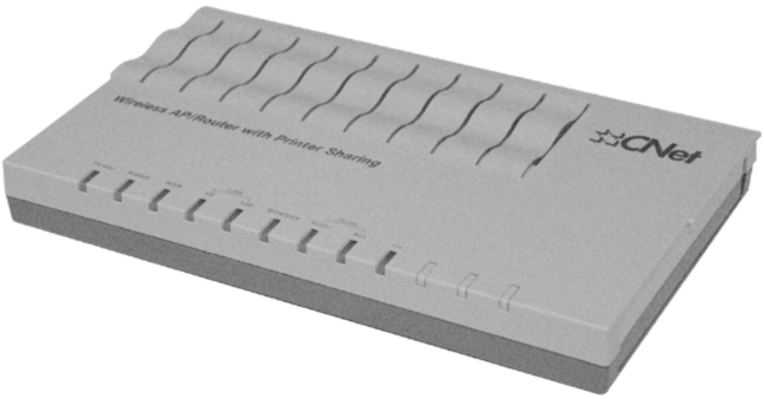
Multi-Function Wireless A/P Router

User's Guide



Model

CNWR-811P

Wireless Access Point Router
W / Printer Sharing

CNet®
TOTAL NETWORK SOLUTIONS

TABLE OF CONTENTS

Document Version: 1.0

P/N 9560DA0007

Chapter 1

Introduction

This Chapter provides an overview of the CNWR-811P's features and capabilities.

Congratulations on the purchase of your new CNWR-811P Multi-Function Wireless A/P Router. The CNWR-811P is a multi-function device providing the following services:

- Shared Internet access via an ADSL or Cable modem.
- Wireless LAN Access Point (base station) for equipment compliant with the IEEE802.11b (DSSS) specifications.
- Network Printer – LAN users can share the printer attached to the CNWR-811P

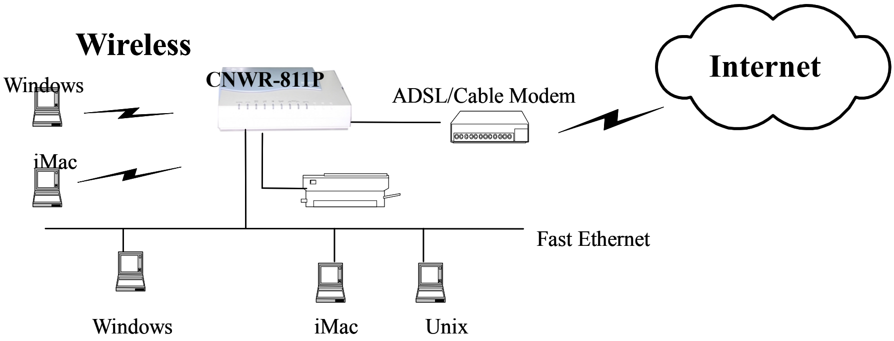


Figure 1: CNWR-811P Multi-function Wireless A/P Router

The CNWR-811P Multi-Function Wireless A/P Router can also be used to connect your local LAN to a remote LAN or WAN, instead of providing shared Internet Access.

CNWR-811P Features

The CNWR-811P incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

LAN Features

- ***Dual LAN ports.*** The CNWR-811P has two (2) 10/100BaseTX Ethernet LAN ports. Normally, the "Hub" port is used to connect the CNWR-811P to your LAN. But if desired, the "PC" port can be used to connect the CNWR-811P directly to your PC, using a standard LAN cable.
- ***DHCP Server Support.*** **D**ynamic **H**ost **C**onfiguration **P**rotocol provides a dynamic IP address to PCs and other devices upon request. The CNWR-811P can act as a **DHCP Server** for devices on your local LAN.
- ***Multi Segment LAN Support.*** LANs containing one or more segments are supported, via the CNWR-811P's built-in static routing table. If NAT (Network Address Translation) is disabled, the CNWR-811P will function as a static router.

