CANYON

CNP-WF514

Wireless Broadband Router

User Manual

Table of Contents

Thank you for purchasing **CANYON CNP-WF514**. We sincerely wish you to enjoy the wireless broadband router. It provides user an easy and stable high speed internet connection. It is also equipped with built-in NAT technology that acts as a firewall to protect the network from outside intrusions. Ultimately, the device is implemented with an IEEE 802.11b/g access point which is capable of wireless LAN network. To fully utilize the functions and features of **CANYON CNP-WF514**, please read through the user manual before you get started.
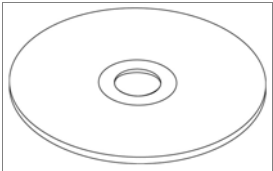
Introduction

Safety Precautions

Please observe all safety precautions before using the device. Please follow all procedures outlined in this manual to properly operate the device.

- Do NOT attempt to disassemble or alter any part of the device that is not described in this guide.
- Do NOT place the device in contact with water or any other liquids. The device is NOT designed to be liquid proof of any sort.
- In the event of liquid entry into device interior, immediately disconnect the device from the computer. Continuing use of the device may result in fire or electrical shock. Please consult your product distributor or the closest support center.
- To avoid risk of electrical shock, do not connect or disconnect the device with wet hands.
- Do NOT place the device near a heat source or directly expose it to flame.
- Never place the device in vicinity of equipments generating strong electromagnetic fields. Exposure to strong magnetic fields may cause malfunctions or data corruption and loss.
- All images in the user manual are for user reference only. Actual products might differ slightly than images shown here.

Package Contents

Product Image	Item Name
	CNP-WF514 Main Unit
	Standing Base
	Power Adapter
	Warranty Card
	Quick Guide
	Documentation CD

Hardware Overview
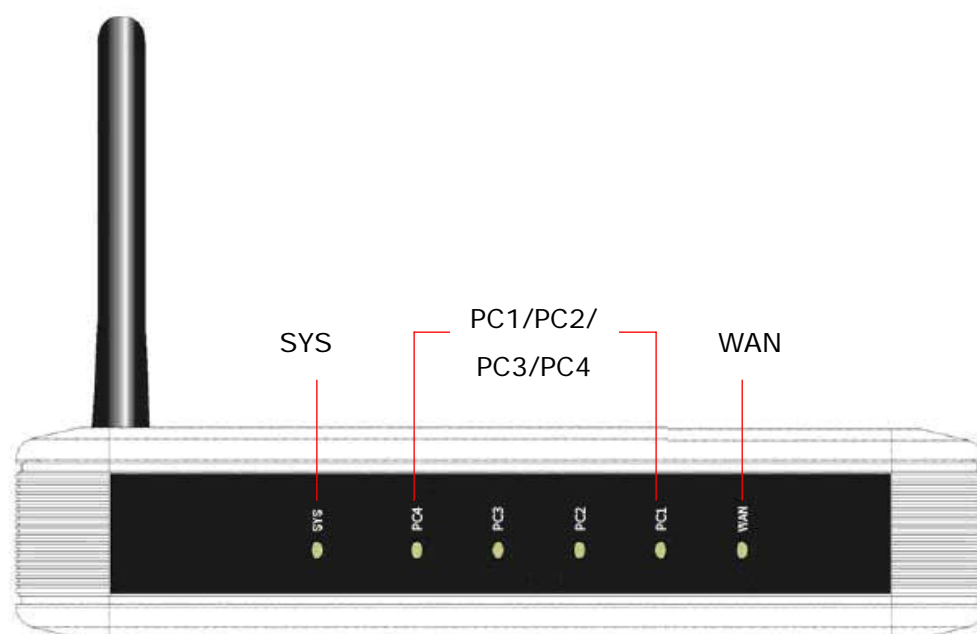
SYS	Power status indicator
WAN	WAN interface status indicator
PC1/PC2/PC3/PC4	LAN interface status indicator
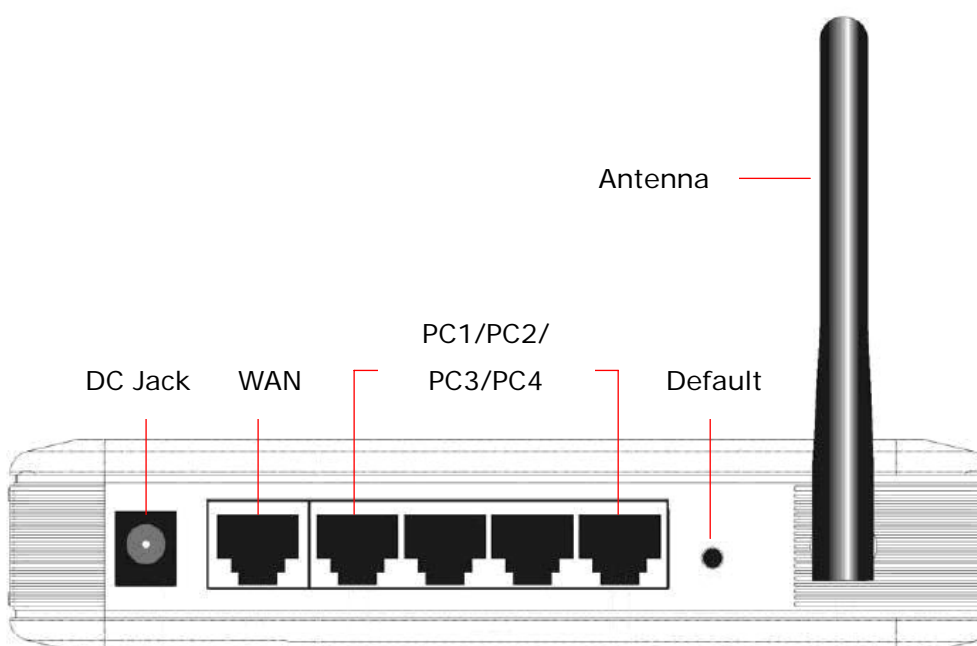
DC Jack	Connects to power adapter
WAN	Connects to cable/DSL modem or other Ethernet devices
PC1/PC2/PC3/PC4	Connects to LAN port on PC or other Ethernet devices
Default	Reset device to factory default settings
Antenna	Transmits signals

Getting Started

Connecting to Device

Please follow the steps below to connect the modem and PC(s) with **CANYON CNP-WF514**:

1. Begin by searching for an appropriate location to setup device. Please keep in mind to keep the device in the center of working area as the signal strength and data transfer rate falls off with distance.
2. It is also recommended to place device at a higher position to ensure minimum obstacle interference.
3. Make sure that all network devices are powered off, including the device itself, PCs, switches, cable or DSL modem, and other peripherals.
4. Connect the modem to WAN port of the device by one CAT 5 Ethernet cable.
5. Connect PC(s) with the LAN ports (PC1/PC2/PC3/PC4) of the device by CAT 5 Ethernet cables. One PC connects to only one port using one cable.
6. Power on the cable or DSL modem.
7. Plug in the power of the device. The Power status indicator at the front panel of device will light up as soon as the power adapter is connected properly.
8. Power on PC(s).

