermined URL will be used as a target address for Repeater to check the Internet connection.

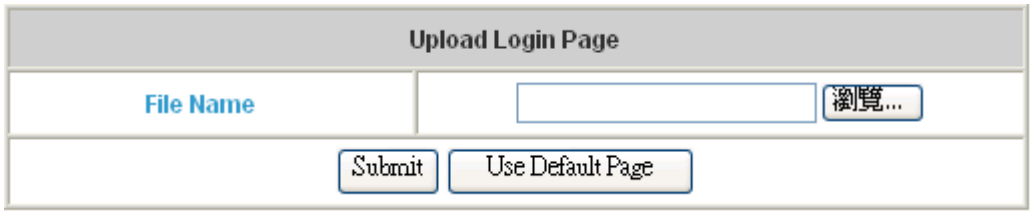
Upload File:

1. Upload Login page

There are three frames with blue edges, which represent 3 sections for user to define the user interface.

If you want to use user-defined interface on Repeater, please enter the filename of the login webpage in the first part of the interface, or browse and click such file. If you want to recover the factory default setting of the login interface, click the "**Use Default Page"** button. After the upload is completed, click the **"Preview"** at the bottom of this page to preview your user-defined login user interface.

Figure 5-68 Upload User-defined Login Interface



The user-defined login interface must include the following HTML codes to provide a channel

for the user to key in username and password.

Figure 5-69 HTML Instructions Required for Using User-Defined Interface

```
<form action="userlogin.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Enter">
<input type="reset" name="clear" value="Clear">
</form>
```

If the user-defined login interface includes a graphic file, the HTML code of the graphic file path must be the upload graphic file. In the **Upload Image** at the third section of this interface **Upload Image File,** key in the path and file name of such graphic file or browse to select such file. The maximum size of the graphic file is 512K.

Figure 5-70 Path of Graphic File in User Login Interface

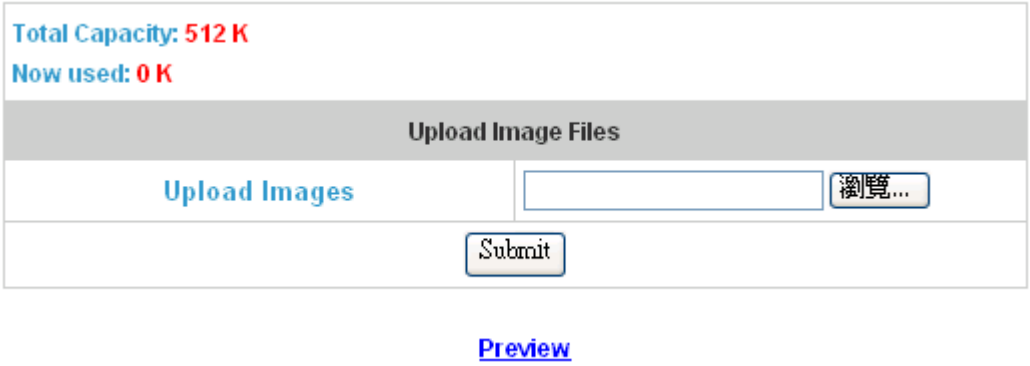
```
<img src="images/xx.jpg">
```

After the graphic file is uploaded, the second section **Existing Image Files** of this page will list the graphic files uploaded to Repeater. You can select or delete any graphic file, and the system will show the used space of the graphic file in the third section.

Figure 5-71 Graphic File Description

After the web page and graphic files are uploaded, you can click **"Preview"** at the bottom of this page to preview your user interface.

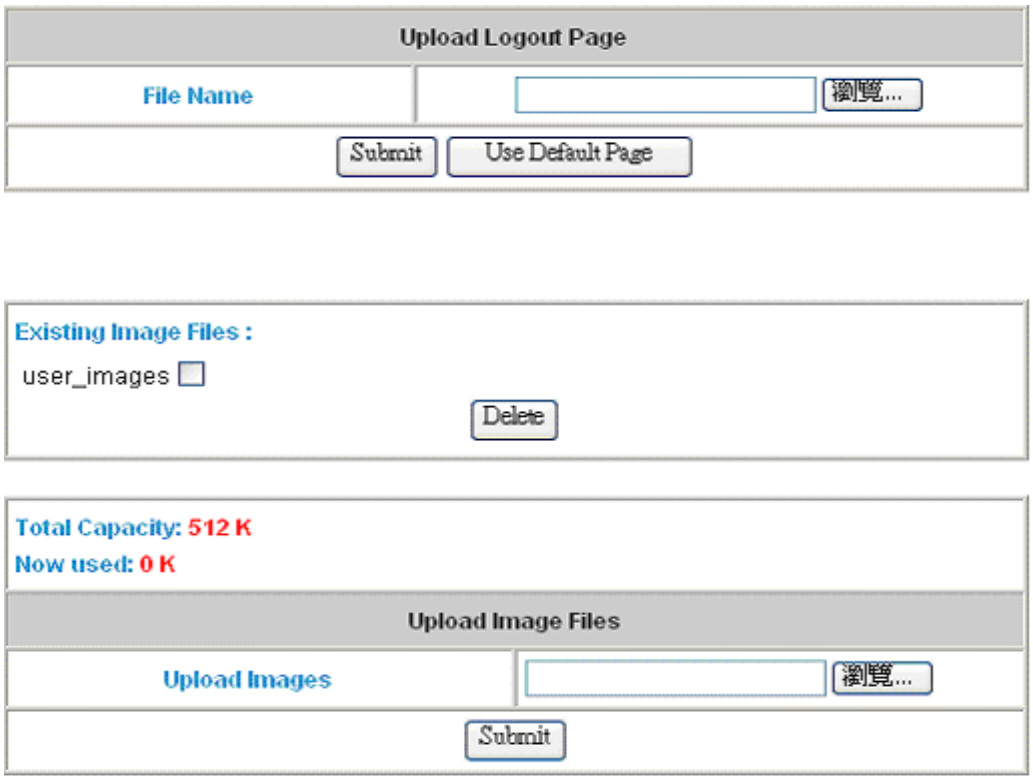
Figure 5-72 Path of Graphic File for User Logout Interface



2. Upload Logout Page

The system will provide you with the user-defined logout interface, which is similar to the user login interface.

Figure 5-73 Upload User Logout Interface



The difference resides on that your user-defined user logout interface must include the

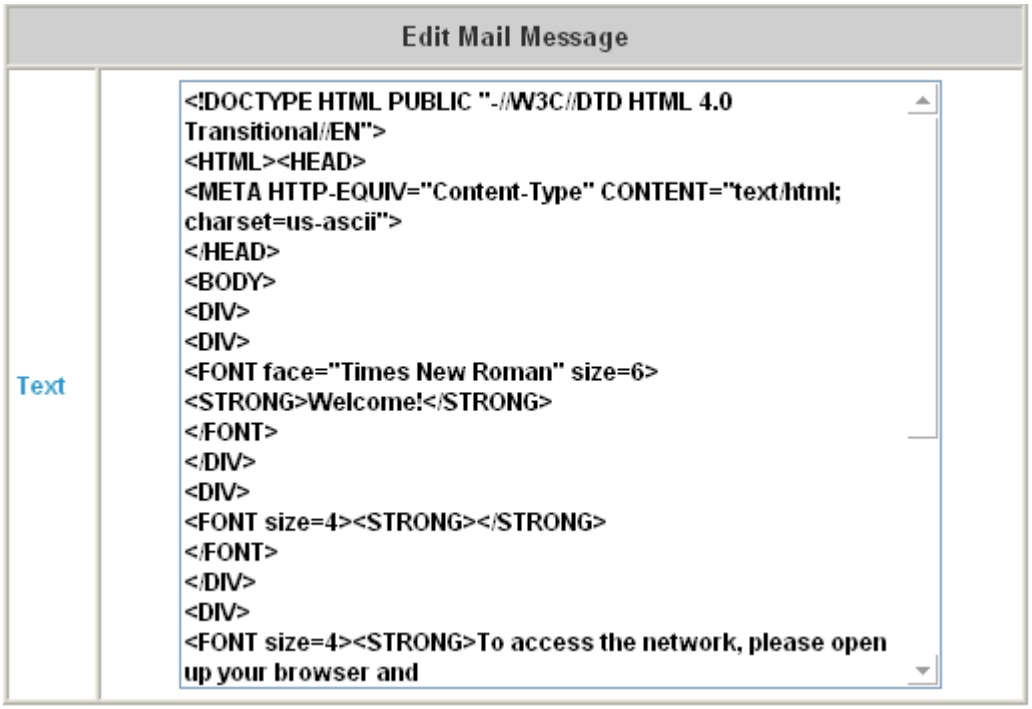
following HTML codes to provide users a channel to enter the username and password.

Figure 5-74 HTML Codes Required for User Logout Interface

```
<form action="userlogout.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Logout">
<input type="reset" name="clear" value="Clear">
</form>
```

POP3 Message: the system can allow administrator to edit its own warning mail sent to user who has opened a mail browser without logging on to the internet beforehand.