Internet Access Features

- ***Shared Internet Access.*** All users on the LAN can access the Internet through the CNWR-811P, using only a single external IP Address. The local (invalid) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation).
- ***ADSL & Cable Modem Support.*** The CNWR-811P has a 10BaseT Ethernet port for connecting an ADSL or Cable Modem. All popular ADSL and Cable Modems are supported.
- ***PPPoE Support.*** Connect to your ISP using PPPoE (PPP over Ethernet), if your ISP uses this method.
- ***Fixed or Dynamic IP Address.*** On the WAN connection, the CNWR-811P supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

Configuration & Management

- ***Easy Setup.*** Use your WEB browser from anywhere on the LAN for configuration.
- ***Remote Management.*** The CNWR-811P can be managed from a workstation anywhere on the LAN, using a WEB browser.

Wireless Features

- ***Standards Compliant.*** The CNWR-811P complies with the IEEE802.11b (DSSS) specifications for Wireless LANs.
- ***Security Features.*** Support for WEP (Wired Equivalent Privacy) and Access Control is included.
- ***Simple Configuration.*** If the default settings are unsuitable, they can be changed quickly and easily.

Advanced Internet Functions

- ***Virtual Servers.*** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- ***User-Defined Virtual Servers.*** Internet users can access non-standard Internet Servers on your LAN by using this feature.
- ***Special Internet Applications.*** Internet applications such as Internet Videoconferencing, Telephony, Games Servers, and other special-purpose Servers are supported.
- ***DMZ.*** One (1) PC on your local LAN can be configured to allow unrestricted 2-way communication with Servers or individual users on the Internet.

Security Features

- ***Configuration Data***. Optional password protection is provided to prevent unauthorized users from modifying the configuration.
- ***Access Control Features***. The LAN Administrator can limit Internet access by individual workstations.
- ***Wireless LAN Security***. WEP (Wired Equivalent Privacy) is supported, as well as Wireless access control via station address.
- ***Firewall Protection.*** All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources. (This protection is lost if NAT is disabled.)

NAT Firewall Protection

The firewall protection provided by the CNWR-811P is an intrinsic side effect of NAT (Network Address Translation). All users on the LAN share a single external IP address. From the external viewpoint, there is no network, only a single device.

For internal users, the CNWR-811P acts as a “transparent proxy server”, translating the multiple internal IP addresses into a single external IP address.

For external requests, any attempt to connect to local resources are blocked. The CNWR-811P will not “reverse translate” from a global IP address to a local IP address.

This type of “natural” firewall provides an impregnable barrier against malicious attacks.

Package Contents

The following items should be included:

- The CNWR-811P Unit
- Wireless PCMCIA Card
- Power Adapter
- Quick Installation Guide
- CD-ROM containing the on-line manual and Print Port Driver.

If any of the above items are damaged or missing, please contact your dealer as soon as possible.

Physical Details

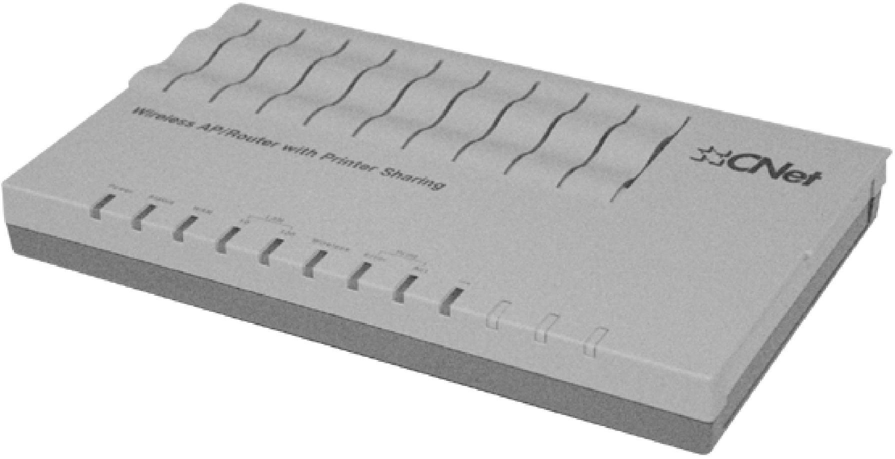


Figure 2: CNWR-811P Multi-Function Wireless A/P Router

LEDs

Power

On - power on

Off - no power

Status (Red)

On - Error condition.