Windows XP Setup

1. Click on Start → Settings → Control Panel.
2. Click on Network and Internet Connections icon.
3. Click on Network Connections
4. Right click on Local Area Connection icon and click on Properties.
5. Select TCP/IP option and click on Properties. The Properties dialog box will be displayed.
6. Check "Obtain an IP address automatically" and "Obtain DNS server address automatically" options.
7. Click Ok to confirm modifications.

Windows Vista Setup

1. Click on Start → Settings → Network Connections.
2. Right click on Local Area Connection icon and click on Properties.
3. Click on Continue in User Account Control dialog box.
4. Select TCP/IPv4 option and click on Properties. The Properties dialog box will be displayed.
5. Check "Obtain an IP address automatically" and "Obtain DNS server address automatically" options.
6. Click Ok to confirm modifications.

Windows 2000 Setup

1. Click on Start → Settings → Control Panel.
2. Double click on Network and Dial-up Connections icon. The Network dialog box will be displayed.
3. Right click on Local Area Connection icon and click on Properties.
4. Select TCP/IP option and click on Properties. The Properties dialog box will be displayed.
5. Check "Obtain an IP address automatically" and "Obtain DNS server address automatically" options.
6. Click Ok to confirm modifications.

Windows 98/ME Setup

1. Click on Start → Settings → Control Panel.
2. Double click on Network icon. The Network dialog box will be displayed.
3. Please make sure that appropriate network card is installed before proceeding. Click on the Configuration label.
4. Select TCP/IP option and click on Properties. The Properties dialog box will be displayed.

NOTE:

Select the TCP/IP item with an arrow "→" pointing to the network card if more than one TCP/IP options is present.

5. Make sure that the option "Obtain IP address automatically" is checked.
6. Make sure that the "WINS Resolution" option is checked under WINS Configuration dialog box.
7. From Gateway dialog box, remove all entries from the Installed gateways

by selecting them and clicking on Remove.

8. From DNS Configuration dialog box, remove all entries from DNS server search order box and Domain suffix search order box by selecting them and clicking on Remove. Click on Disable DNS.

9. Click Ok to confirm modifications.

NOTE:

To access the device via a wireless connection, PC must be equipped with 802.11b or 802.11g wireless adapter/PCI card. The configuration should be set as below:

- Operation Mode: Infrastructure
- SSID: Default
- Authentication: Disabled
- Encryption: Off

Device Configuration

Before setting up the device, please make sure that the host PC(s) is set on the IP sub-network accessible by **CANYON CNP-WF514** device. The default network address of the device is set as 192.168.1.1. Please configure IP address of host PC at 192.168.1.XXX where XXX is a number between 002 and 254. The subnet mask should be 255.255.255.0. Please follow below steps to enter web browser management mode.
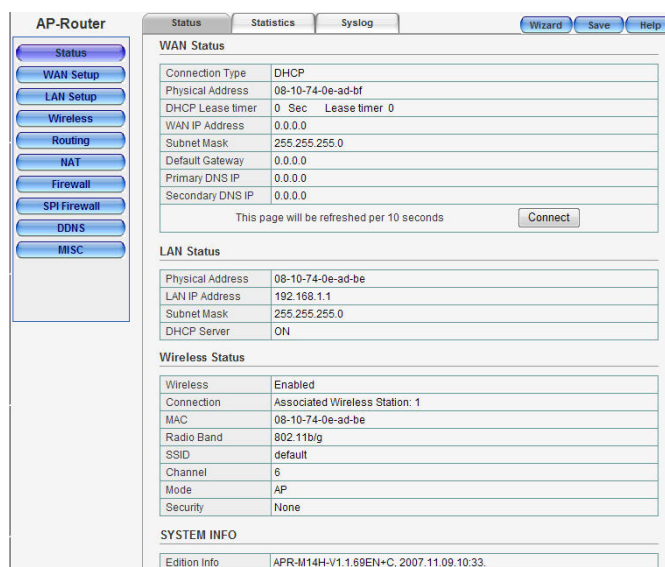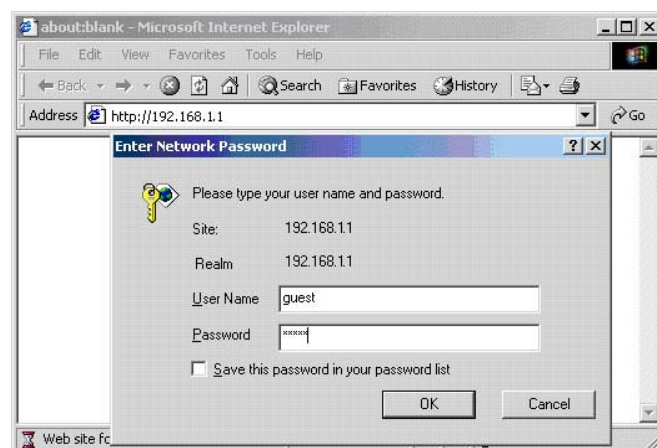
1. Open a browser (**Internet Explorer browser only**) and type in "192.168.1.1" at the address bar and press Enter.
2. Type "guest" at the user name text box and "guest" again at the password text box.
3. The home page of web browser management mode will be displayed.
4. Click on 8 different functions on the main router menu on the left. The corresponding information will be displayed at right.
5. Click on Help at any time to bring up help menu.

NOTE:

The factory settings of user name and the password are by default "guest". It is recommended that user change that information to better maintain network security.

