CWR-500

Wireless Router

User Guide

CNet
TOTAL NETWORK SOLUTIONS

CWR500-- Wireless 11b Broadband Router with Four (4) 100/10Mbps Switch ports

The CWR500 is a Wireless Broadband Router with four (4) 100/10Mbps Switch ports and one IEEE802.11b wireless access point. With this cost economics device, an entire network, wire and wireless, can access to the Internet using a single high speed ADSL or Cable modem. A built-in firewall protects networks from outside intruders, while a built-in Access Control lets LAN administrators limit Internet access from individual workstations. Authorized Internet users are able to access to Web, FTP, and other servers on your LAN. The “Exposed Computer” and “Special Internet Application” features allow users to use special-purpose servers, two-way communication devices, and other non-standard Internet applications (such as ICQ, NetMeeting, Game, Quick Time, Real Player, etc.)

KEY FEATURES

- IEEE 802.11 Direct Sequence high rate compatible.
- Provides two external dipole detachable antenna.
- Provides one WAN port for use with a ADSL or Cable modem.
- Provides four 100/10Mbps N-Way switch ports with auto MDI/MDI-X RJ-45 connectors.
- Complete web management using standard internet browser.
- Dynamic Host Configuration Protocol (DHCP) support.
- Internet sharing Static IP, Dynamic IP.
- Protocols TCP/IP, PPPoE, RIP.
- Provides firewall : NAT, Comprehensive logging,
- Provides VPN pass through, PAP/CHAP. (User Authentication)
- Provides user assignable DMZ.
- Maximum Users 253 PCs.
- Platforms supported Win 95/98/ME/NT/2000/XP/Linux.

SPECIFICATIONS(the equipment version marketed in US is restricted to usage of the channels 1-11 only)

Model	CWR500
ChipSets	Realtek RTL8181 / RTL8305 / Philps SA 2400 RF / Gatax W22 PA
RTOS	Linux
Standards	• IEEE 802.3u: 100BASE-TX • IEEE 802.3: 10BASE-T • IEEE 802.11b: Wireless LAN
Protocols	• DHCP, IP, NAT, PPPoE, IEEE 802.11b
Ports	• All ports 100BASE-TX/10BASE-T
Media Support	• 100BASE-TX: Category 5 TP • 10BASE-T: Category 3, 4 or 5 TP
LAN Data Rate	• 148810 packets/second per port @ 100Mbps, maximum • 14880 packets/second per port @ 10Mbps, maximum
AP Data Rate	• 1 / 2 / 5.5 / 11 Mbps per Channel
Modulation TYPE	• CCK,BPSK,QPSK
Channel	• 11 channels (US, Canada) • 13 channels (ETSI) • 14 channels (Japan)
Frequency Range	• 2.4 ~ 2.4835GHz
Flash Memory	• 2M bytes
SDRAM	• 16M bytes
Duplex Modes	• All ports support Half-Duplex and Full-Duplex operation
Auto-MDI/MDIX	• All ports support Auto-MDI/MDIX
LED Indicators	• LED (Green): Status LED (Green): Power LED (Green): WLAN • LED1 (Green): WAN port for 100M • LED2 (Green): WAN port for Link/Activity • LED1 (Green): LAN port for 100M • LED2 (Green): LAN port for Link/Activity
External Power Adapter	• Output 5VDC, 2.5Amp (Input according to country)
Power Consumption	• 10W maximum
Environment	• Operating Temperature: 0° ~ 45°C (32° ~ 113°F) • Storage Temperature: -20° ~ 70°C (-4° ~ 158°F) • Humidity: 10% ~ 90% Non-Condensing
Certifications	• FCC Class B, CE
Dimensions	• 178 x 110 x 30 mm

Mobile of end product

Federal Communication Commission Interference Statement
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 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.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Frequency range:
– 2.4-2.4835 GHz, direct sequence spread spectrum
Number of Channels:
– Europe: 13 (CH01-CH13)
– US: 11 (CH01-CH11)
– France: 4 (CH10-CH13)
– Japan: 14 (CH01-CH14)

CONTENTS

1 Introduction

1.1 Product overview

Congratulations on your purchase of this wireless broadband router, CWR-500. During the design process, we have given much thought to make this device as convenient to use as possible. The end result is the wireless broadband router that can be set up in minutes, allowing network users to access the Internet via either the high-speed ADSL or Cable connection.

1.2 Main benefits

- Cost-effective solution using high-speed ADSL or Cable connection.
- Ideal Solution for the small office or SOHO users.
- Access to the Internet without waiting.
- Have the system up and running in minutes.
- Multiple functions.

1.3 About this manual

The instructions in this manual describe how to connect and configure a Wireless Broadband Router to a network and set up an Internet connection. The manual has been written for network administrators and experienced users and makes a few assumptions about the readers. If you want to install the Wireless Broadband Router on your network you should be familiar with:

- Microsoft Windows 95/98/Me or Windows NT/2000/XP
- Any TCP/IP-enabled systems like Mac OS and UNIX
- TCP/IP and related issues

1.4 Package list

The following items should be included in the Wireless Broadband Router package:

- One (1) Wireless Broadband Router
- DC12V 1.5A Power Adapter
- Manual
- Four (4) Rubber Feet (for desktop placement)

2 Hardware Installation

2.1 Overview

This chapter details the step-by-step procedure needed to properly install the Wireless Broadband Router hardware. Topics discussed in this chapter include connecting and disconnecting the Wireless Broadband Router to and from the modem, the network, and the power unit.

2.2 Preparation

The following items are needed for installation of the Wireless Broadband Router unit:

- The Wireless Broadband Router unit.
- One power adapter.
- UTP cable. (Cat.5 Twisted-pair)
- One ADSL/Cable modem with RJ-45 LAN interface.

2.2.1 Connecting wireless broadband router to the ADSL/Cable modem (WAN)

1. Ensure the modem's power is switched off.
2. Connect one end of the UTP cable to the Wireless Broadband Router's WAN connector at the rear panel of the device.
3. Connect the other end of the UTP cable to the modem's UTP (RJ-45) port.
4. The connection is now completed.

2.2.2 Connecting wireless broadband router to the network (LAN)

1. Connect one end of the UTP cable to the Wireless Broadband Router.
2. Connect the other end of the UTP cable to any network computer.
3. The connection is now completed.

2.2.3 Connecting the power adapter

1. Connect the power adapter to the Wireless Broadband Router's Power adapter jack.
2. Plug the Power adapter into a power outlet.
3. Turn the modem's power on.
4. The connection is now completed.