Figure 5-75 POP3 Message



Enhance User Authenticate: the system allow administrator to enter at most 40 predetermined MAC addresses, only the user come from these MAC addresses will be able to

reach the login page.

Figure 5-76 MAC Address Control Interface

MAC Address Control			
Item	MAC Address	Item	MAC Address
1		2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

(Total:40) First Prev Next Last

5.2.7 On-demand User Configuration

On-Demand user: When you connect the Printer to Repeater's console port, there are 2000 On-demand users account available. By default, the On-demand user database is empty. While you press the Printer's button, the On-demand user will be created, then print out a receipt (Figure 5-77), which will contain this On-demand user's information. (Figure 5-78) (Figure 5-79).

Figure 5-77 Receipt Information

```
            Welcome!
------------------------
 Username: Cipher
 Password: q6m34m3b
      Price: US$2
      Usage: 60 minute(s)
------------------------
 ESSID:
  W-5101
 Shared WEP Keys
 (HEX 40 bit):
------------------------
 Valid to use until:
  2004/05/05 12:46:56
------------------------
           Thank You!
2004
```

Figure 5-78 On-demand User Configuration

On-demand User Configuration	
Store Name	bonalinx (e.g.: bonalinx. Max: 8 char)
Receipt Header	Welcome! (e.g.: Welcome!)
Receipt Footer	Thank You! (e.g.: Thank You!)
Printer Baud Rate	38400
Assign To Group	1:Group1
WLAN ESSID	W-5101 (e.g.: bonalinx)
WEP Key	cipherium

On-demand Users List Billing Configuration Upload On-demand User

Figure 5-79 On-demand User Page Field and Description

Field	Description
Store Name	You can specify the prefix of the user name, max is 8 char., for example: D-Link.
Receipt Header	You can configure the receipt's header in this filed.
Receipt Footer	You can configure the receipt's footer in this filed.
Printer Baud Rate	You can specify the baud rate to support specific printer,the default setting is 9600.
Assign to Group	You can assign the on-demand to a pre-determined group.
WLAN ESSID	You can specify the AP's ESSID in this filed.
WEP Key	You can specify the AP's WEP key in WEP Key filed.

- **On-demand User List**: A list about on-demand user. A sample list is shown below.

Figure 5-80 On-demand User List

To delete specific users accounts, click on the checkboxes besides those user accounts then click the **Delete** button. To delete all user accounts, click **Delete All**.

- **Billing Configuration:** Billing rule for Administrator to setup at most 10 profiles.

Figure 5-81 Billing Configuration

Billing Configuration					
Button	Status	Type	Account Expire Date	Validity Duration	Price
1	◉ Enable ○ Disable	◉ Data 1 Mbyte ○ Time hrs mins	1 days	1 days	300
2	○ Enable ◉ Disable	○ Data Mbyte ○ Time hrs mins	days	days	
3	○ Enable ◉ Disable	○ Data Mbyte ○ Time hrs mins	days	days	
4	○ Enable ◉ Disable	○ Data Mbyte ○ Time hrs mins	days	days	
5	○ Enable ◉ Disable	○ Data Mbyte ○ Time hrs mins	days	days	
6	○ Enable ◉ Disable	○ Data Mbyte ○ Time hrs mins	days	days	
7	○ Enable ◉ Disable	○ Data Mbyte ○ Time hrs mins	days	days	
8	○ Enable ◉ Disable	○ Data Mbyte ○ Time hrs mins	days	days	
9	○ Enable ◉ Disable	○ Data Mbyte ○ Time hrs mins	days	days	
0	○ Enable ◉ Disable	○ Data Mbyte ○ Time hrs mins	days	days	

Status: Enable/Disable this billing rule.

Type: Administrator may choose Data or Time as user's billing rule.

Time: maximum session time is 24305days

Data Transfer: maximum data transfer is 2002Mbyte.

Account Expire day: After this number of days, if user didn't not activate for the first time, the account will be expired automatically.

Validity Duration: The account will remain valid after this number of days; prior that user has activated his/her account.

Price: Price for the online access.

- **Upload On-demand User:**

Figure 5-82 Upload On-demand User

Note1: The format of each line is "ID, Password, type, Data transfer or Session length, Activation deadline, Validity duration" without the quotes. There must be no space between the fields and commas. When adding user accounts by uploading a file, any existing account in the embedded database that has the same user name as the one defined in the uploaded file will not be replaced by the new one.

Note2: The unit of data transfer is byte. The unit of session length is second.

Upload On-demand User Account	
File Name	瀏覽...
Submit	

File Name: Key in or browse the file that contains the on-demand users information (format as described in Note 1).

5.3 Group Profile

The Repeater provides three kinds of Profile configurations, including **Firewall Profile**, **Specific Route Profile**, and **Login Schedule Profile**.

5.3.1 Firewall Profile

The system offers Global and 5 firewall profiles. If you want to set up the firewall rules to suit all users, you can set such firewall profile in Global, and the other five firewall profiles can be set without conflict between one another.

Figure 5-83 Example of Firewall Profile

Firewall Profiles

Global:Global

Profile Name: Global

Filter Rule Item	Active	Action	Name	Source	Destination	Protocol	MAC
1	☐	Block		ANY	ANY	ALL	
2	☐	Block		ANY	ANY	ALL	
3	☐	Block		ANY	ANY	ALL	
4	☐	Block		ANY	ANY	ALL	
5	☐	Block		ANY	ANY	ALL	
6	☐	Block		ANY	ANY	ALL	
7	☐	Block		ANY	ANY	ALL	
8	☐	Block		ANY	ANY	ALL	
9	☐	Block		ANY	ANY	ALL	
10	☐	Block		ANY	ANY	ALL	

(Total:50) First Prev Next Last

Filter Rule Item: The filter rule uses a serial filter to determine the permission of transmission from the source address to the target address or examine whether there is a data loss. Please click **Index Number** for the detailed information.

Figure 5-84 Select the Group for Applying Firewall Profile Rules

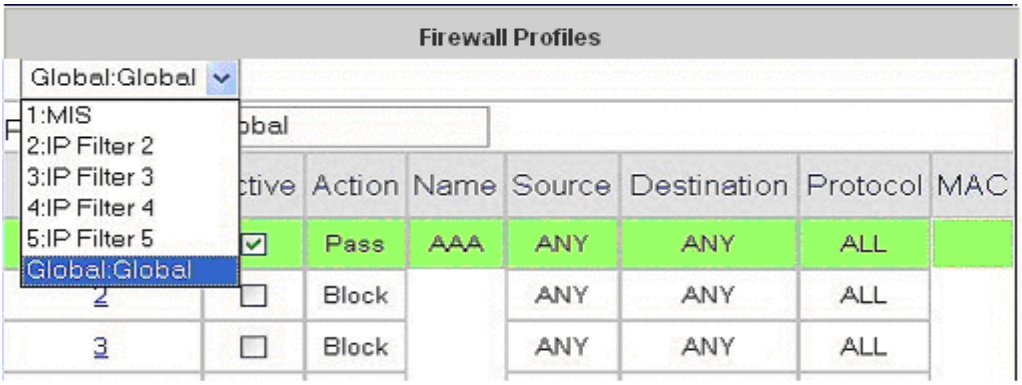
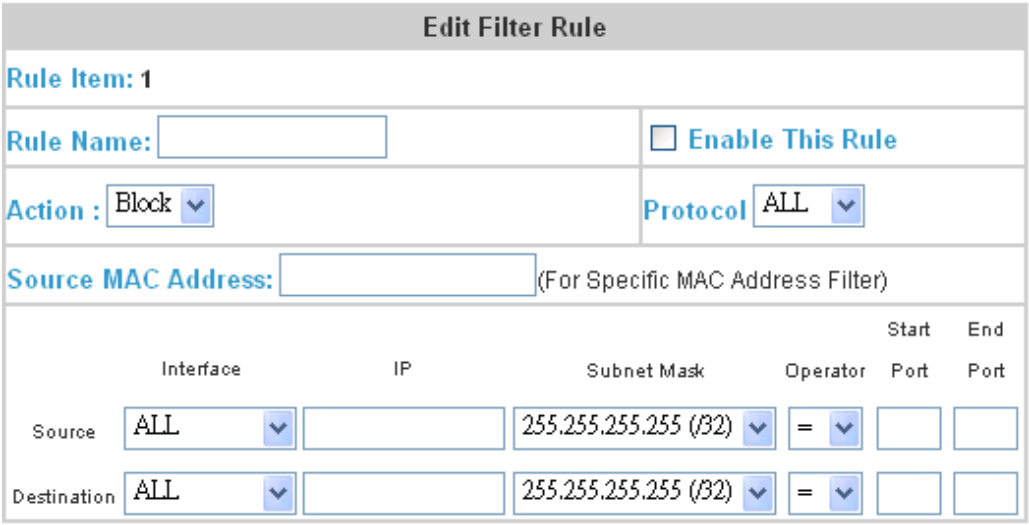


Figure 5-85 Example of Edit Filter Rule



The figure above sets up the first IP Filter rule for the first firewall profile, in which all of its contents are sent from 192.168.1.1, and the destination is 192.168.1.100; Port=54 packets, which will be blocked directly by the system regardless of TCP, UDP, or ICMP.