Internet Connection Wizard

1. **Start Internet Configuration Wizard**

- Internet Configuration Wizard will pop up upon successful login.

NOTE:

In order to enter **Wizard** mode, temporarily disable popup window blocking option if necessary or click on **Wizard** to start.

- Select **pop up** to enable automatic Internet Configuration Wizard prompt window. Click on **Save** to save this setting.
- Click on **Start** to continue or Click on **Exit** to exit.

2. **Select Connection Type**

- Select 1 of 7 connection types instructed by ISP or network administrator.
- Click on **Next** to continue or **Prev** to go back to previous page.
- Click on **Exit** to exit.

2.1   DHCP Connection

Internet Configuration Wizard

Set Physical address

If your ISP check the Physical address, Physical address should be set.

MAC	08-10-74-24-af-9d	Clone MAC
Default MAC	08-10-74-24-af-9d	Default MAC

| Prev | Next | | Exit |

- Click on **Clone MAC** or type in MAC address if required by ISP.
- Click on **Default MAC** to restore to default MAC address.
- Click on **Next** to continue or **Prev** to go back to previous page.
- Click on **Exit** to exit.

2.2   PPPoE Connection

Internet Configuration Wizard

PPPoE Account & Password

Set PPPoE Account & Password

Set PPPoE account & password which are supplied from your ISP

| PPPoE Account | 12345@example.eg |
| PPPoE Password | •••••••• |

| Prev | Next | | Exit |

- Type in **PPPoE Account** and **PPPoE Password** provided from ISP.
- Click on **Next** to continue or **Prev** to go back to previous page.
- Click on **Exit** to exit.

2.3 Static IP Connection

Internet Configuration Wizard

Static IP

IP Address	118.166.69.170
Subnet Mask	255.255.255.255
Gateway	118.166.69.170
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

Set Static IP

Fill the blank input box with the values which are suppplied from your ISP

[Prev] [Next]   [Exit]

- Type in **IP Address**, **Subnet Mask**, **Gateway**, **Primary DNS**, and **Secondary DNS** provided from ISP.
- Click on **Next** to continue or **Prev** to go back to previous page.
- Click on **Exit** to exit.

2.4 PPTP DHCP Connection

Internet Configuration Wizard

PPTP

PPTP User Name	12345@example.eg
PPTP Password	•••••••
Server IP Address	0.0.0.0
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

Set PPTP

Set PPTP user name,password,server IP address & others values which are supplied from your ISP

[Prev] [Next]   [Exit]

13

- Type in **PPTP User Name**, **PPTP Password**, **Server IP Address**, **Primary DNS**, and **Secondary DNS** provided from ISP.
- Click on **Next** to continue or **Prev** to go back to previous page.
- Click on **Exit** to exit.

2.5   PPTP Static IP Connection

Internet Configuration Wizard

PPTP   **Set PPTP**

PPTP User Name	12345@example.eg
PPTP Password	•••••••
Server IP Address	0.0.0.0
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

Set PPTP user name,password,server IP address & others values which are supplied from your ISP

Prev   Next   Exit

- Type in **PPTP User Name**, **PPTP Password**, **Server IP Address**, **Subnet Mask**, **Gateway**, **Primary DNS**, and **Secondary DNS** provided from ISP.
- Click on **Next** to continue or **Prev** to go back to previous page.
- Click on **Exit** to exit.

2.6   L2TP DHCP Connection

Internet Configuration Wizard

L2TP   **Set L2TP**

L2TP User Name	12345@example.eg
L2TP Password	•••••••
Server IP Address	0.0.0.0
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

Set L2TP user name,password,server IP address & others values which are supplied from your ISP

Prev   Next   Exit

- Type in **L2TP User Name**, **L2TP Password**, **Server IP Address**, **Primary DNS**, and **Secondary DNS** provided from ISP.
- Click on **Next** to continue or **Prev** to go back to previous page.
- Click on **Exit** to exit.

2.7   L2TP Static IP Connection
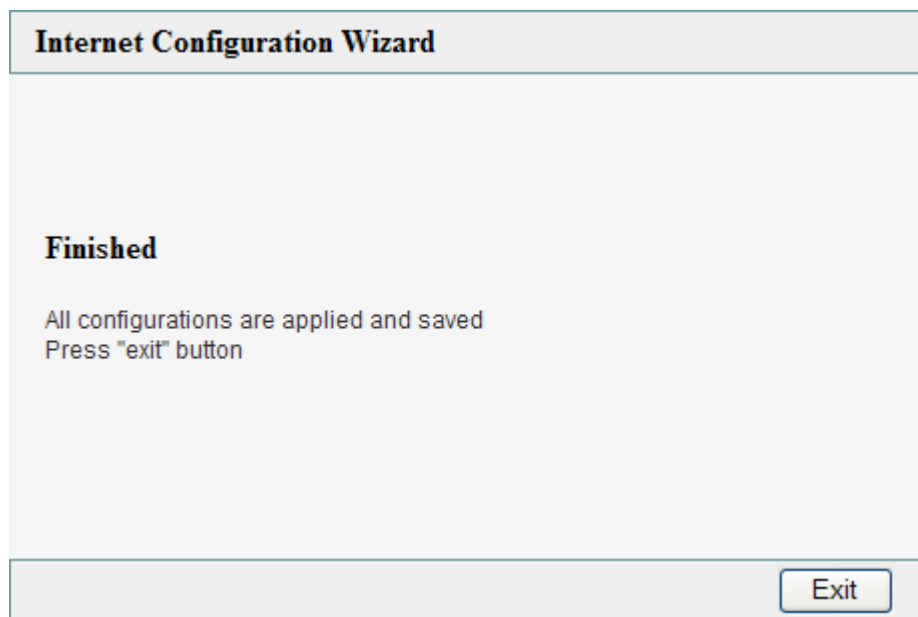
- Type in **L2TP User Name**, **L2TP Password**, **Server IP Address**, **Subnet Mask**, **Gateway**, **Primary DNS**, and **Secondary DNS** provided from ISP.
- Click on **Next** to continue or **Prev** to go back to previous page.
- Click on **Exit** to exit.