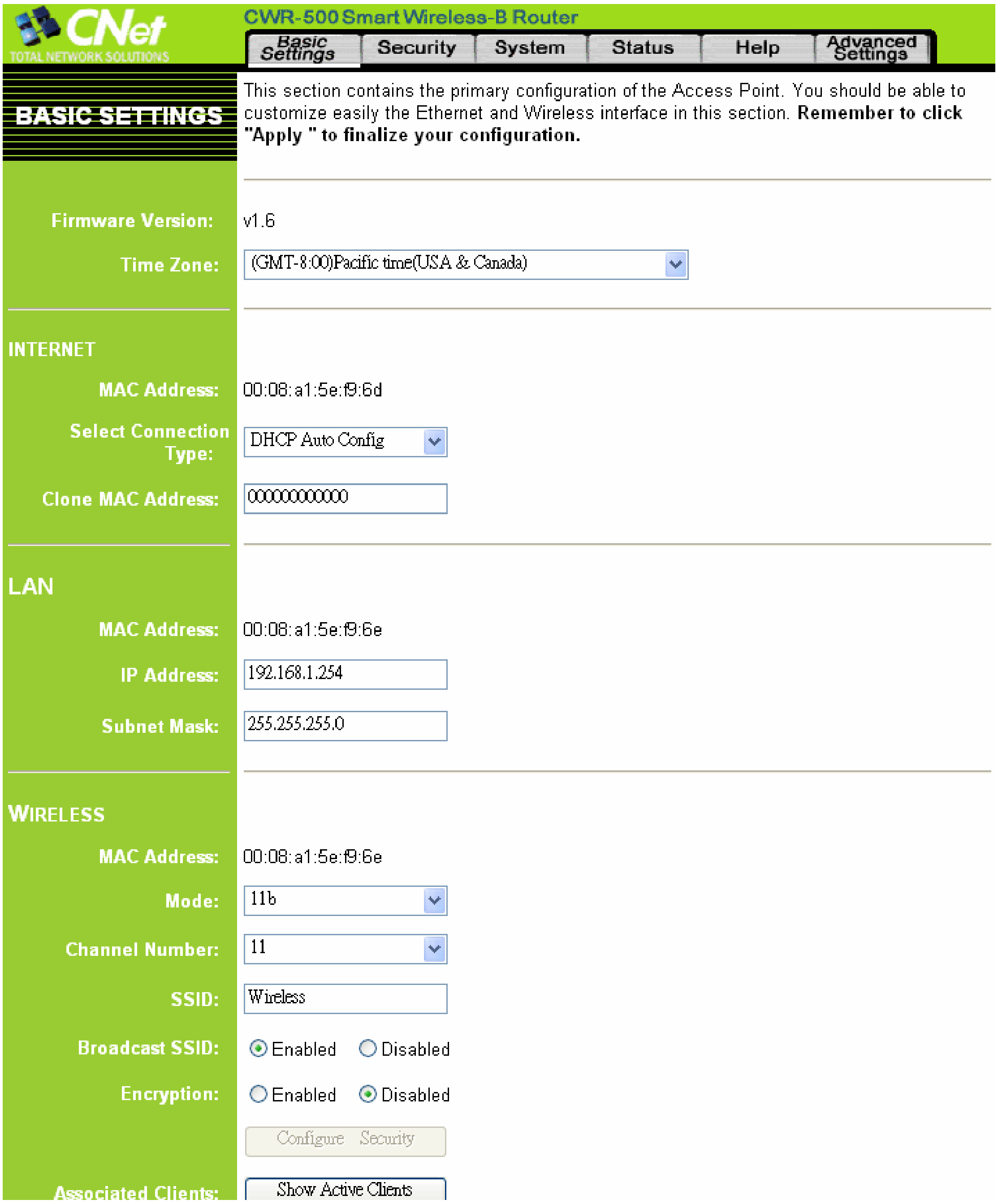
2.3 Resetting the wireless broadband router

The Wireless Broadband Router has a reset button on the front panel of the device. In some circumstances, you might need to reset the Wireless Broadband Router. Please follow the directions listed below to reset the Wireless Broadband Router.

1. Press the reset button and hold while the Wireless Broadband Router is powered on. Wait for 6 seconds, then release button.
2. Reset the ADSL/Cable modem.

3 Primary Setup

This page is used to configure the parameters for Internet, LAN and Wireless setup.



BASIC SETTINGS

This section contains the primary configuration of the Access Point. You should be able to customize easily the Ethernet and Wireless interface in this section. **Remember to click "Apply " to finalize your configuration.**

Firmware Version: v1.6

Time Zone: (GMT-8:00)Pacific time(USA & Canada)

INTERNET

MAC Address: 00:08:a1:5e:f9:6d

Select Connection Type: DHCP Auto Config

Clone MAC Address: 000000000000

LAN

MAC Address: 00:08:a1:5e:f9:6e

IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

WIRELESS

MAC Address: 00:08:a1:5e:f9:6e

Mode: 11b

Channel Number: 11

SSID: Wireless

Broadcast SSID: ● Enabled ○ Disabled

Encryption: ○ Enabled ● Disabled

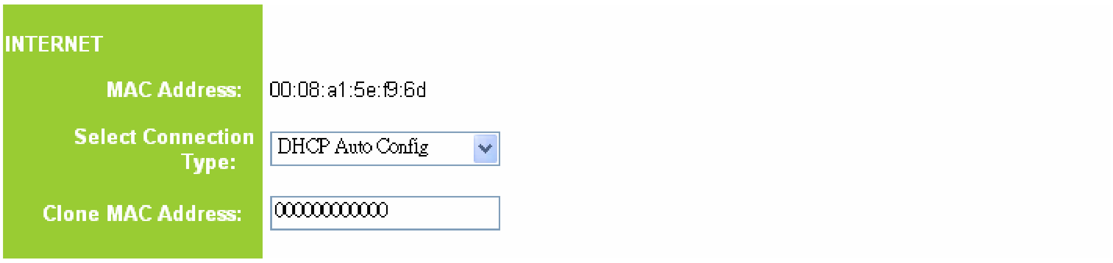
Configure Security

Associated Clients: Show Active Clients

3.1 Internet setup

The user can configure the connection type (DHCP, fixed IP or PPPoE) and parameters for Internet network which connects to the WAN port of your Access Point. Refer to the ISP (Internet Service Provider) and select the appropriate option and fill in the information needed to connect. Here you may change the setting for IP address, PPPoE, DNS, etc…

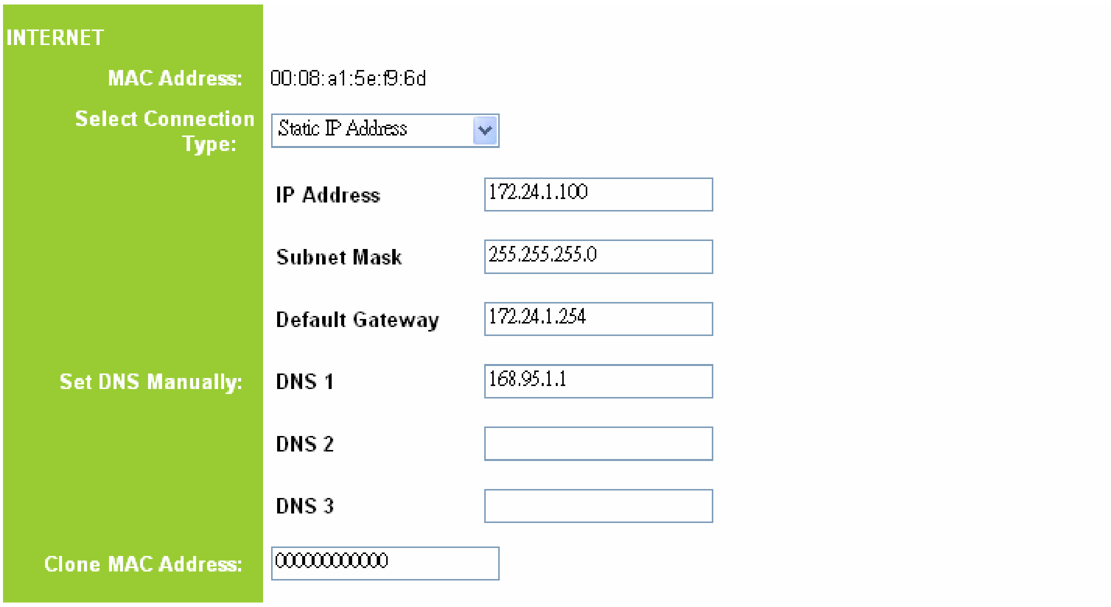
DHCP: If the user set the device as DHCP client, the device will get automatically IP address from the DHCP server.