Rule Name: Name this IP Filter rule.

Enable this Rule: Such rule will be effective when selected.

Action: If your setting matches,

Pass：The packet passes successfully.

Block：The packet is blocked.

Protocol: Provides three kinds of protocols: TCP, UDP, and ICMP for your choice. All stands for all three protocols chosen.

Source MAC: Source Address of the MAC Address.

Source (Destination) IF: Source (Destination) Interface includes 4 interfaces: WAN, Public LAN, Private LAN and wireless for your choice. ALL stands for all the four interfaces.

Source (Destination) IP Address: IP address of Source (Destination).

Source (Destination) Subnet Mask: Subnet Mask of Source (Destination).

Source (Destination) Operator: Provides the comparison rules: =(Equal), != (Not Equal), > (Larger Than), and < (Less Than).

Source(Destination) Start Port: Start Port of Source (Destination)。

Source(Destination) End Port: End Port of Source (Destination)。

5.3.2 Specific Route Profiles

The Repeater system provides the route profile setup function, letting Administrator to determine the network path which suits all routers best and send the packet to the destination through network. Administrator can use the pull-down menu to select and set your desired route profile.

Figure 5-86 Example of Editing Specific Route Profile

Specific Route Profile

Global:Global

Profile Name: Global

Route Item	Destination		Gateway	Default
	IP Address	Subnet Netmask	IP Address	
1		255.255.255.255 (/32)		☐
2		255.255.255.255 (/32)		☐
3		255.255.255.255 (/32)		☐
4		255.255.255.255 (/32)		☐
5		255.255.255.255 (/32)		☐
6		255.255.255.255 (/32)		☐
7		255.255.255.255 (/32)		☐
8		255.255.255.255 (/32)		☐
9		255.255.255.255 (/32)		☐
10		255.255.255.255 (/32)		☐

Profile Name: Name of this Specific Route Profile.

Destination IP Address: It is the network or Server IP that specifies the destination of the connection. The IP 192.168.202.0 is used as the destination of the connection.

Subnet Netmask: It specifies the netmask destination; the subnet mask of 192.168.202.0 is an example.

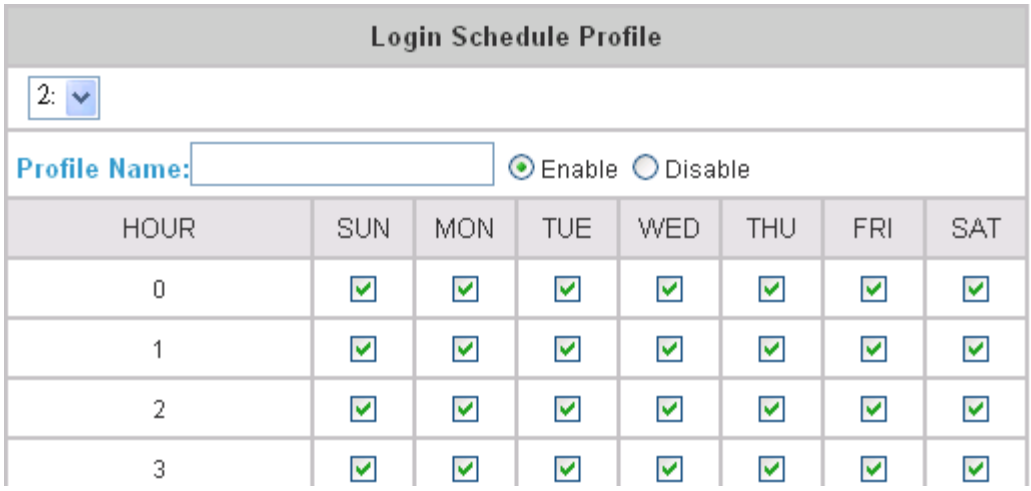
Gateway IP Address: It specifies the IP address for the next connected router. The setting here is 192.168.200.253 because it is behind the router at 192.168.202.0.

After the static route is changed, it is necessary to restart Repeater to refresh the setting.

5.3.3 Login Schedule Profiles

The user's login schedule can be set. After the setup is completed, please click **"Apply"** to save the settings in Repeater.

Figure 5-87 Example of Guest Login Schedule Management Interface



5.4 Network Configuration

Five functions are provided to control individual jobs of the network transmission, which include **Network Address Translate**, **Privilege List**, **Walled Device list**, and **Proxy Server Properties.**

5.4.1 Network Address Translate

1. Static Assignments

If you have several IP addresses, you can assign them to the WAN port of Repeater. You can define at most 40 groups for the correspondence combination at the Ethernet end (Virtual IP Address) and WAN end (Public IP Address). The WAN port of Repeater will automatically set the public address defined here. These settings will be effective immediately after you click

the **"Apply"** button.

Figure 5-88 Defining the Static Assignment Address Correspondence

Static Assignments		
Item	Internal IP Address	External IP Address
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

(Total:40) First Prev Next Last

2. Public Accessible Server

This function allows Administrator to define at most 40 virtual servers, so that the computer other than those of the managed network can access the server in the managed network. According to the different services provided, the network service can be provided on the TCP port or UDP port, or both. These settings will be effective immediately after you click "**Apply**".

Figure 5-89 Defining Public Accessible Server

Public Accessible Server					
Item	External Service Port	Local Server IP Address	Local Server Port	Type	Enable
1				○TCP ○UDP	☐
2				○TCP ○UDP	☐
3				○TCP ○UDP	☐
4				○TCP ○UDP	☐
5				○TCP ○UDP	☐
6				○TCP ○UDP	☐
7				○TCP ○UDP	☐
8				○TCP ○UDP	☐
9				○TCP ○UDP	☐
10				○TCP ○UDP	☐

3. Port and IP Redirect

When any user attempts to connect to the destination defined in this interface, the connection packet will be converted to the corresponding destination. You can define at most 40 groups on this interface for the redirect condition. These settings will be effective immediately after you click **"Apply".**

Figure 5-90 IP Address and Network Port Redirect

Port and IP Redirect					
Item	Destination		Translated to Destination		Type
	IP Address	Port	IP Address	Port	
1					○ TCP ○ UDP
2					○ TCP ○ UDP
3					○ TCP ○ UDP
4					○ TCP ○ UDP
5					○ TCP ○ UDP
6					○ TCP ○ UDP
7					○ TCP ○ UDP
8					○ TCP ○ UDP
9					○ TCP ○ UDP
10					○ TCP ○ UDP

(Total:40) First Prev Next Last

5.4.2 Privilege List

1. Privilege IP Address List

Although all devices at the user end are managed, sometimes you still need to have a user end with some exception processing. For example, if the server has been put on the managed network and you want to login to the network from such server without going through the Public LAN. To permit a specific device at the user end to have the network access right without going through the Public LAN, you only have to key in the IP address at user end, as shown in **Figure 5-90** privilege IP address. This system allows at most 100 Privilege IP addresses. These settings will take effect immediately after you click **"Apply"**.

Warning: *Permitting certain IP address to have network access rights without going through standard authentication process at the Public LAN may cause security problems.*

Figure 5-91 Privilege IP Address

Privilege IP Address List		
Item	Privilege IP Address	Remark
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

(Total:100) First Prev Next Last

2. Privilege MAC Address List

Besides permitting specific IP address at user end to have the "free" network access right without going through the Public LAN, the system also provides a way to do so according to the MAC address at the user end. In **Figure 5-92** Direct Connecting MAC Address, enter the MAC address at the user end. This system permits at most 100 Privilege MAC addresses to have network access right without going through the Public LAN. The format of the MAC address is **XX:XX:XX:XX:XX:XX**. These settings will be effective immediately after you click **"Apply".**

Warning: *Permitting specific IP address to have network access rights without going through the Public LAN may cause security problems.*

Figure 5-92 Direct Connecting MAC Address

Privilege MAC Address List			
Item	MAC Address	Group	Remark
1	00:11:22:33:44:55	Group1	
2		Guest	
3		Guest	
4		Guest	
5		Guest	
6		Guest	
7		Guest	
8		Guest	
9		Guest	
10		Guest	

(Total:100) First Prev Next Last

5.4.3 Monitor IP List

The system will send out the packet regularly, to monitor and control the status of the IP addresses on the list. If the monitored IP address does not exist, the system will send out an e-mail to Admin once every 30 minutes, such as: 1:00, 1:30, 2:00, 2:30, and 3:00 until the problem is fixed. Click "**Monitor**" to view all monitored IP (**Figure 5-93**). A maximum of 40 IP address for the monitoring is allowed.

Figure 5-93 Monitor IP List

Admin Email	
Sender	
Receiver	
Interval	1 Hour

Monitor IP List			
Item	IP Address	Item	IP Address
1		2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

(Total:40) First Prev Next Last

Monitor

Sender: The email address of administrator server who is in charge of the monitoring.

Receiver: The email address of a predefined IP user who is being monitored.

Interval: The interval time for administrator server to dispatch a warning or an instruction message.

Monitor IP list: The list of the IP addresses taken under surveillance.