3.   Wireless AP Configuration

- Select a **Radio Band** type from the drop down box. (802.11b/g is recommended)
- Select **Radio Mode** from the drop down box. (AP+WDS is recommended)
- Type in **SSID** as desired. (SSID must be identical in all devices connecting to device)
- Select a broadcasting channel from drop down box. (Device is set on channel 6 by default)
- Click on **Next** to continue or **Prev** to go back to previous page.
- Click on **Exit** to exit.

4. **Installation Completed**

Internet Configuration Wizard

Finished

All configurations are applied and saved
Press "exit" button

Exit

- Click on **Exit** to finish Internet Configuration Wizard.

Status

Status **Statistics**	**Wizard** **Save** **Help**

WAN Status

Connection Type	DHCP
Physical Address	08-10-17-22-1a-0c
DHCP Lease timer	0 Sec Lease timer 0
WAN IP Address	0.0.0.0
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Primary DNS IP	0.0.0.0
Secondary DNS IP	0.0.0.0
This page will be refreshed per 5 seconds	**Connect**

LAN Status

Physical Address	08-10-17-22-1a-0b
LAN IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	ON

Wireless Status

Wireless	Enabled
Connection	Disconnected
MAC	08-10-17-22-1a-0b
Radio Band	802.11b/g
SSID	default
Channel	6
Mode	AP
Security	None

SYSTEM INFO

Edition Info	APR-M14H-V1.1.02EN-OEM, 2006.04.11.15:50.

1. This section displays various router information divided into 3 tabs.

2. The 1st tab displays parameters of **WAN/LAN/Wireless** connection, and **System Info**.

   - **WAN Status**: WAN interface parameters of the device.

   NOTE:

   Click on **Connect** to refresh IP address with **DHCP** connection type and to initiate a dial up connection with **PPPoE** connection type.

   - **LAN Status**: LAN interface parameters of the device.

   - **Wireless Status**: WLAN interface parameters of the device.

   - **System Info**: Displays device firmware version.

System Run Time

System Run Time	0 days 2 hours 8 minutes 33 seconds

Type	Current NAT	Transmit Accumulation Statistic				Rate (KB/s)	
		Received Packets	Received Bytes (K)	Sent Packets	Sent Bytes (K)	Upload	Download
TCP	0	0	0	0	0	0	0
UDP	0	0	0	0	0	0	0
ICMP	0	0	0	0	0	0	0
OTHER	0	0	0	0	0	0	0
TOTAL	0	0	0	0	0	0	0

Refresh

3. The 2nd tab displays statistics of packets from WAN port. Click on **Refresh** to update data monitor table to receive most recent data.

- **System Run Time**: Displays system run time from last system restart.
- **Statistics**: Monitors current sent/received packets through both wireless and wired connection.

Syslog

```
20070101(12:00:00):[SYSTEM]:load default parmarm!
20070101(12:00:00):[SYSTEM]:Router started.|
20070101(12:00:03):[SYSTEM]:WAN port link down.
20070101(12:02:09):[WIRELESS]:Wireless client 00-1B-77-06-8C-CD is associated with the AP.
20070101(12:02:12):[SYSTEM]:WAN port link down.
20070101(12:07:52):[WIRELESS]:Wireless client 00-16-6F-1A-39-BE is associated with the AP.
20070101(12:07:52):[SYSTEM]:WAN port link down.
```

Refresh   Clear

4. The 3rd tab displays system logs including system events, network abnormalities.

WAN Setup

WAN Setup

- ● Dynamic IP User (Cable Modem)
- ○ PPPoE User (ADSL)
- ○ Static IP User
- ○ PPTP
- ○ L2TP

DHCP Client Setup

MAC	08-10-74-24-af-9d	Clone MAC
Default MAC	08-10-74-24-af-9d	Default MAC
MTU	1514	
Primary DNS	168.95.1.1	
Secondary DNS		
	Apply	

1. This section assists user to setup network connection types and their subsidiary functions. The default setting is Dynamic IP connection type.
2. Click on **Save** to save modified settings.

Dynamic IP Setting

DHCP Client Setup

MAC	08-10-73-06-0d-1c	Clone MAC
Default MAC	08-10-73-06-0d-1c	Default MAC
MTU	1514	
Primary DNS		
Secondary DNS		
	Apply	

1. Click on **Dynamic IP User (Cable Modem)** option.
2. Click on **Clone MAC** to replace current device MAC address with host PC MAC address. Click on **Default MAC** to restore to default.
3. Enter **MTU** (Maximum Transmission Unit) value if required. The default value is set at 1496.

NOTE:

It is recommended to set MTU value between 1200 and 1500 range.

4. Enter **Primary DNS** and **Secondary DNS** IP address if required by ISP provider.

5. Click on **Apply** to confirm modifications.

6. Click on **Save** to save modified settings.

PPPoE Setting

1. Click on **PPPoE User (ADSL)** option.

2. Type in **PPPoE Account** and **PPPoE Password** provided from ISP.

3. Click on **MAC Clone** to replace current device MAC address with host PC MAC address. Click on **Default MAC** to restore to default.

4. Enter **MTU** (Maximum Transmission Unit) value if required. The default value is set at 1496.

NOTE:

It is recommended to set MTU value between 1200 and 1500 range.

5. Enter **Primary DNS** and **Secondary DNS** IP address if required by ISP provider.

6. Select a connection mode if necessary. The default setting is "**Connect to Internet automatically**".

7. Click on **Apply** to confirm modifications.

8. Click on **Save** to save modified settings.

Static IP Setting

1. Type in **WAN IP Address**, **Subnet Mask**, **Default Gateway**, **Primary DNS** and **Secondary DNS** address provided by ISP.
2. Click on **MAC Clone** to replace current device MAC address with host PC MAC address. Click on **Default MAC** to restore to default.
3. Enter **MTU** (Maximum Transmission Unit) value if required. The default value is set at 1496.

NOTE:

It is recommended to set MTU value between 1200 and 1500 range.

4. Click on **Apply** to confirm modifications.
5. Click on **Save** to save modified settings.

PPTP Setting

1. Type in **User Name** and **Password** provided by ISP.
2. Type in PPTP **Server IP Address**.
3. Select connection type. Please follow instructions from ISP. Enter Static **WAN IP Address/Subnet Mask/Gateway** if necessary.
4. Enter **Primary DNS** and **Secondary DNS** IP address if required by ISP provider.
5. Enter **MTU** (Maximum Transmission Unit) value if required. The default value is set at 1496.