INTERNET

MAC Address:	00:08:a1:5e:f9:6d
Select Connection Type:	DHCP Auto Config
Clone MAC Address:	000000000000

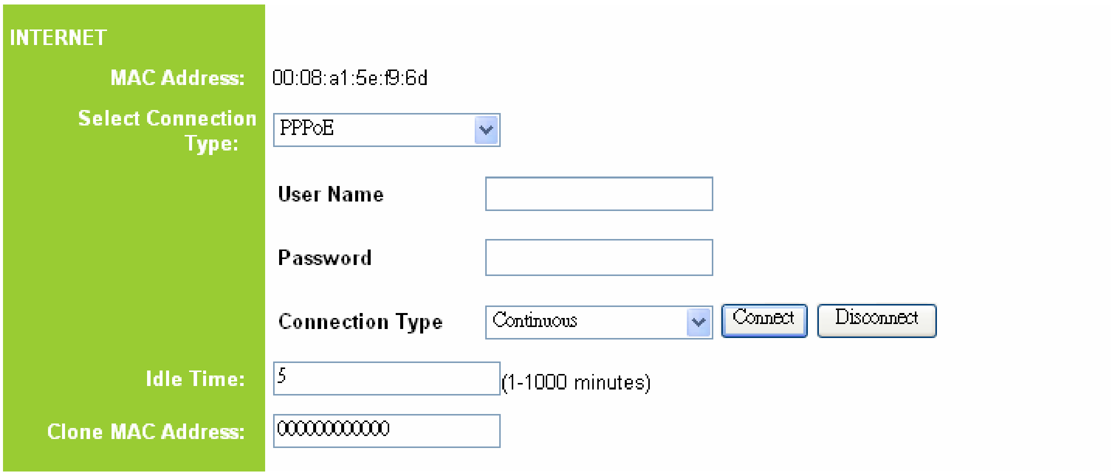
Fixed IP: The user can specify an IP address.



INTERNET

MAC Address:	00:08:a1:5e:f9:6d	
Select Connection Type:	Static IP Address	
	IP Address	172.24.1.100
	Subnet Mask	255.255.255.0
	Default Gateway	172.24.1.254
Set DNS Manually:	DNS 1	168.95.1.1
	DNS 2	
	DNS 3	
Clone MAC Address:	000000000000	

PPPoE: Enter the username and password you use when logging onto your ISP through a PPPoE connection.


INTERNET

MAC Address: 00:08:a1:5e:f9:6d

Select Connection Type: PPPoE

User Name

Password

Connection Type: Continuous

Idle Time: 5 (1-1000 minutes)

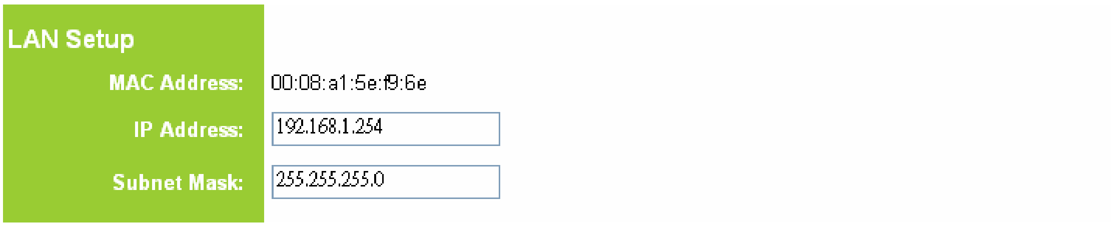
Clone MAC Address: 000000000000

MAC address: It shows the MAC address of the WAN interface.

Clone MAC Address: Clone MAC address allows the user to copy the previous MAC address and using it on your new network.

3.2 LAN interface setup

The user can configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP,etc..


LAN Setup

MAC Address: 00:08:a1:5e:f9:6e

IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

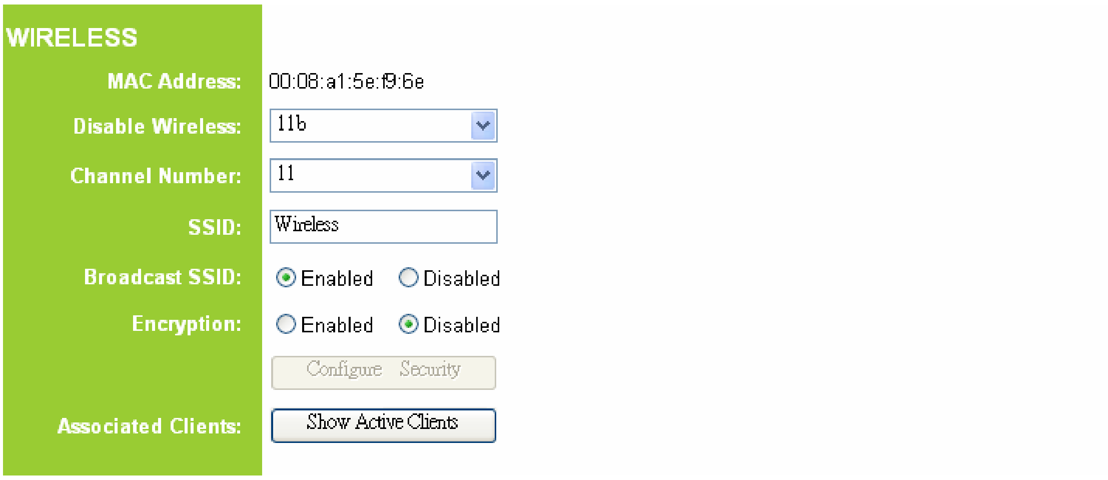
MAC address: It shows the MAC address of the LAN interface.

IP address: The IP address of the LAN interface. The default IP address is 192.168.1.1.

Subnet Mask: The subnet mask of the LAN interface. The default subnet mask is 255.255.255.0.

3.3 Wireless interface setup

The user can configure the parameters for wireless network which connects to the wireless LAN port of your Access Point. Here you may change the settings for alias name, SSID, channel number, etc...



WIRELESS

MAC Address: 00:08:a1:5e:f9:6e

Disable Wireless: 11b

Channel Number: 11

SSID: Wireless

Broadcast SSID: ● Enabled ○ Disabled

Encryption: ○ Enabled ● Disabled

Associated Clients:

MAC address: It shows the MAC address of the WLAN interface.
Disable Wireless: The user can disable the wireless function.
Channel: Select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must use the same channel in order to function correctly.
SSID: The SSID is the network name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all devices in your wireless network.
Broadcast SSID: A zero byte length SSID is called the broadcast SSID, an access point can respond to computers sending probe packets with the broadcast SSID. If this feature is enabled on the access point, any wireless user can associate with the access point by using a blank (null) SSID.
Associated Clients: Click "Show Active Clients", the table shows the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client.
Mode: Enable encryption allows you to setup WEP key value.
Key Length: There are 2 levels of encryption to use, the user can select 64-bit or 128-bit.

Key Format: ASCII or HEX.

ASCII. (American Standard Code for Information Interchange)**:** Consists of 256 numbers assigned to the alphabet, numbers, punctuation, control character and etc.

hexadecimal notation**:** While the more common decimal system uses a base of ten to represent all possible numbers, hexadecimal notation uses a base of sixteen: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, A, B, C, D, E, F. While such a system may seem confusing at first, it works extremely well in computing environments. For example, a single byte of information can be represented as eight bits (10011101), decimal numerals (913), or simplified to hex (9D). In hex, every byte can be shown as two hexadecimal characters.

Default Tx Key: Select the key number to use.