Monitor: Show monitor IP status. (**Figure 5-94**)

Figure 5-94 Monitor IP result

Monitor IP result		
No.	IP	Result
1	192.168.1.200	

5.4.4 Walled Garden List

This system allows users to login to certain websites before passing through the Public LAN. You only need to enter the IP address (or Domain Name) of these websites into the Walled Garden List. You can enter up to 20 addresses into this list. This function lets you provide some free service to users. For example, you can provide a brief introduction of the local site, facilities and path guide on a website, and list the address of the website in the Walled Garden. Even the users having no network access right can link to the website of the Walled Garden to obtain the precious information related to the local site. This function can be used to provide users a free chance to experience the network service. The customer can experience the actual network service without any preparation in advance. These settings will be effective immediately after you click **"Apply".**

Figure 5-95 Defining Walled Garden Server Address

Walled Garden List			
Item	Address	Item	Address
1		2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

5.4.5 Proxy Server Properties

Internal Proxy Server: Repeater has a built-in proxy server, if you active this function, end user can specify Repeater as proxy server, no need to enter the IP address and Port.

External Proxy Server: Base on Repeater security management, only port 80 is allowed (it will appear on login webpage). If you have built a Proxy Server in your network environment, and the user's browser is set to Proxy, you must setup your External Proxy Server IP Address and Proxy Port of the Repeater, in order to have proper operations in the Proxy network environment. These settings will be effective immediately after you click "**Apply**".

Figure 5-96 Proxy List

Internal Proxy Server	
Built-in Proxy Server	Enable Disable

External Proxy Server		
Item	Server IP	Port
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

5.4.6 Dynamic DNS

Dynamic DNS: Repeater provides a convenient DNS function, translating the IP address of WAN port to a domain name, facilitating Administrator to connect to WAN port. If the DHCP is activated at WAN port, this function will also update the newest IP address regularly to DNS server.

Figure 5-97 Dynamic DNS

Dynamic DNS	
DDNS	○ Enable ◉ Disable
Provider	DynDNS.org(Dynamic)
Host name	*
Username/E-mail	*
Password/Key	*

Administrator may choose to **enable/disable** this function, choose his own **DNS provider**, define a **hostname for WAN port IP address** (this hostname will be the domain name for WAN port), and key in the ID and password at DNS provider.

5.5 Utilities

This function provides utilities for you to customize and maintain your system including **Change Password**, **Backup/Restore Strategy**, **Firmware Upload,** and **Restart.**

5.5.1 Change Password

To change the Administrator's password, please key in the present Administrator's Password in the field, and then the new Administrator's Password. You must key in the new password twice for confirmation purposes.

Figure 5-98 Change Administrator's Account

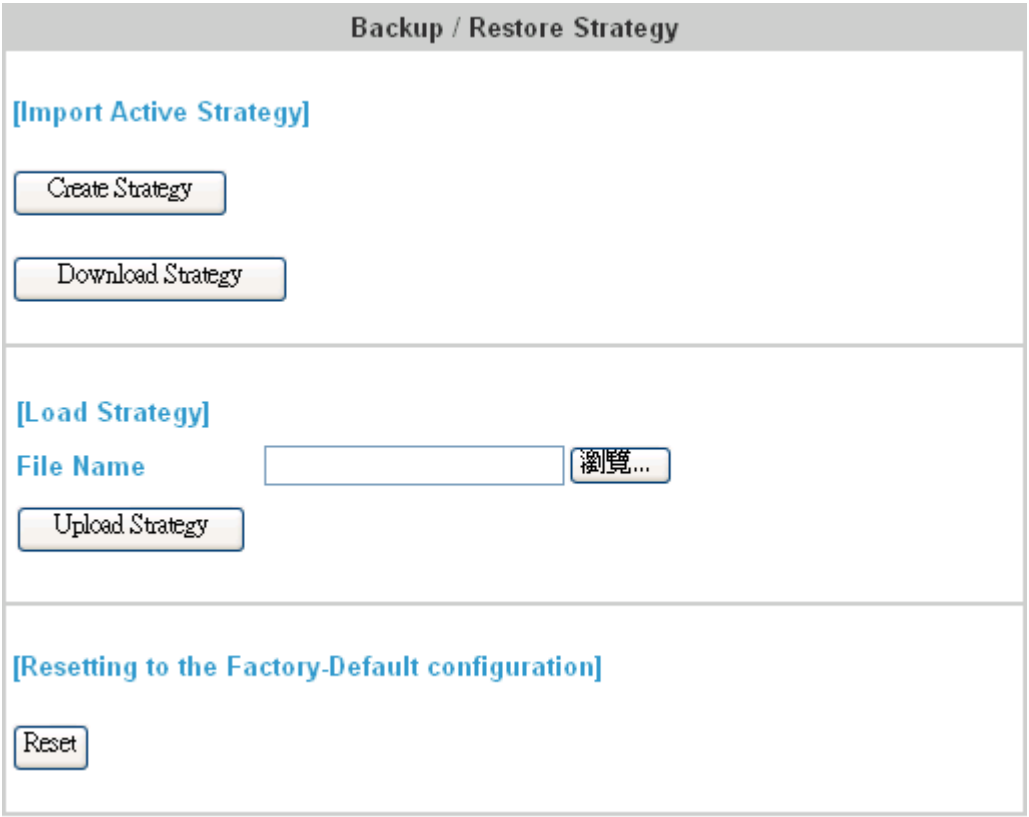
Change Password	
Old Password	
New Password	
Verify Password	

Caution: *If you lost or forgot the Administrator's Password, you can still change the Administrator's password through the text mode management interface on the serial port.*

5.5.2 Backup / Restore Strategy

It provides the backup function; resumes current setting of Repeater. This function can also restore the factory default setting.

Figure 5-99 Backup and Restore



Import Active Strategy: Generate the backup (image) file.

Load Strategy: It loads the backup graphic file for the setup status (Caution: Such graphic file must be generated by Repeater).

Resetting to the Factory-Default configuration: Restore to the default setting of Repeater.

5.5.3 Firmware Upgrade

You can upgrade your Repeater firmware from the Cipherium website.

Figure 5-100 Executing the Firmware Upgrade

Firmware Upgrade	
Current Version	1.00.C3
File Name	Browse

Warning: *Firmware upgrade may cause data loss. Please refer to the version description to see if there is any limitation before upgrading your firmware.*

Click "**Browse**" to browse the files. After you have found the firmware image file, click "**Submit**" and the browser will upload such file to Repeater, and then the system will start upgrading the file.

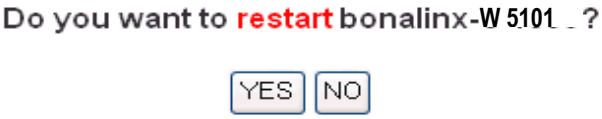
You must restart the system before the upgrade firmware is effective. If you have modified any setting, remember to save the setting before restarting the system.

Warning: *Please restart the system through the management interface. Do not turn off the system directly and then turn on the power again. Doing so may damage the upgraded firmware.*

5.5.4 Restart

This function allows you to safely restart Repeater, the restart takes about three minutes. If you need to turn off the power, we recommend you to restart Repeater, and turn off the power after you hear a beep.

Figure 5-101 Restart



Caution: *All online users connected to the system will be disconnected when the system is restarting.*

5.6 Status

This function provides the system status information and the online user status, such as **System Status**, **Interface Status**, **Current Users**, **Traffic History**, **DHCP Server Reporting**, and **Notify Configuration.**

5.6.1 System Status

You can use this function to get an overview of the system status. Please refer to the following example.

Figure 5-102 System Status Example

System Status		
	Current Firmware Version	1.00.C3
	System Name	bonalinx-W-5101
	Admin info	N/A
	Succeed Page	http://www.cipherium.com.tw
	External Syslog Server	N/A:N/A
	Proxy Server	Enabled
	Internet Connection Detection	Pass
Manage	SSH	10.0.0.0/8
	SNMP	Disabled
History	Retain Days	3 Days
	Email To	
Time	External Time Server	tock.usno.navy.mil
	Date Time(GMT+0:00)	Thu, 22 Apr 2004 15:13:33 +0800
User	Idle Logout Timer	10 Min(s)
	Multiple Login	Disabled
	Guest Account	Disabled
DNS	Preferred DNS Server	168.95.1.1
	Alternate DNS Server	N/A
Friendly	Login	Disabled
	Logout	Disabled

Figure 5-103 System Status Description

Item	Description

Firmware Version		The firmware version currently used by Repeater
System Name		System name, and the default is Repeater
Administrator Info		Administrator's related information will be shown on the login screen when a user has a connection problem.
Succeed Page		The starting web page after a user logs on successfully.
Syslog To		The IP address and port number of the external Syslog Server
Proxy Server		Proxy Server is enabled or disabled.
Internet Connection Detection		When the connection at **WAN** is abnormal (**Internet Connection Detection**), all online users can log on to the network.
Manage	**Remote Manage IP**	It permits a specific IP address to set up the Repeater from the WAN port.
	SNMP	Enable/disable SNMP management function
History	**Retain Days**	The system will retain the user information up to a maximum of 3 days.
	Email To	Send the history to this email address.
Time	**Time Server Name**	The Repeater uses an External Time Server to check time.
	Date Time	The system time is local time.
User	**Logout Timer**	It is the logout time for idling. The online user will be forced to logout after being idled for a duration of this logout time.
	Multiple Login	It does/doesn't allow multiple logins for a user.
	Guest Account	Enable/disable the Guest Account
DNS	**Primary DNS serve**	Primary DNS Server IP Address
	Secondary DNS server	Secondary DNS Server IP Address
Friendly	**Login**	User must click **"Login"** to execute the login procedure. The system will not automatically get the username and password from the previous login for the direct Public LAN login.