NOTE:

It is recommended to set MTU value between 1200 and 1500 range.

6. Click on **Apply** to confirm modifications.
7. Click on **Save** to save modified settings.

L2TP Setting

Dial-up users typically use the PPP (Point-to-Point Protocol) for an Internet connection. PPP is a layer 2 protocol that frames data so it can be sent across a dial-up connection. The protocol allows users to run TCP/IP software such as Web browsers as if they were directly connected to the Internet. In fact, user TCP/IP packets are put into PPP frames for transport across the dial-up link to an ISP. The ISP then extracts the TCP/IP packets and forwards them on the Internet. L2TP enhances PPP by granting a means for a remote user to extend a PPP link across the Internet all the way to a corporate site. In essence, a tunnel is established across the Internet from the ISP to a corporate site and frames are transmitted through the tunnel. Once the tunnel is set up, the ISP is essentially out of the picture and the user communicates to the corporate network over what appears to be a direct dial-up connection.

L2TP

User Name	john
Password	•••••••
Server IP Address	202.139.15..19

Chose one WAN connection type DHCP or Static IP

⊙ DHCP	
○ Static IP	
Primary DNS	61.139.2.69
Secondary DNS	
MTU	1440

Apply

1. Type in **User Name** and **Password** provided by ISP.

2. Type in PPTP **Server IP Address**.

3. Select connection type. Please follow instructions from ISP. Enter Static **WAN IP Address/Subnet Mask/Gateway** if necessary.

4. Enter **Primary DNS** and **Secondary DNS** IP address if required by ISP provider.

5. Enter **MTU** (Maximum Transmission Unit) value if required. The default value is set at 1496.

NOTE:

It is recommended to set MTU value between 1200 and 1500 range.

6. Click on **Apply** to confirm modifications.

7. Click on **Save** to save modified settings.

LAN Setup

System IP Setup

System IP Address	192.168.1.1
Subnet Mask	255.255.255.0
☑ DHCP Server on	
DHCP IP Pool	192.168.1. 2 -192.168.1. 102

Apply

1. This section assists user to designate a specific IP address to the device and other IP addresses to PC(s) or network machines connected to the device. The section is divided into 2 tabs.

2. The 1st tab configures PC(s) connected to device and other settings. Type in **System IP Address** of device LAN port IP address. This is the default gateway IP address of LAN client(s)/host PC(s).

3. Type in **Subnet Mask** of the device LAN segment.

4. Enable/disable **DHCP Server** function by clicking on the option. Enabling DHCP Server function allows the device to assign host PC(s) IP address. DHCP IP address range can be allocated by entering range of IP addresses under **DHCP IP Pool** option.

5. Click on **Apply** to confirm modification.

   NOTE:

   User must manually assign IP address of host PC(s) if **DHCP Server on** option is disabled.

DHCP IP Address Reserving

☐ Auto Setup	
Physical Address	
IP Address	192.168.1. 23
	Add

ID	IP Address	Physical Address	Delete
1	192.168.1.23	00-c0-26-a8-4a-9b	Delete

1. Reserve a specific **DHCP IP Address** to a PC or network device by typing the client's MAC address and desired IP segment. Click **Add** to confirm.

2. A Designated IP Table below displays all DHCP IP address reserved. Select an IP address and click on **Delete** to remove it from table.

3. Click on **Save** to save modified settings.

DHCP Client Info

ID	IP Address	MAC Address	Status
1	192.168.1.23	00-c0-26-a8-4a-9b	Static

1. The 2nd tab displays all PC(s) connected to the device.

Wireless

Basic Setting

1. This section assists user to create a network environment that connects wireless PC(s) to a wired LAN. It also allows wireless stations to access network resources and share the broadband Internet connection. The section is divided into 6 tabs.
2. The 1st tab defines basic settings for wireless networking. Check on **Disabled Wireless** and click on **Apply** to disable wireless function. Uncheck to restore.
3. Select **Radio Band** and **Radio Mode** from the drop down menu boxes.
4. Check on **Booster Mode** to increase throughput of data transmission. Uncheck to disable.
5. Type in desired **SSID** (network name shared among all points in a wireless network). **SSID** is case sensitive and must not exceed 32 characters.

NOTE:

It is recommended to change default **SSID** (default) to a unique name for better security.

6. Select a channel (14 channels) for wireless communication. Channels 1, 6, and 11 are non-overlapping channels while all others are overlapping channels.
7. Click on **Apply** to confirm modification.
8. Click on **Save** to save modified settings.

Security Setting

The 2nd tab defines all common security settings for wireless networking. Select one of the **Authentication Type** from the drop down menu box.

- **None**:
  1. Any data will be transmitted without encryption and any PC(s) is able to connect to device without authentication. This is the default setting.
  2. Click on **Apply** to confirm modification.

- **WEP**:
  1. WEP (Wired Equivalent Privacy) utilizes a combination of 64-bit or 128-bit keys to provide access control and encryption security.
  2. Select **Authentication & Encryption** type (**Open System**, **Shared Key**, and **Auto Select**) from the drop down menu box.
  3. Select **KEY Length** (64 bits/128 bits) and **WEP Mode** (HEX/ASCII) as desired. Settings on PC(s) must match that of the device.
  4. Select 1 of 4 keys to type in a string of characters defined in the description box. The key criteria is listed as below:

Key Length	HEX Format	ASCII Format
64 bit	10 hexadecimal digits	5 ASCII characters
128 bit	26 hexadecimal digits	13 ASCII characters

  5. Click on **Apply** to confirm modification.

Security Configuration

| Authentication Type | WPA Personal ▼ |
| Accessorial Authentication & Encryption | TKIP ▼ |

Pre-Shared Key

Key Format	Please input 8-63 characters
KEY	**********
Rekey Time (sec)	86400

Apply

- **WPA Personal**:
  1. WPA (Wi-Fi Protected Access) is an advanced security standard that utilizes pre-shared key to authenticate wireless stations and encrypt data during communications.
  2. Select **Authentication & Encryption** type (**TKIP** and **AES**) from the drop down menu box.
  3. Type in Pass Phrase with size ranging from 8 to 63 characters under **KEY** option.
  4. Specify time WPA key must be renewed. The default value is 86400.
  5. Click on **Apply** to confirm modification.