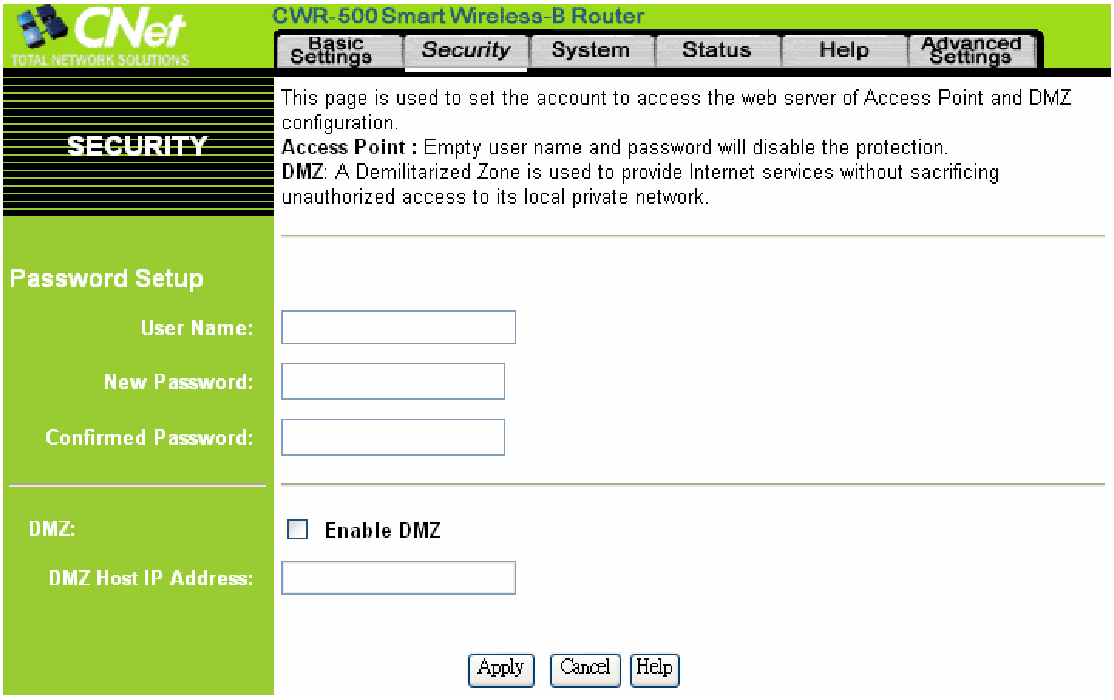
Encryption Key Number: Each key must consist of ASCII or HEX digits.

To save all the settings, click “Apply Changes”. After the device save all the settings, it will show as following, then click “OK” to finish the saving.

Change setting successfully!

4 Security

This page is used to set the account to access the web server of Access Point and WEP security.



This page is used to set the account to access the web server of Access Point and DMZ configuration.
Access Point : Empty user name and password will disable the protection.
DMZ: A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network.

Password Setup

User Name:

New Password:

Confirmed Password:

DMZ: □ Enable DMZ

DMZ Host IP Address:

4.1 Password setup

It is used to set the account to access the web server of your device. Empty user name and password will disable the protection.

4.2 DMZ setup

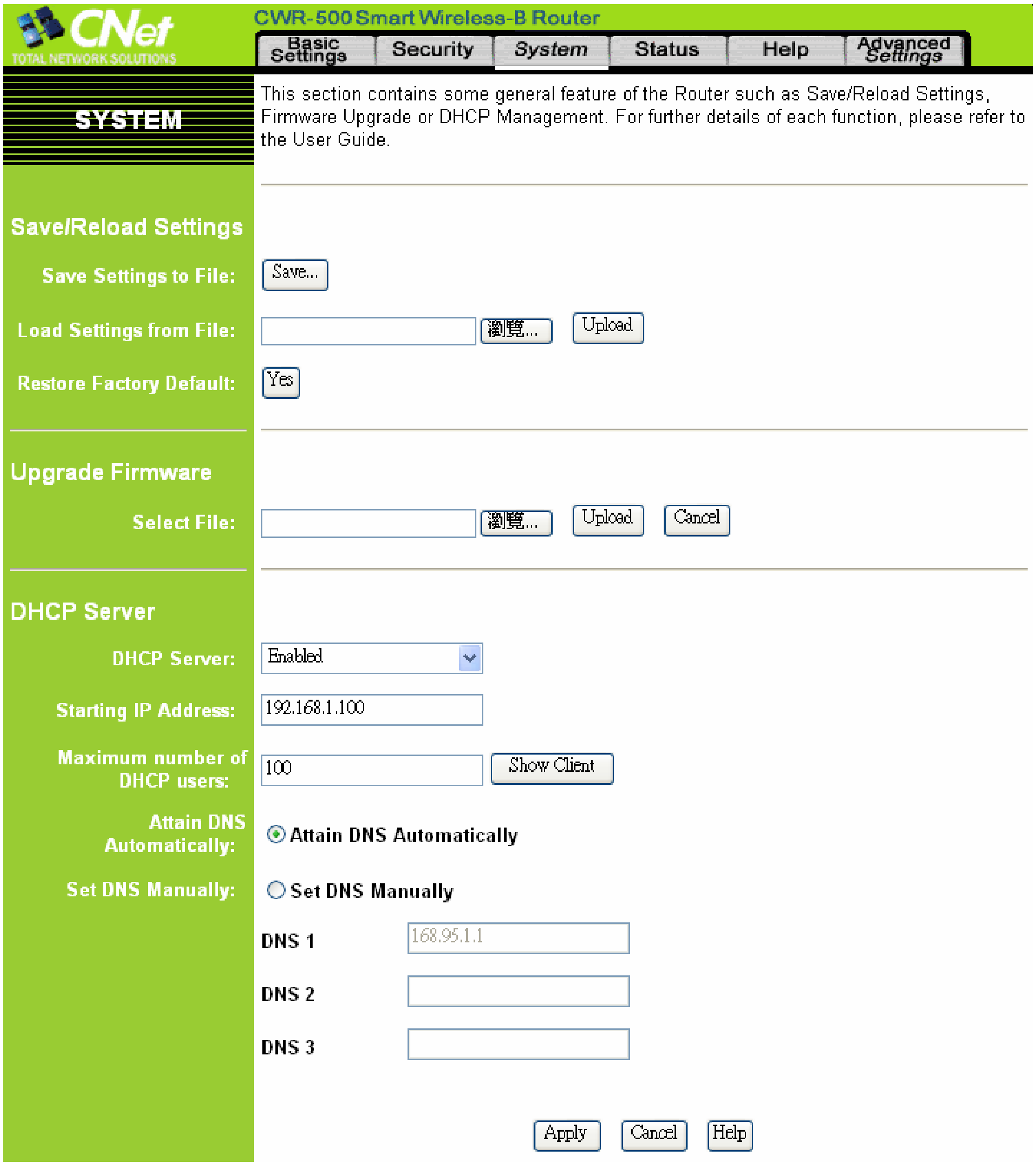
A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.
If the user wants to use the DMZ function, check “Enable DMZ”.
DMZ Host IP Address: Enter the DMZ host IP, note that the IP address must be in the same subnet of your local computer IP address.

To save all the settings, click “Apply Changes”. After the device save all the settings, it will show as following, then click “OK” to finish the saving.

Change setting successfully!

5 System

This page allows you to save current settings to a file or reload the settings from the file which was saved previously. You also could reset the current configuration to factory default or upgrade the Access Point firmware to new version. Please note, do not power off the device during the uploading because it may crash the system. Besides, you could setup DHCP server in this router.