	Logout	If a user login, a small window will show the user's information and provide a logout button for the logout. "**Disable**" stands for the case that closing the small windows will not cause a logout to the user.

5.6.2 Interface Status

In this function, you can have an overview on the information of each interface including **WAN port**, **Wireless port**, **Public LAN**, and **Private LAN Port.**

Figure 5-104 Interface Status Example

Interface Status		
WAN	MAC Address	00:02:6F:2E:13:AE
	IP Address	10.2.3.59
	Subnet Mask	255.255.255.0
Wireless	Mode	NAT
	MAC Address	N/A
	IP Address	192.168.3.254
	Subnet Mask	255.255.255.0
	ESSID	W1300-mix
	Channel	4
	Encryption Function	Enabled
Public	Mode	NAT
	MAC Address	00:02:6F:2E:13:AD
	IP Address	192.168.1.254
	Subnet Mask	255.255.255.0
LAN1 DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.1.1
	End IP Address	192.168.1.100
	Lease Time	1440 Min(s)
Private	Mode	NAT
	MAC Address	00:02:6F:2E:13:AD
	IP Address	192.168.2.254
	Subnet Mask	255.255.255.0
LAN2 DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.2.1
	End IP Address	192.168.2.100
	Lease Time	1440 Min(s)

Figure 5-105 Interface Status Example

Item		Description
WAN	**MAC Address**	The MAC address of the WAN port
	IP Address	The IP address of the WAN port
	Subnet Mask	The Subnet Mask of the WAN port
Wireless	**Mode**	Wireless port mode: NAT mode
	MAC Address	The MAC address of the Wireless port
	IP Address	The IP address of theWireless port
	Subnet Mas	The Subnet Mask of the Wireless port
	ESSID	The ESSID of the Wireless port
	Channel	The Channel of Wireless
	Encryption Function	Encryption function of wireless
Public LAN	**Mode**	Public LAN mode: NAT mode
	MAC Address	The MAC address of the Public LAN
	IP Address	The IP address of the Public LAN
	Subnet Mask	The Subnet Mask of the Public LAN
Public DHCP Server	**Status**	Enable/disable the DHCP server on Public LAN
	WINS IP Address	Set the WINS server IP on DHCP server
	Start IP Address	Starting IP Address in DHCP IP range
	End IP address	End IP address in DHCP IP range
	Lease Time	The lease time of IP Address
Private	**Mode**	Private LAN port mode: NAT mode
	MAC Address	The MAC address of the Private LAN port
	IP Address	The IP address of the Private LAN port

	Subnet Mask	The Subnet Mask of the Private LAN port
Private DHCP Server	**Status**	Enable/disable the DHCP function on the Private LAN port
	WINS IP Address	Set the WINS server IP address on the DHCP server
	Start IP Address	Starting IP Address in DHCP IP range
	End IP address	End IP Address in DHCP IP range
	Lease Time	The lease time of the IP address

5.6.3 Current Users

In this function, you can obtain the information of each online user including **Username**, **IP Address**, **MAC Address**, **Packets In**, **Bytes In**, **Packets Out**, **Bytes Out, Idle Time** and **Logout**. Administrator can use this function to force a specific online user to logout. If you want to force a user to logout, you only have to click the hyperlink **Logout** next to the online user's name.

Figure 5-106 Online User Data

Current Users List					
Item	Username	Pkts In	Pkts Out	Idle	Logout
		Bytes In	Bytes Out		

Refresh

5.6.4 Traffic History

You can check the history of Repeater by this function. The history of each day will be saved independently. This system will save the history in the DRAM for more than 3 days.

Figure 5-107 History Example

Traffic History	
Date	Size (Byte)
2004-04-22	65

> ***Caution:*** *Since the history is saved in DRAM, if you need to restart the Repeater and want to keep the history, then please manually duplicate the history.*

If you have entered Administrator's e-mail address in the system configuration interface, then the system will automatically send out the history of the previous day to such e-mail address.

The first line of the history is the title, and the actual history starts from the second line. Each line includes a record, and each record consists of 10 fields **Date**, **Type, Name**, **IP**, **MAC**, **Packets In**, **Bytes In**, **Packets Out,** and **Bytes Out** to show the history of each user.

Figure 5-108 Traffic History Example (2)

Traffic History (2004-04-22)								
Date	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out

5.6.5 DHCP Server Reporting

The system provides the DHCP Server related reports for your reference. You can get the current users leasing the IP by sorting the IP, Age, and Name or search the data by IP, MAC, and Client Name.

Figure 5-109 DHCP Server Reporting Example

General Statistics	GO!
DHCP lease file entries, sorted by IP	GO!
DHCP lease file entries, sorted by Age	GO!
DHCP lease file entries, sorted by Name	GO!

Find the entry for this IP address:		GO!
Find the entry for this MAC address:		GO!
Find the entry for this Client Name:		GO!

5.6.6 Notify Configuration

The Repeater will save the history into the internal DRAM. If you want to automatically send the history to your email address, please enter your e-mail address in the receiver field.

Figure 5-110 Notify Configuration Example

Notify Configuration	
History Email	Sender: Receiver: Interval: 1 Hour
Syslog To	IP: Port:

Sender: The email address of administrator server who is in charge of the history bookkeeper.

Receiver: The email address of a predefined IP user who is being monitored.

Interval: The Interval column shows the interval for sending the history email. If you choose one day, then the history mail will be sent to you once a day.

Syslog To: It specifies the IP and Port of the Syslog server.

6 Technical Support

If you have any other technical questions, please feel free to contact our technical support department: support@cipherium.com.tw

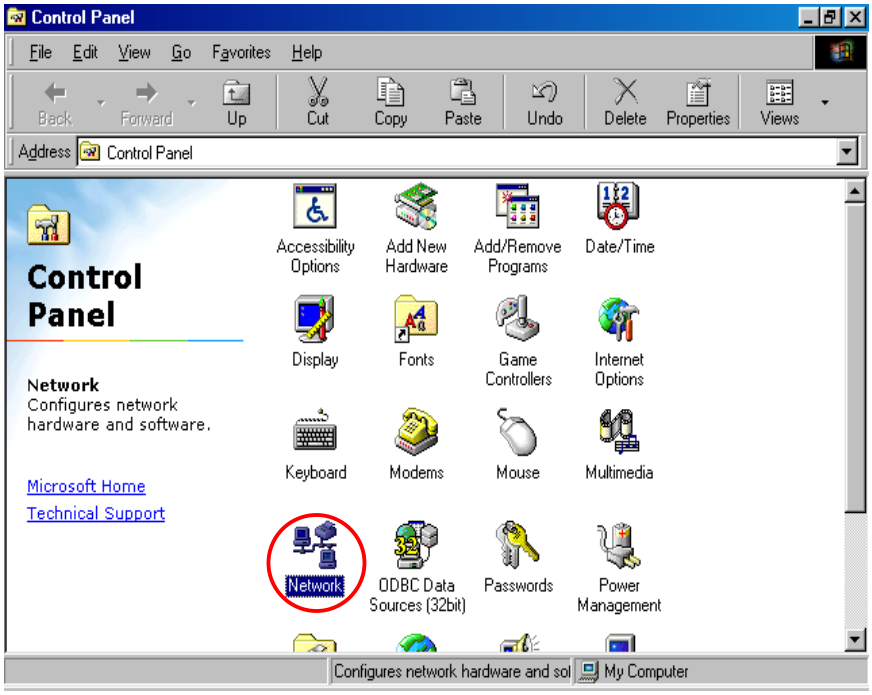
7 Appendix - Windows TCP/IP Setup

If you have not changed the factory default settings of the Repeater and Windows 95/98/ME/2000 TCP/IP, it is not necessary to make any modification here. With the factory default settings, the Repeater will automatically assign an appropriate IP address (and related information) to each PC after the PC has been booted.