  NOTE:

  TKIP (Temporal Key Integrity Protocol) utilizes a stronger encryption algorithm and includes Message Integrity Code while **AES** (Advanced Encryption System) utilizes a symmetric 128 bit block data encryption, the strongest encryption currently available.

Security Configuration

| Authentication Type | WPA2 Personal ▼ |
| Accessorial Authentication & Encryption | AES ▼ |

Pre-Shared Key

Key Format	Please input 8-63 characters
KEY	**********
Rekey Time (sec)	86400

Apply

- **WPA2 Personal**
  1. WPA2 is a more advanced version of WPA which only authenticates access and encrypts data transmission with **AES** type.

2. Type in Pass Phrase with size ranging from 8 to 63 characters under **KEY** option.
3. Specify time WPA key must be renewed. The default value is 86400.
4. Click on **Apply** to confirm modification.

Security Configuration

Authentication Type	WPA&WPA2 Personal ▾

Pre-Shared Key

WPA	⦿ TKIP ○ AES
WPA2	⦿ AES
KEY Mode	Please input 8-63 characters
WPA Pass Phrase	**********
WPA2 Pass Phrase	**********
Rekey Time (sec)	86400
	Apply

- **WPA&WPA2 Personal**:
  Auto-select WPA or WPA2 detects PC wireless authentication information and adjusts its setting accordingly. The operations are identical to that of WPA and WPA2. Please refer to previous sections for detailed information.

Filter List Setting

Wireless Access Control Configuration

☑ Enable Wireless Access Control	Apply
○ Defined items in MAC list are PERMITTED to connect AP, others are DENIED	Apply
⦿ Defined items in MAC list are DENIED to connect AP, others are PERMITTED	

MAC		Add
Descript		

ID	MAC	Descript	Delete
1	CC-00-AA-BB-FF-12	pc1	Delete

1. The 3rd tab specifies wireless access control based on MAC address of PC(s).
2. Check on **Enable Wireless Access Control** and click on **Apply** to implement access control.
3. Check on appropriate radio button option and click on **Apply** to implement security control type.

4. Type in **MAC** address of PC(s) and optional comments if necessary under **Descript** box. Click on **Add** to edit modified rule.

5. An Access Control Table below displays all PC(s) under access control on the network. Select a rule and click on **Delete** to remove it from table.

6. Click on **Save** to save modified settings.

WDS Setting

Wireless Bridge Configuration

Wireless Bridge MAC		Add
Descript		

Current Wireless Bridge Information

No	MAC	Descript	Delete
1	00-33-CF-25-A1-00	wds	Delete

1. The 4ᵗʰ tab creates wireless bridge between 2 or more router device.

2. Type in **MAC** address of other router device(s) and optional comments if necessary under **Descript** box. Click on **Add** to edit modified rule.

3. A Wireless Bridge Information Table below displays all router devices bridged on the network. Select a router device and click on **Delete** to remove it from table.

4. Click on **Save** to save modified settings.

WDS Setting

Advanced Setting

Beacon Interval	100	(20-1000 ms)
RTS Threshold	2347	(256-2432)
DTIM Interval	1	(1-255)
Transmit Rate	Auto	
Preamble Type	⊙ Long ○ Short ○ Auto	
802.11g protection	⊙ CTS ○ RTS/CTS ○ Disabled	
	Apply	

1. The 5ᵗʰ tab adjusts advanced wireless function.

2. Type in the **Beacon Interval** between each beacon broadcast. A beacon is a packet broadcasted by the device to assist in network synchronization. The default value is 100.

3. Type in **RTS Threshold** value as desired between 256 and 2432. The default value of 2347 should only be modified when encountering inconsistent data flow.

4. Type in **DTIM Interval** frequency between each DTIM (Delivery Traffic Indication Message) broadcast. Lower value result in more efficient networking while preventing PC(s) from entering power saving mode. Higher value interferes with wireless transmission yet allowing PC(s) to enter sleep mode thus saving power consumption.

5. Select maximum **Transmit Rate** (Transmission rate of data packets)of the device. The default value is **Auto**.

6. Select **Preamble Type** (Length of CRC block in the frames during wireless communication). **Short** Preamble is appropriate for heavy traffic wireless network while **Long** Preamble provides better communication reliability.

7. Select **802.11g Protection** type between **CTS**, **RTS/CTS**, or disabled.

8. Click on **Apply** to confirm modification.

9. Click on **Save** to save modified settings.

Association Table

No	MAC Address	Status	Band	Rate	Signal Quality	RSSI	Power Save

Refresh

1. The 6th tab displays all PC(s) connected to device via wireless network.
2. Click on **Refresh** to update table.

Routing

Routing Table Management

Type	Target	Mask	Gateway
NET ▼			

Add

ID	Type	Target	Mask	Gateway	Delete
0	NET	10.0.0.0	255.255.255.0	192.168.1.8	Delete

1. This section assists user to create static route(s) between network and device.

2. Select Route **Type** and type in **Target** IP address, Subnet **Mask**, and **Gateway** IP. Click on **Add** to add routing information.

3. A Routing Table below displays all static routing paths. Select a routing path and click on **Delete** to remove it from table.

4. Click on **Save** to save modified settings.

NAT

Network Address Translation (NAT) technology allows multiple users at local network to gain access to Internet through a single public IP address while user PC(s) are still under firewall protection.

DMZ Host Setup

DMZ Host Setup

☑ DMZ	192.168.1. 11	Apply

1. DMZ function enables PC to be exposed to the Internet for use of special purpose services.
2. Check **DMZ** option and enter desired PC IP address to be exposed.
3. Click on **Apply** to confirm modification.
4. Click on **Save** to save modified settings.

FTP Private Port

FTP Private Port

☑ Port Number	1025	Apply

1. FTP function enables File Transfer Protocol which does not use the standard port 21.
2. Check **Port Number** and enter the port number.
3. Click on **Apply** to confirm modification.
4. Click on **Save** to save modified settings.

Virtual Server Setup

Virtual Server Setup

Rule Name	FTP
Internal Server IP Address	192.168.1. 6
Protocol	TCP
External Port	21
Internal Port	21
	Add

ID	Rule Name	Internal IP	Protocol	External Port	Internal Port	Delete
1	FTP	192.168.1.6	TCP	21	21	Delete

1. Virtual server allows PC(s) located outside of network to be able to access services on PC(s) connected to the device.