This section contains some general feature of the Router such as Save/Reload Settings, Firmware Upgrade or DHCP Management. For further details of each function, please refer to the User Guide.

Save/Reload Settings

Save Settings to File:

Load Settings from File:

Restore Factory Default:

Upgrade Firmware

Select File:

DHCP Server

DHCP Server: Enabled

Starting IP Address: 192.168.1.100

Maximum number of DHCP users: 100

Attain DNS Automatically: ● Attain DNS Automatically

Set DNS Manually: ○ Set DNS Manually

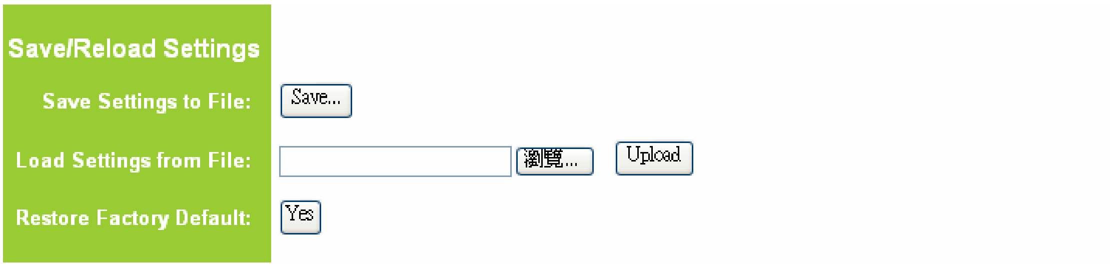
DNS 1: 168.95.1.1

DNS 2:

DNS 3:

5.1 Save/reload settings

It allows the user to save current settings to a file or reload the settings from the file which was saved previously. Besides, the user could reset the current configuration to factory default.



Save/Reload Settings

Save Settings to File: Save...

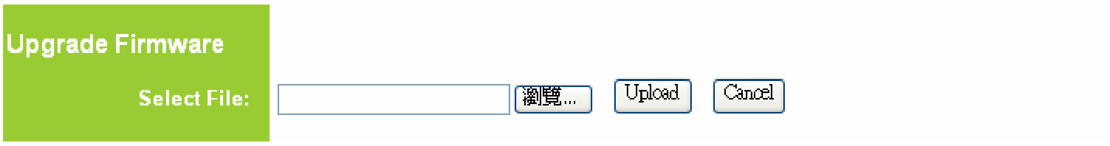
Load Settings from File: 瀏覽... Upload

Restore Factory Default: Yes

Save Settings to File: The user can save the current settings.
Load Settings from File: The user can reload the settings from the file which was saved previously. After browsing to the file, click "Upload", and the settings will be reloaded.
Reset Settings to Default: the user could reset the current configuration to factory default.

5.2 Upgrade firmware

It allows the user to upgrade the device firmware to new version. Make sure that the firmware the user wants to upgrade is on the local hard drive. After browsing to the file, click "Upload", and the firmware will be upgraded. Please note, do not power off the device during the upload because it may crash the system.
After the firmware is uploaded, it will show as following, then click "OK" to finish the upload.

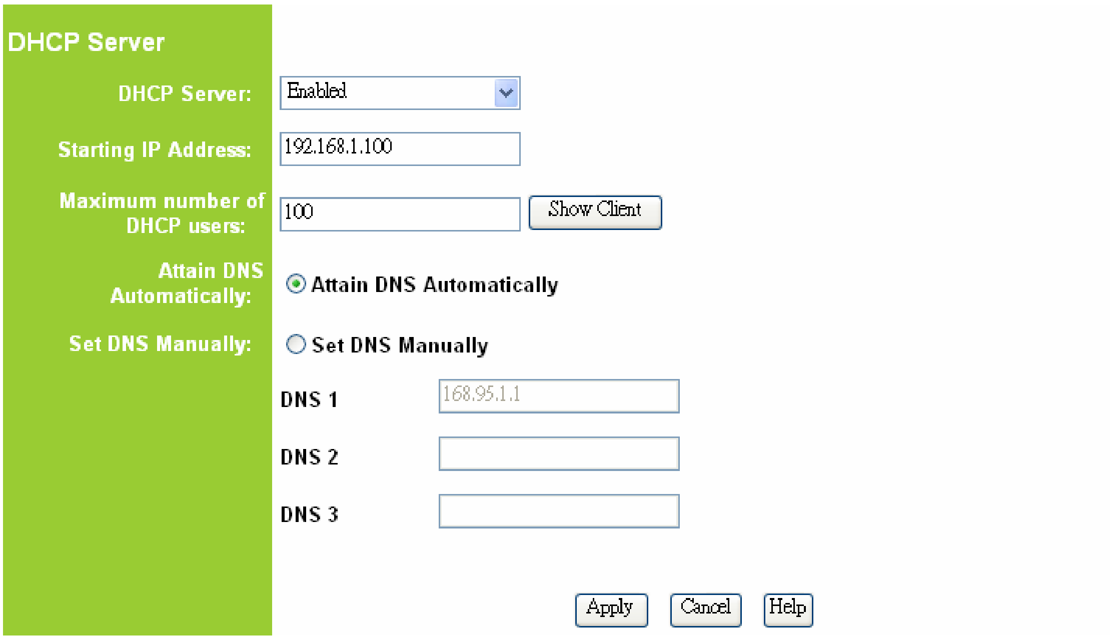


Upgrade Firmware

Select File: 瀏覽... Upload Cancel

5.3 DHCP server

The router has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the router. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. The user can select "Enable" or "Disable" the DHCP server.



DHCP Server

DHCP Server: Enabled

Starting IP Address: 192.168.1.100

Maximum number of DHCP users: 100

Attain DNS Automatically: ● Attain DNS Automatically

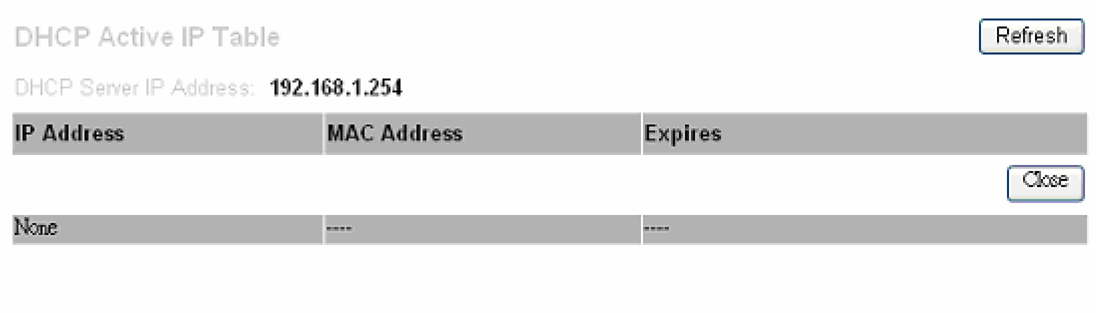
Set DNS Manually: ○ Set DNS Manually

DNS 1 168.95.1.1

DNS 2

DNS 3

DHCP Server: The user can select "Enable" or "Disable" the DHCP server.
Starting IP Address: The user can specify the starting IP address used to allocate to the requesting computer.
Maximum number of DHCP Servers: The user can specify the IP range used to allocate to the requesting computer.
Click "Show Clients" to see the assigned IP address, MAC addresses, and time expired for each DHCP leased client.