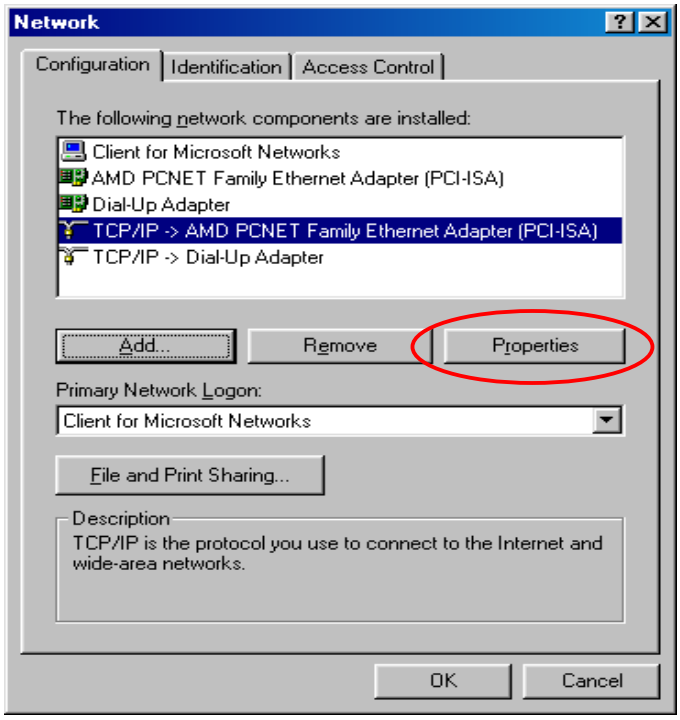
If the version of Windows operating system is not for servers, the default TCP/IP settings will treat the PC as the DHCP client. You can check the TCP/IP setup according to the following procedure:

7.3 Check the TCP/IP Setup of Windows 9x/ME

1. Select **Start -Console –Network.**

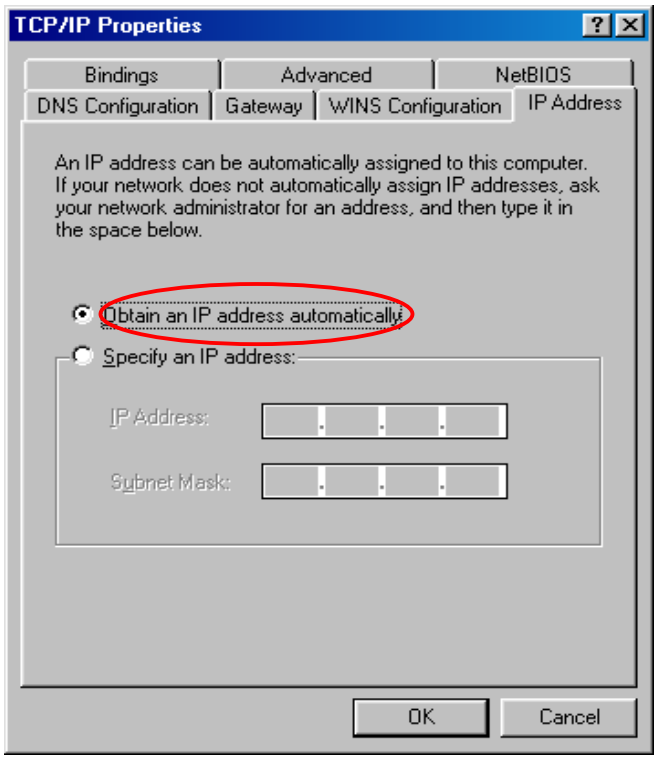


2. Select the TCP/IP communication protocol of the network card, and then click **"Properties"**.



Using DHCP

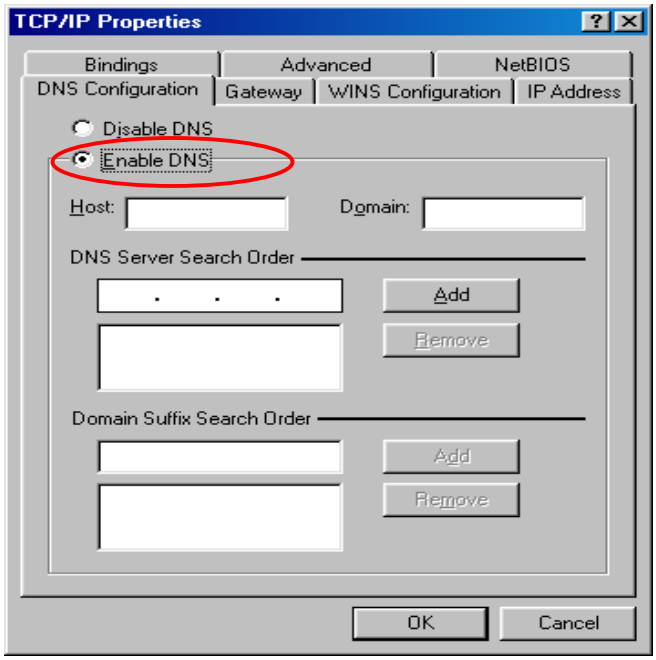
If you want to use DHCP, please select **"Obtain an IP Address Automatically",** which is also the default setting of Windows. Reboot the PC to make sure an IP address is obtained from the Repeater.



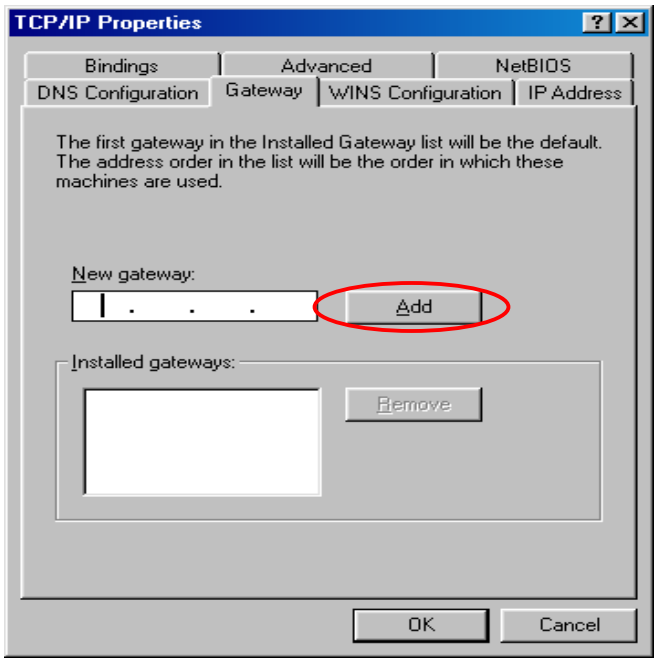
Using Specific IP Address

If you have completed the setup for your PC, please inform the network administrator before modifying the following setup.

1. If the DNS Server column is blank, please click **"Enable DNS"**, and then enter the DNS address or the DNS address provided by ISP. After this procedure is completed, click **"OK"**.

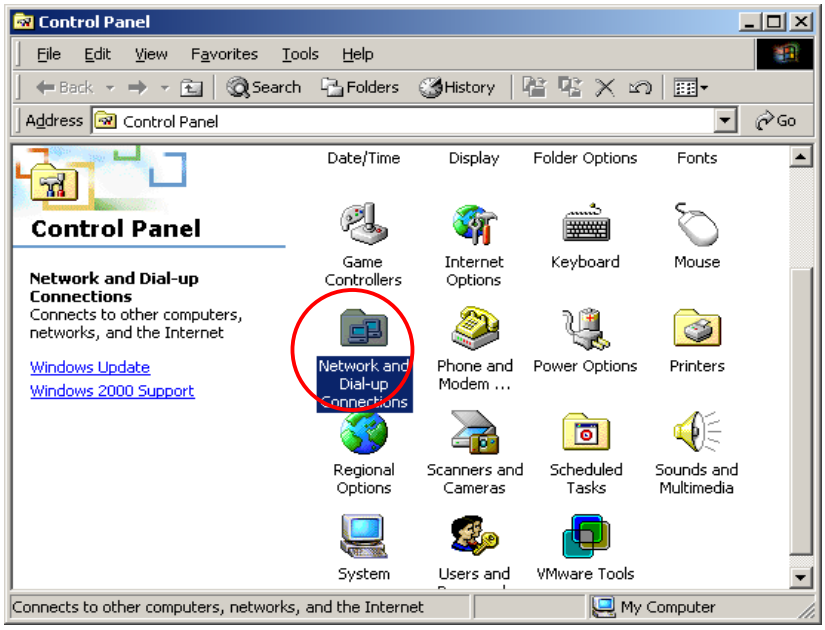


2. Click the **"Gateway"** icon, and enter the IP address of the Repeater in the new gateway. After this procedure is completed, click **"Add"** (You can ask the network administrator for the IP address specified for the Repeater).