2. Type in the description of the rule desired under **Rule Name**.

3. Type in internal **IP address** of the client PC(s) desired for public port number packet access.

4. Select the **Protocol** type including TCP, UDP, FTP, HTTP, HTTPS, POP3, SMTP, DNS, TELNET, IPSEC, and PPTP.

5. Enter **External Port** number that the public port number will be changed to when the packet enters the network.

6. Enter **Internal Port** number from the Internet that will be redirected to the private IP address in the network.

7. Click on **Add** to add modified rule.

8. A Virtual Server Table below displays all valid virtual servers available on the network. Select a rule and click on **Delete** to remove it from table.

9. Click on **Save** to save modified settings.

Port Triggering

Port Triggering

Predefined Trigger Rules	Select one of the predefined rules ▼
Rule Name	
Trigger Protocol	TCP ▼
Trigger Port	-
Forward Protocol	TCP ▼
Forward Port	
	Add

ID	Rule Name	Trigger Condition	Forward Condition	Delete
1	GuruGuru	tcp:31200	tcp:9292	Delete

1. Port Triggering function commands router to remember outgoing data for specific port numbers, recalls the matching requested data, and pulls the data back to the proper PC(s) by its IP address and port mapping rules.

2. Select one of the predefined rules or type in the description of the service desired under **Rule Name**.

3. Select outbound port protocol type between **TCP** and **UDP** under **Trigger Protocol**.

4. Type in all of the outbound range of port numbers. Port numbers are separated by comma. Use a dash in between port numbers to define a range of port numbers.

5. Select inbound port protocol type between **TCP** and **UDP** under **Forward Protocol**.
6. Type in all of the inbound range of port numbers. Port numbers are separated by comma.
7. Click on **Add** to add modified rule.
8. A Trigger Port Table below displays all valid trigger rules available on the network. Select a rule and click on **Delete** to remove it from table.
9. Click on **Save** to save modified settings.

Firewall

The device provides extensive firewall protections by restricting connection parameters to limit the risk of attacks and creates packet filtering rules by restricting service ports, IP address or MAC address.

MAC Filtering Configuration

1. MAC Filtering function blocks certain PC(s) from Internet access based on MAC addresses.
2. Click on **Start/Stop** to turn on/off the MAC filtering configuration.
3. Check the option to allow all other PC(s) whose MAC address(es) are not on the list to be permitted of Internet access.
4. Type in **MAC address** (in format of XX-XX-XX-XX-XX-XX) of desired PC and select **Permit/Deny** to manage its Internet accessibility. Click **Add** to add modified rule.
5. A MAC Filtering Table below displays all valid MAC filtering rules available on the network. Select a rule and click on **Delete** to remove it from table.
6. Click on **Save** to save modified settings.

Connection Filtering Configuration

Connection Filtering Configuration

Status	The current status is enabled	Stop
☑ If checked, the undefined item in IP Address list is allowed to access Internet;Unchecked means reverse		Apply

Rule Name	test
Source IP Address	192. 68.1. 11 - 192.168.1. 12
Protocol	TCP ▼
Destination Port	80 - 80
status	Permit ▼

Days To Block	☐ Everyday	☑ Sun ☑ Mon ☐ Tue ☑ Wed ☐ Thu ☐ Fri ☐ Sat
Times To Block	☐ All Day	00:00 ▼ - 00:00 ▼
	Add	

Rule Name	Source IP	Protocol	Dest Port	Days	Times	Rule	Delete
test	192.168.1.2-192.168.1.7	ALL	None	Everyday	All Day	Permit	Delete

1. Connection Filtering function blocks certain PC(s) from Internet access based on time.
2. Click on **Start**/**Stop** to turn on/off the MAC filtering configuration.
3. Check the option to allow all other PC(s) whose IP address(es) are not on the list to be permitted of Internet access.
4. Type in the description of the rule desired under **Rule Name**.
5. Type in source IP address desired to apply this access control rule.
6. Select protocol type including **TCP**, **UDP**, **FTP**, **HTTP**, and **ALL**.
7. Type in a range of port numbers to block corresponding PC(s) from accessing Internet.
8. Select days and/or time to apply this access control rule. Click **Add** to add modified rule.
9. An Access Control Table below displays all valid access control rules available on the network. Select a rule and click on **Delete** to remove it from table.
10. Click on **Save** to save modified settings.

URL Filtering Configuration

URL Filtering Configuration

Note: You can use wildcards(* and ?);"*"is the multi-letters;"?" is a letter;For example:*.*sex*.* express that all URL with "sex" will be blocked!

| Input Filtering Keyword | *.example.com | Add |

ID	Filtering Keyword	Delete
1	*.example.com	Delete

1. URL Filtering function blocks certain website accesses by specifying keywords.
2. Type in keywords to block PC(s) from accessing Internet websites. Wildcards such as "*" (a string of characters) or "?" (a single character) are available. Click **Add** to add modified rule.
3. A Keyword filtering Table below displays all valid keyword rules available on the network. Select a rule and click on **Delete** to remove it from table.
4. Click on **Save** to save modified settings.

Ping Filtering Configuration

Ping Filtering Configuration

| ☐ Discard ping request from WAN interface | Apply |
| ☐ Discard ping request from LAN interface | Apply |

1. Ping Filtering function rejects ping requests from other devices.
2. Check on one or both options to **Discard ping request from WAN/LAN interface**.
3. Click on **Apply** to confirm modification.
4. Click on **Save** to save modified settings.

SPI Firewall

SPI (Stateful Packet Inspection) **Firewall** enhances data security in a network environment more efficiently and effectively by examining additional characteristics of data packets and applying logical analysis.

1. Check on **Set SPI Firewall State** and click **Apply** to activate SPI Firewall function.

2. Check on **Limit the max session of the host** and specify its maximum session value to limit network sessions. Click on **Apply** to confirm modifications.

3. Check on **Limit the max unfinish session of the host** and specify its maximum unfinished session value to limit unfinished network sessions. Click on **Apply** to confirm modifications.