DHCP Active IP Table

DHCP Server IP Address: 192.168.1.254

IP Address	MAC Address	Expires
None	----	----

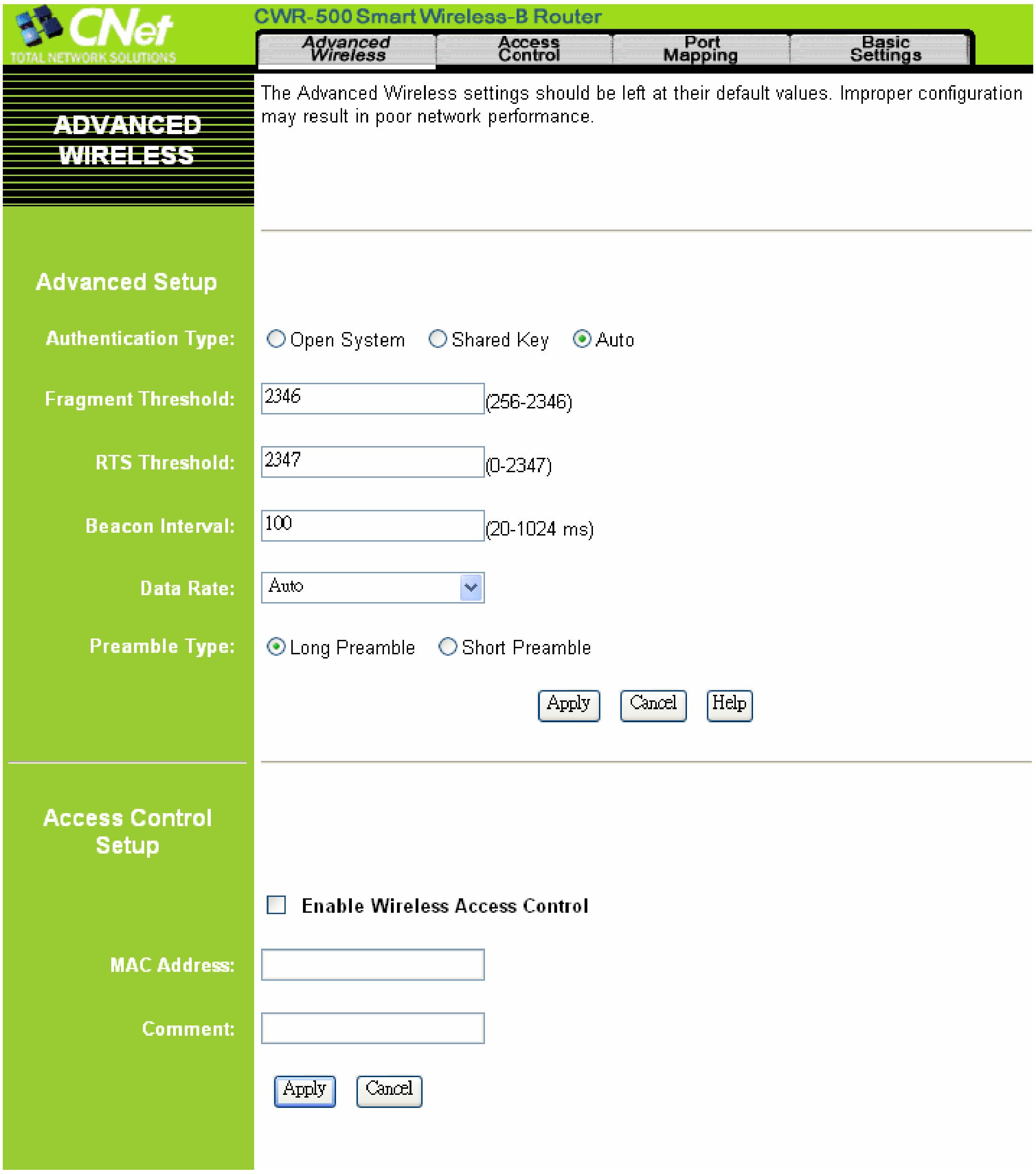
DNS: The DNS (Domain Name System) IP Addresses currently used by the Router are shown here. Multiple DNS IP settings are common. In most cases, the first available DNS entry is used.

To save all the settings, click “Apply Changes”. After the device save all the settings, it will show as following, then click “OK” to finish the saving.

Change setting successfully!

6 Advanced Wireless

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point and these settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. Here you may change wireless encryption settings as well as wireless network parameters. If you enable wireless access control, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When this option is enabled, no wireless clients will be able to connect if the list contains no entries.



The Advanced Wireless settings should be left at their default values. Improper configuration may result in poor network performance.

Advanced Setup

Authentication Type: ○ Open System ○ Shared Key ● Auto

Fragment Threshold: 2346 (256-2346)

RTS Threshold: 2347 (0-2347)

Beacon Interval: 100 (20-1024 ms)

Data Rate: Auto

Preamble Type: ● Long Preamble ○ Short Preamble

Access Control Setup

□ Enable Wireless Access Control

MAC Address:

Comment:

6.1 Advanced setup

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your device.

Authentication Type: Open system or share key.

> **Open system**: The default authentication service that simply announces the desire to associate with another station or access point. A station can authenticate with any other station or access point using open system authentication if the receiving station designates open system authentication.
>
> **Share key**: The optional authentication that involves a more rigorous exchange of frames, ensuring that the requesting station is authentic. For a station to use shared key authentication, it must implement WEP.

Fragment Threshold: Fragment threshold defines a threshold above, which the wireless packet will be split up, or fragmented. For a fragmented packet, if transmission of part of it were to be interfered with, only the portion that was successfully transmitted would need to be resent. Throughput will generally be lower for fragmented packets, since the fixed packet overhead consumes a higher portion of the RF bandwidth.

RTS Threshold: The RTS threshold sets an upper threshold at which point the device will issue an RTS packet. The RTS (Request to Send) packet is used for the purpose of avoiding data collisions on the wireless LAN. There are several trade offs to consider when setting this parameter. Setting this parameter to a small value causes RTS packets to be sent more often, consuming more of the available bandwidth, therefore reducing the apparent throughput of other network packets. However, the more often RTS packets are sent, the quicker the system can recover from interference or collisions. Refer to the IEEE 802.11 standard for more information on the RTS/CTS mechanism.

Beacon Interval: This represents the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).

Data Rate: The actual rate at which data transmission occurs varies according to the strength of signal transmitting the data. Distance and environment can affect the strength of the signal that can be transmitted and received. The signal strength determines the type of modulation technique used to encode data, which affects the volume of data (i.e. the number of bits) that can be encoded in a given space of the carrier signal. The IEEE 802.11b standard specifies that WLAN devices adapt the rate of transmission to use the best rate achievable. Each wireless device first determines if conditions diminish signal strength and then chooses one of four possible bit rates (1, 2, 5.5, or 11 Mbps) based on this learned information.

By default, the unit adaptively selects the highest possible rate for transmission. Select the basic rates to be used among the following options: Auto, 1, 2, 5.5, or 11 Mbps. For most networks the default setting, Auto will be the best choice. When (Auto Rate Fall Back) is enabled the transmission rate will select the optimum rate. If obstacles or interference are present, the system will automatically fall back to a lower rate.

Preamble Type: Preamble is the first sub-field of PPDU, which is the appropriate frame format for transmission to PHY (Physical layer). There are two options, Short Preamble and Long Preamble. The Short Preamble option improves throughput performance. The Preamble type of Node should be the same as AP's when in Access Point Client mode.

6.2 Access control

If the user enables wireless access control, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your device. When this option is enabled, no wireless clients will be able to connect if the list contains no entries.

To save all the settings, click "Apply Changes". After the device save all the settings, it will show as following, then click "OK" to finish the saving.

Change setting successfully!