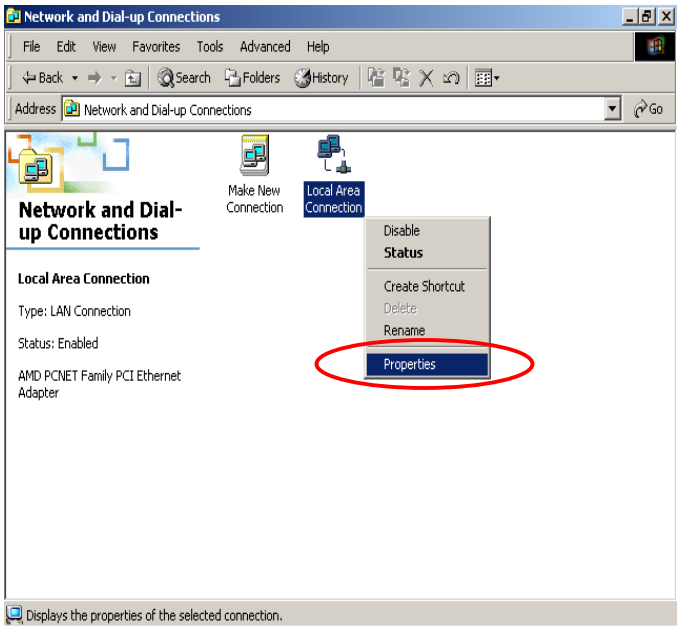


7.4 Check the TCP/IP Setup of Windows 2000

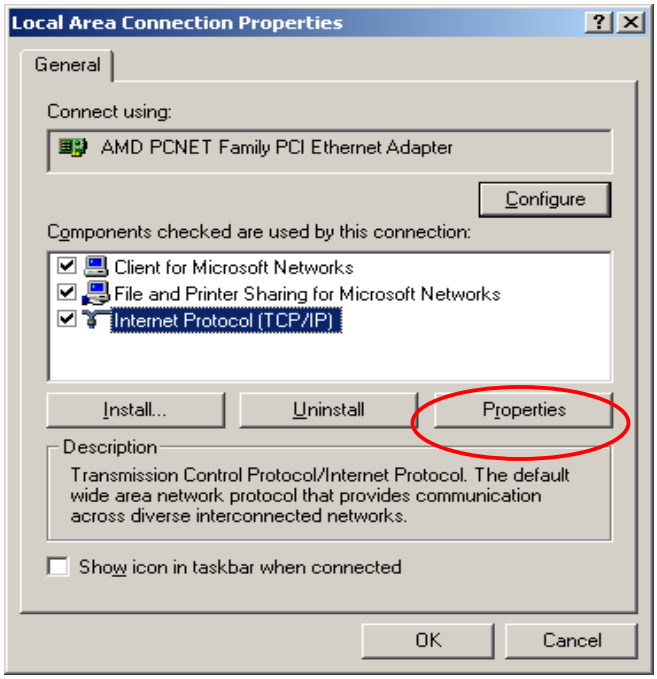
1. Select **Start - Console – Network and Dial-up Connections.**



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

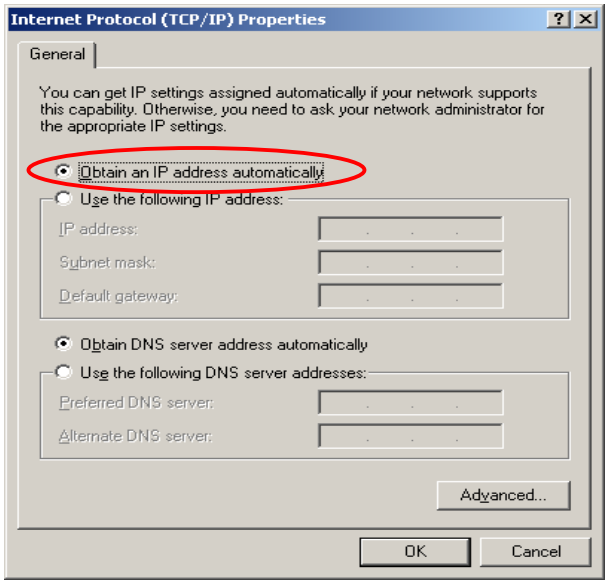


3. Select **Internet Protocol(TCP/IP)**, and then click **"Properties"**.



Using DHCP

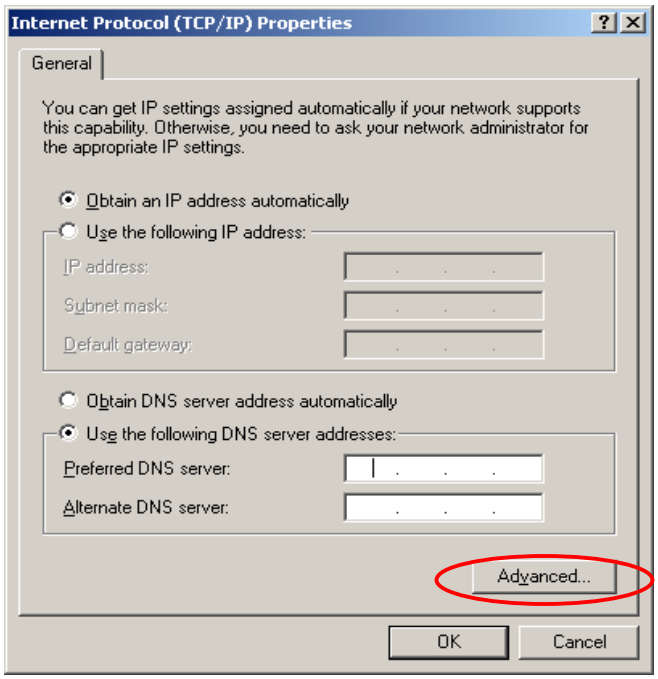
If you want to use DHCP, please select **"Obtain an IP Address Automatically",** which is also the default setting of Windows. Reboot the PC to make sure an IP address is obtained from the Repeater Repeater.



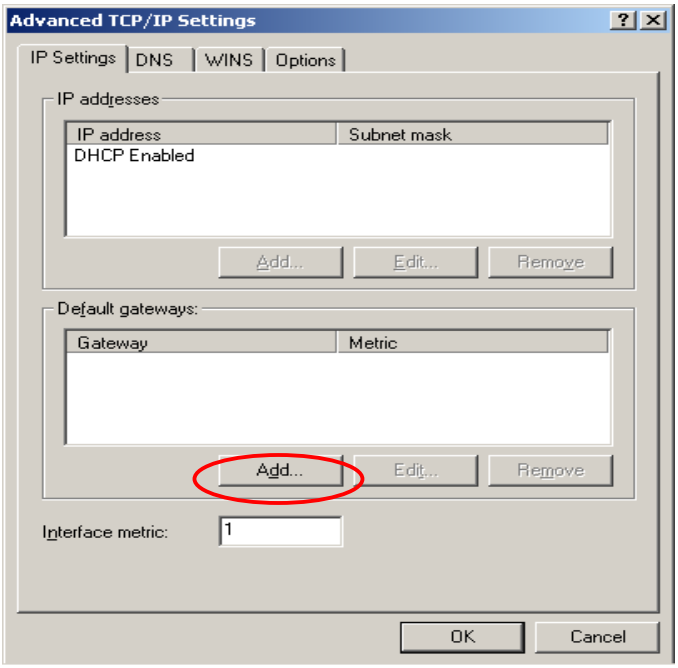
Using Static IP Address

If you have completed the setup for your PC, please inform the network administrator before modifying the following setup.

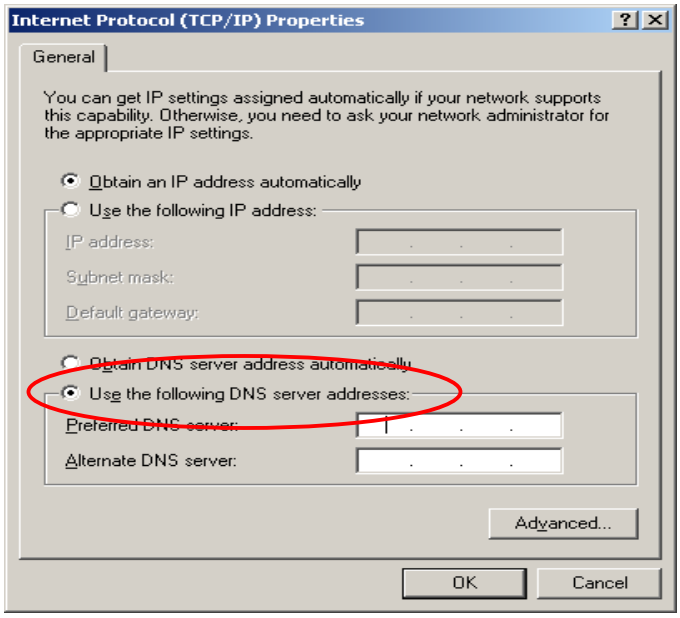
1. Click **"Advanced"** in the window of **Internet Protocol (TCP/IP).**



2. Click the "**IP Settings"** icon, and then **"Add"** in the **"Default Gateways"** column to enter the IP address of the Repeater. After this procedure is completed, click **"Add".** (You can ask the network administrator to give you the IP address specified for the Repeater.)

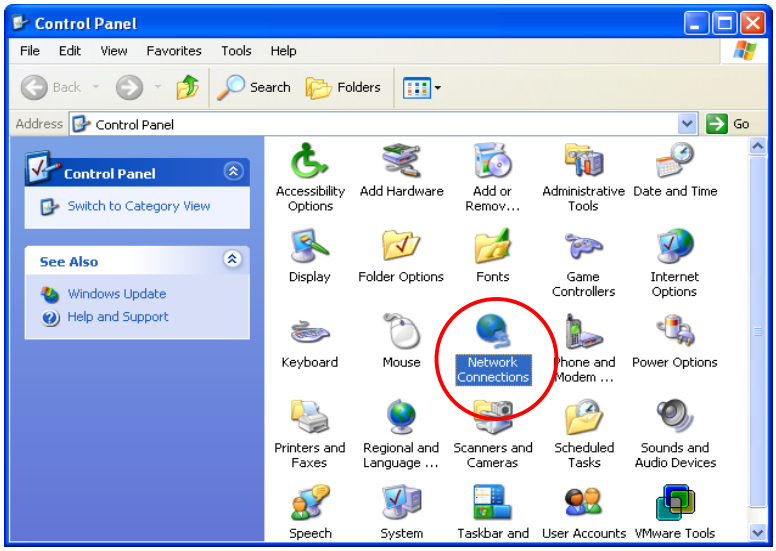


3. If the DNS Server column is blank, please click **"Using the following DNS Server Address"** in the window of Internet Protocol (TCP/IP), and then enter the DNS address or the DNS address provided by ISP. After this procedure is completed, click **"OK"**.