4. Check on **The host created NAT sessions exceeding ____ in ____ seconds** and specify session value and time period to limit NAT sessions in designated time period.

5. Check on **The host send bytes exceeding ____ (Kbytes) in ____ seconds** and specify total data amount and time period to limit NAT sessions in designated amount of data transmission. Click on **Apply** to confirm modifications.

6. Check on **Lock of the host** and specify number of seconds to prohibit visits from illegal hosts for a user specified time duration.

7. Check on **Record to system log** and click on **Apply** to record events on system log.

8. Click on **Apply** to confirm modification.

9. Click on **Save** to save modified settings.

DDNS

Dynamic Domain Name System (DDNS) maps the static domain name to a dynamic IP address. Account, password, static domain name must be obtained from DDNS service provider.

DDNS Setup

DDNS Setup	
* Sign up www.dyndns.org first.(Free)	
DynDNS Operation	⊙ Start ○ Stop
User ID	
Password	
Host Name	
Information	close!
Apply	Refresh

1. Click on **Start/Stop** to turn on/off **DynDNS Operation**.

NOTE:

User must sign up on www.dyndns.org to obtain DynDNS service before starting.

2. Type in account name, password, and domain obtained from DDNS provider.

3. Click **Apply** to confirm modification and **Refresh** to display most recent update.

4. Click on **Save** to save modified settings.

MISC

Login ID & Password Setup

Login ID & Password Setup		
Login name is "guest"		Apply
New Password	•••••	
Confirm New Password	•••••	

1. The default Login ID is "guest" and the default password is also "guest".

2. To change password, type in new password and type in the same new password again to confirm.

3. Click **Apply** to confirm modifications.

4. Click on **Save** to save modified settings.

NOTE:

To reset device to factory default setting, press **RESET** button on the device front panel. The Login ID and password will be reset to "guest".

Remote Management

Remote Mgmt		
☑ Management Port	8080	Apply

1. The Remote Management function allows user to manage the device through Internet from a remote location.
2. Check **Management Port** option and type in the corresponding port number.
3. Click **Apply** to confirm modifications.
4. Click on **Save** to save modified settings.

NOTE:

To access web based management page, simply type in http://<WAN IP Address>:8080 (for example: http://192.168.1.8:8080).

UPnP Setup

UPnP Setup

☑ Enable UPnP Server		Apply

1. The UPnP function exposes the device on the Intranet (internal) network. PC(s) connected to the device does not require further configuration to access the network.
2. Check **Enable UPnP Server** option.
3. Click **Apply** to confirm modifications.
4. Click on **Save** to save modified settings.

System Time Setup

System Time Setup

System Time	Feb 27 2004 7:17:54	
GMT	(GMT+08:00) Beijing, Hongkong, KualaLumpur, Singapore ▾	Apply

1. The System Time Setup function configures device time.
2. Select one of the time zones from the drop down menu.
3. Click **Apply** to confirm modifications.
4. Click on **Save** to save modified settings.

WAN Link Status & Setup

WAN Link Status & Setup

WAN Link Status	100Mbps-Full	WAN Link Setup	Auto ▾	Apply

1. The WAN Setup function configures device connection bandwidth.
2. Select one of the connection bandwidth from the drop down menu.
3. Click **Apply** to confirm modifications.
4. Click on **Save** to save modified settings.

Restore Default/Restart System

Restore Default / Restart System	
Restore Default	Restart System

1. Click on **Restore Default** to restore all device settings to factory setting.
2. Click on **Restart System** to reboot the device.

Firmware Upgrade

Firmware Upgrade		
New Firmware File:	Browse...	Apply

1. Click on **Browse** to locate firmware file on host PC.
2. Click **Apply** to confirm modifications.

NOTE:

Press briefly on **Default** button to reset the device. Press and hold the button for at least 5 seconds to restore device to factory default settings.

Troubleshooting

Please refer to the following procedures if **CNP-WF514** does not function as it should be. Be advised that the following instructions are only intended for simply troubleshooting purpose. Please contact your local authorized shops for further troubleshooting and technical support.

- **Do not remember password.**
    1. Press and hold the reset button on the front panel of device for more than 5 seconds.
    2. Unplug power adapter and wait for 5 seconds before plugging it in again.
- **Device malfunctioning with cable/DSL modem connection.**
    1. Please check signal stability from cable/DSL modem. There should be a signal indicator on the modem displaying its connection status. Contact ISP if the signal is bad.
    2. Please check status indicators on the front panel of device. When working properly, the SYS indicator should be solid and the WAN indicator should be blinking. The LAN indicator(s) should also be blinking with corresponding PC(s) connect to the device.
    3. Please verify that the network cables are working properly.
    4. Enable DHCP server function. Please refer to LAN setup section
    5. Reset the device as described at above section if all else failed.
- **Setup PC(s) to obtain IP address manually.**
    The below instructions only refer to Windows XP verison OS only. Please refer to OS manufacturer for other OS
    1. Click on Start → Settings → Control Panel.
    2. Click on Network and Internet Connections and then Network Connections.
    3. Right click on Local Area Connection icon and select Properties.
    4. Highlight Internet Protocol (TCP/IP) item and click on Properties.
    5. Type in the following information on the corresponding properites:
        - IP address: 192.168.1.XXX where XXX is a number between 2 and 253.
        - Subnet mask: 255.255.255.0
        - Default gateway: 192.168.1.1
        - Preferred DNS server: 192.168.1.1
        - Alternate DNS server: leave this property blank.
    6. Click on OK to confirm modifications.

Appendix

Technical Specifications

Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE802.11b
Channels	13 Channels
Management Interface	Web Based
Network Ports	WAN: 1 X 10/100 RJ-45 Port LAN: 4 X 10/100 RJ-45 Ports (with switching function)
Cabling Type	Cat 5 Ethernet Network Cable
RF Power Output	15 ± 2dBm
Wireless Security	WPA/WPA2, WEP 64/128bit, Wireless MAC Filtering
LED Indicators	SYS, WLAN, LAN Link/Activity, WAN
Temperature	Operating: 0° to 40° C Storage: -20° to 70° C
Humidity	Operating: 10% to 85 % non-condensing Storage: 5% to 90 % non-condensing
Dimensions	135mm(L) X 95.4mm(W) X 28mm(H)
Weight	210g
Power	DC 9V, 700mA