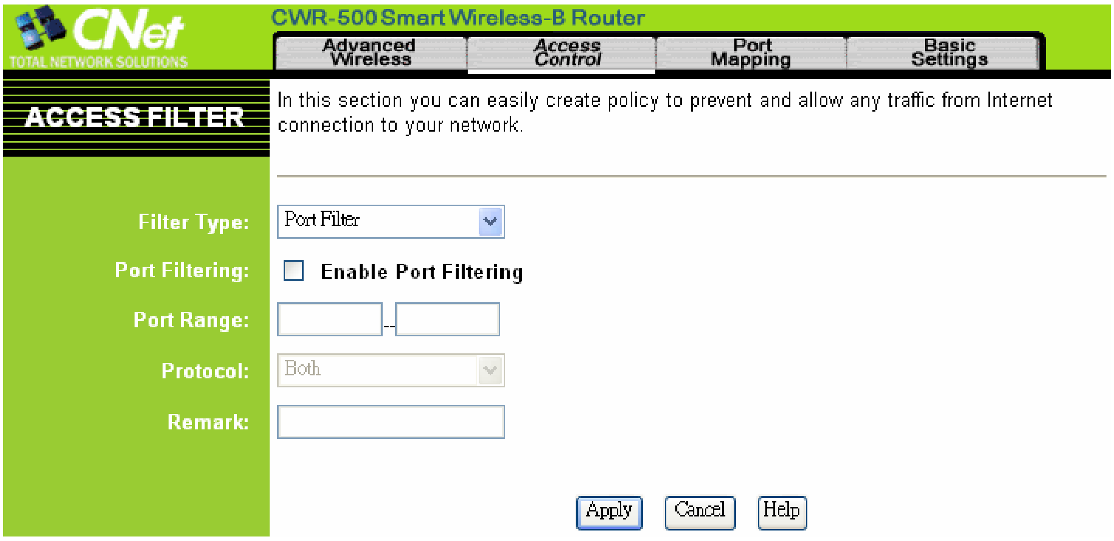
Only those MAC addresses which match to the control list can associate with the router. If the user wants to deny one of the MAC address listed in the list, check "Selected" and click "Delete Selected" or click "Delete All" to deny all clients.

7 Access Filters

This page is used to restrict certain types of data packets from your local network to Internet through the device. Use of such filters can be helpful in securing or restricting your local network.

7.1 Port filter

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the device. Use of such filters can be helpful in securing or restricting your local network.
If the user wants to filter some types of data packets or block local network users from accessing restricted web sites, check “Enable Port Filtering”



In this section you can easily create policy to prevent and allow any traffic from Internet connection to your network.

Filter Type: Port Filter

Port Filtering: □ Enable Port Filtering

Port Range: --

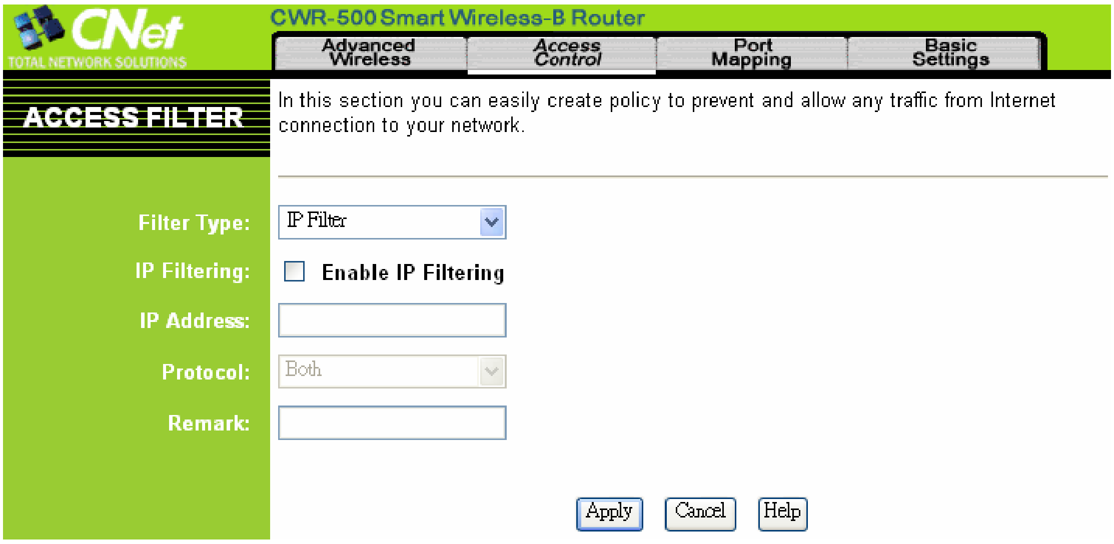
Protocol: Both

Remark:

Port Range: Enter the port range to restrict.
Protocol: TCP, UDP or both.
Comment: Explanatory notes.
To save all the settings, click “Apply Changes”, the port range, protocol and comment will be listed in the “Current Filter Table”.
If the user doesn’t want to filter the ports listed in the list, check “Selected” and click “Delete Selected” or click “Delete All” to delete all filtered ports.

7.2 IP filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the device. Use of such filters can be helpful in securing or restricting your local network.



In this section you can easily create policy to prevent and allow any traffic from Internet connection to your network.

Filter Type: IP Filter

IP Filtering: □ Enable IP Filtering

IP Address:

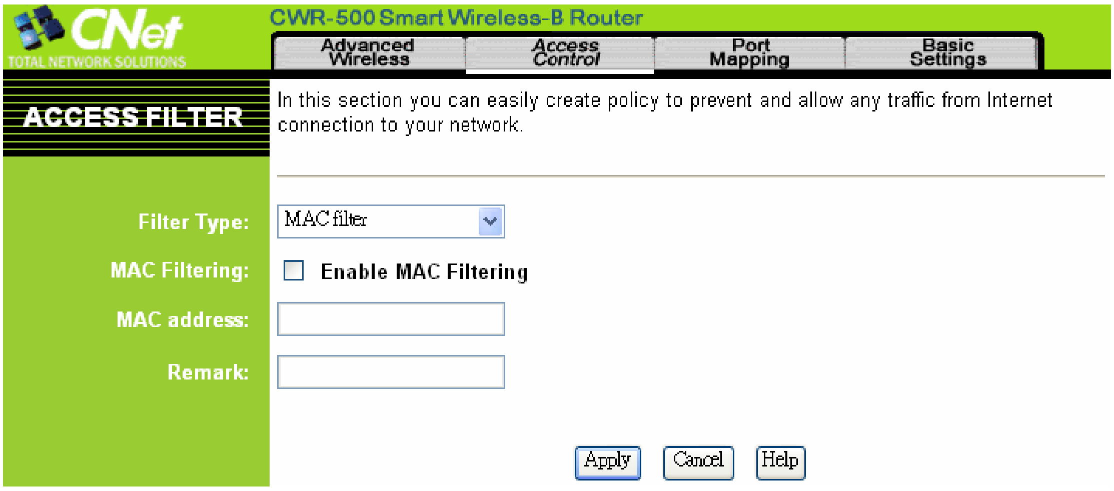
Protocol: Both

Remark:

Local IP Address: Enter the IP address the user wants to filter.
Protocol: TCP, UDP or both.
Comment: Explanatory notes.
To save all the settings, click “Apply Changes”, the IP address, protocol and comment will be listed in the “Current Filter Table”.
If the user doesn’t want to filter the IP addresses listed in the list, check “Selected” and click “Delete Selected” or click “Delete All” to delete all filtered IP addresses.

7.3 MAC filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the device. Use of such filters can be helpful in securing or restricting your local network.