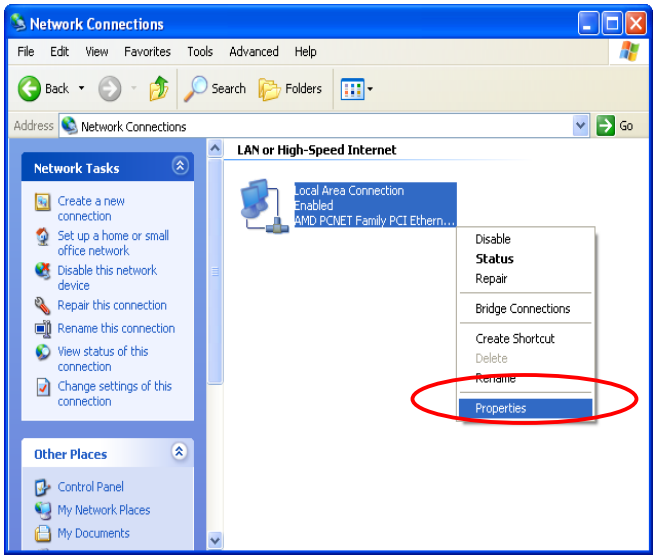


7.5 Check the TCP/IP Setup of Windows XP

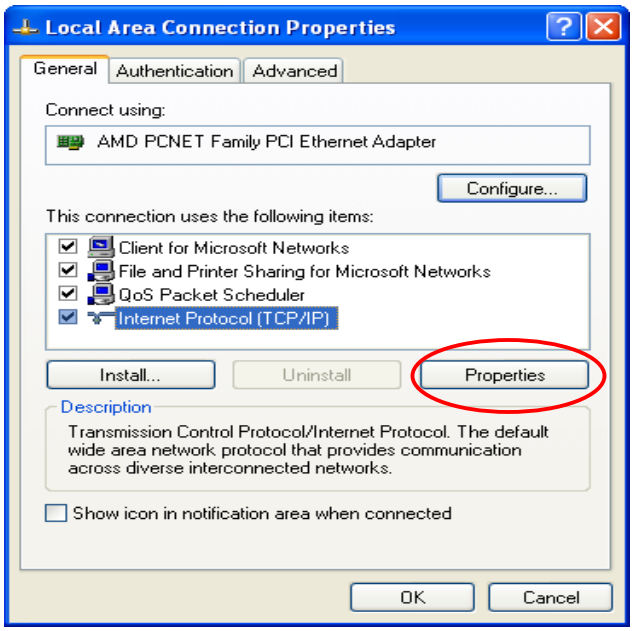
1. Select **Start - Console – Network Connection.**



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

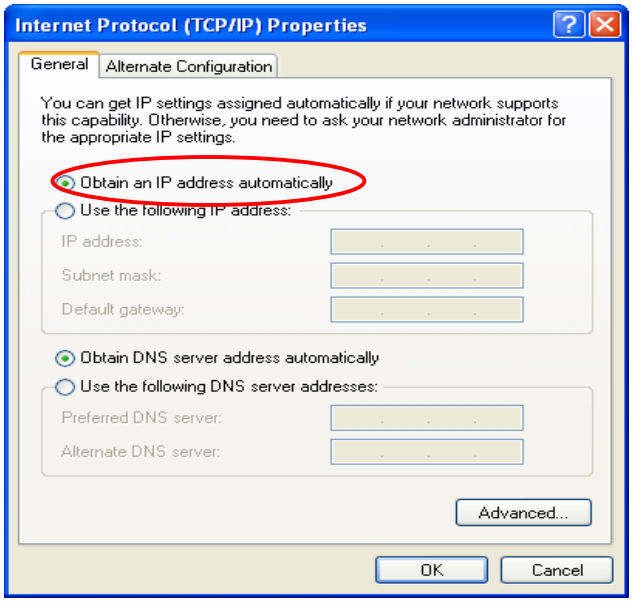


3. Click the **"General"** icon, and then select **"Internet Protocol(TCP/IP)**". Click "**Properties**".



Using DHCP

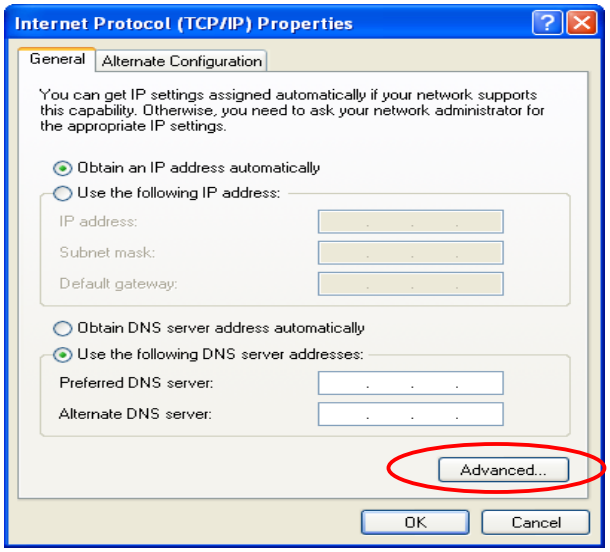
If you want to use DHCP, please select **"Obtain an IP Address Automatically",** which is also the default setting of Windows. Reboot the PC to make sure an IP address is obtained from the Repeater.



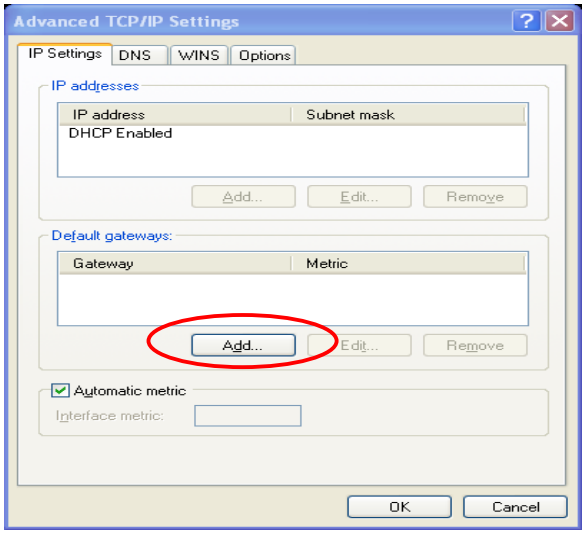
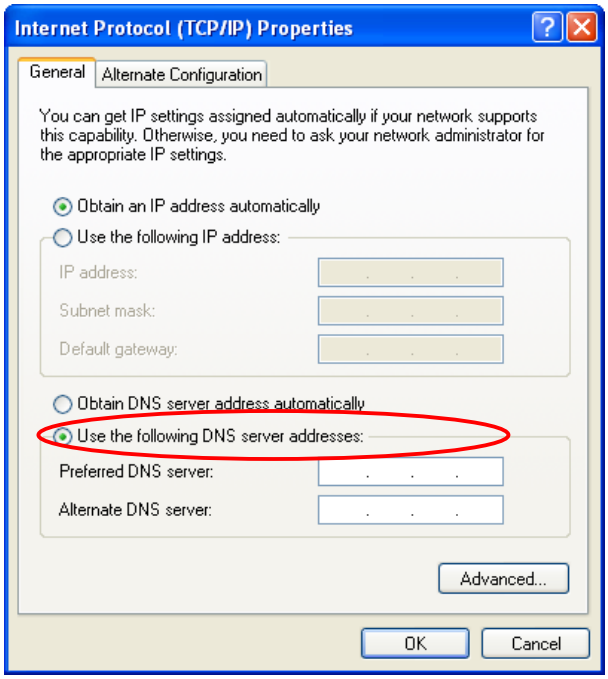
Using Static IP Address

If the setup for your PC is completed, please notice the network administration staff before changing the following settings.

1. Click "Advanced" in the Internet Protocol (TCP/IP) window.



2. Click the "**IP Settings**" icon, and enter the IP address of the Repeater in the **"Default Gateways"** column, and then click **"Add"**. After this procedure is completed, click **"OK"**. (You can ask the network administrator to give you the IP address specified for the Repeater.)



3. If the DNS Server field is blank, please click "**Using the following DNS Server Addresses"** in the Internet Protocol (TCP/IP) Window, and key in the DNS address or DNS address provided by ISP. After this procedure is completed, click **"OK"**