In this section you can easily create policy to prevent and allow any traffic from Internet connection to your network.

Filter Type: MAC filter

MAC Filtering: □ Enable MAC Filtering

MAC address:

Remark:

MAC Address: Enter the MAC address the user wants to filter.

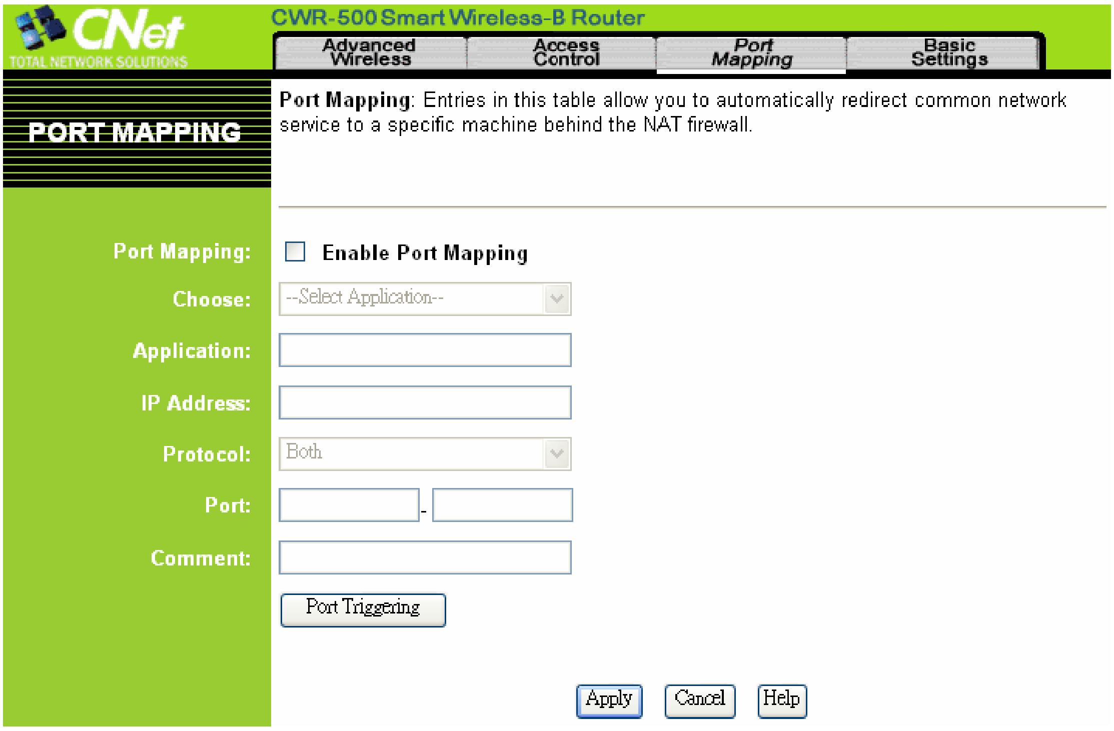
Comment: Explanatory notes.

To save all the settings, click “Apply Changes”, the MAC address and comment will be listed in the “Current Filter Table”.

If the user doesn’t want to filter the MAC addresses listed in the list, check “Selected” and click “Delete Selected” or click “Delete All” to delete all filtered MAC addresses.

8 Port Mapping

Entries in this table allow you to automatically redirect common network service to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on a private local network behind your Gateway's NAT firewall.



Port Mapping: Entries in this table allow you to automatically redirect common network service to a specific machine behind the NAT firewall.

Port Mapping: □ Enable Port Mapping

Choose: --Select Application--

Application:

IP Address:

Protocol: Both

Port: -

Comment:

8.2 Port forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your NAT firewall.

Choose: Select the application the user wants to use.

Application: The selected application will be shown in this table.

IP Address: Enter the IP address that the user wants to forward. Note that the address must be in the same domain of your local computer IP address.

Protocol: TCP, UDP or both.

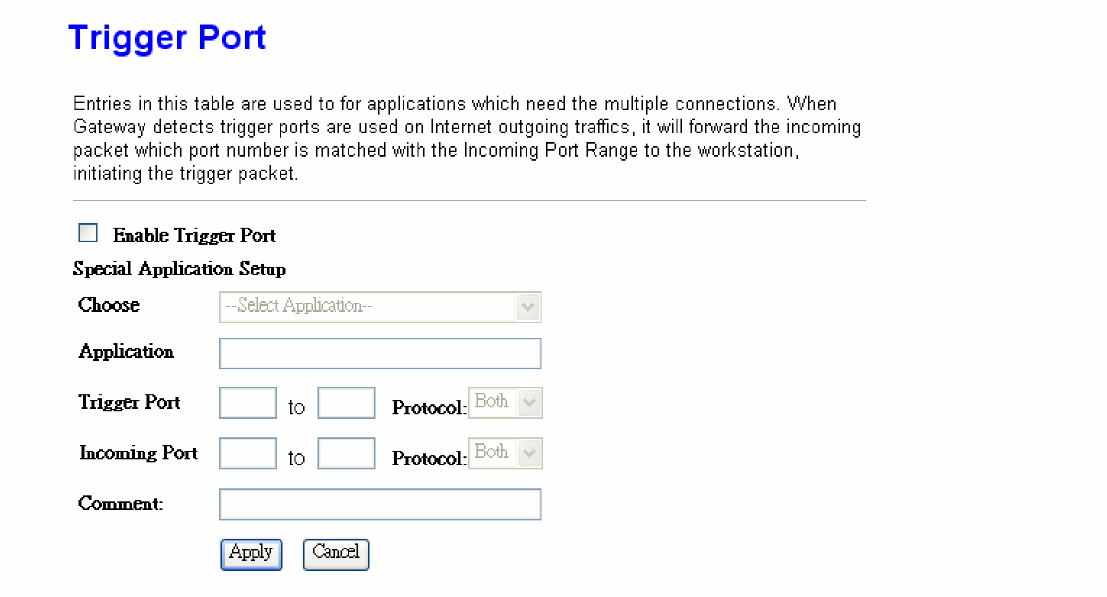
Port: Enter the port range the user wants to forward.

Comment: Explanatory notes.

To save all the settings, click “Apply Changes”, the application, IP address, protocol, port range and comment will be listed in the “Current Port Forwarding Table”.
If the user doesn’t want to use any application listed in the list, check “Selected” and click “Delete Selected” or click “Delete All” to delete all applications.

8.3 Port triggering

Entries in this table are used to for applications which need the multiple connections. When the device detects trigger ports are used on internet outgoing traffics, it will forward the incoming packet which port number is matched with the incoming port range to the workstation, initiating the trigger packet.



Trigger Port

Entries in this table are used to for applications which need the multiple connections. When Gateway detects trigger ports are used on Internet outgoing traffics, it will forward the incoming packet which port number is matched with the Incoming Port Range to the workstation, initiating the trigger packet.

□ Enable Trigger Port

Special Application Setup

Choose: --Select Application--

Application:

Trigger Port: to Protocol: Both

Incoming Port: to Protocol: Both

Comment:

Choose: Select the application the user wants to use.
Application: The selected application will be shown in this table.
Protocol: TCP, UDP or both.
Trigger Port: Trigger port range.
Incoming Port: Incoming port range.
Comment: Explanatory notes.
To save all the settings, click “Apply Changes”, the application, protocol, trigger port, incoming port and comment will be listed in the “Current Trigger Port Table”.
If the user doesn’t want to use any application listed in the list, check “Selected” and click “Delete Selected” or click “Delete All” to delete all applications.
Note: Only IRDC, Windows Media Service and VoIP H.323 can work.