Off - Normal operation

Blinking - This LED blinks during start up.

WAN

On - WAN connection is established.

Flashing - transmitting or receiving data via the WAN port.

LAN: 10

On - LAN connection is using 10BaseT.

Off - No LAN connection.

Flashing - data is being transmitted or received via the LAN port

LAN: 100

On - LAN connection is using 100BaseT.

Off - No LAN connection.

Flashing - data is being transmitted or received via the LAN port

Wireless

On - Wireless connection available; Wireless Access Point is ready for use.

Off - No Wireless connection available.

Flashing - Data is transmitted or received via the Wireless access point. This includes "network traffic" as well as user data.

Print Error

On - Printer error detected.

Off - No printer error detected.

Print Act

On - Connection to printer established.

Off - No connection to printer; printer is Off or Off-line.

Flashing - Data is being transmitted to the printer.

Rear Panel

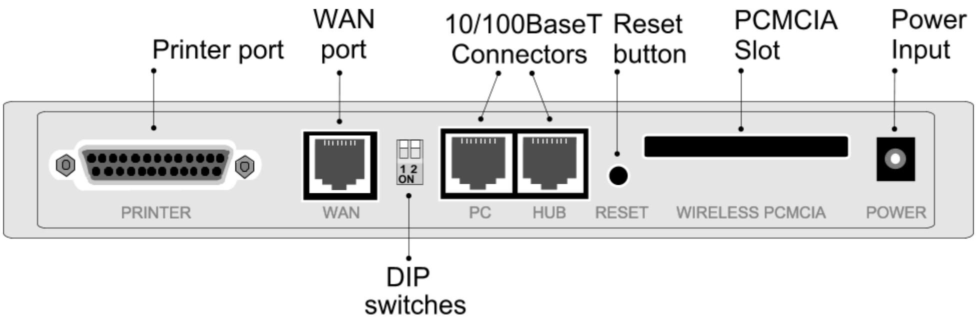


Figure 3: Rear Panel

Printer Port

Standard parallel printer port. If you wish to share a printer, connect it here.

WAN port (10BaseT)

Connect the ADSL or Cable Modem here. If your modem came with a cable, use the supplied cable. Otherwise, use a standard LAN cable.

DIP switches

Refer to the following table..

PC port (10/100BaseTX)

If connecting directly to your PC (no Hub) use this port and a standard LAN cable (RJ45 connectors).

HUB port (10/100BaseTX)

Use a standard LAN cable (RJ45 connectors) to connect this port to a 10BaseT or 100BaseTX hub.

Use EITHER the PC port OR the Hub port. You can NOT use both.

Reset Button

When pressed and released, the Wireless A/P Router will reboot (restart).

This button can also be used to clear ALL data and restore ALL settings to the factory default values.

To restore the factory default values:

1. Power Off
2. Hold the Reset Button down while you Power On.
3. Keep holding the Reset Button for a few seconds, until the RED LED has flashed TWICE.
4. Release the Reset Button. The Wireless A/P Router is now using the factory default values.

PCMCIA slot

Insert the supplied Wireless PCMCIA card into this slot.

- ***Ensure the power is OFF before inserting or removing the PCMCIA Card.***
- ***Do not use any other PCMCIA Card.***

Power port (12V)

Connect the supplied power adapter here.

DIP Switches

DIP Switch Setting	Description
1=off 2=off	Normal Operation
1=off 2=on	DHCP Server function disabled.
1=on 2=off	Used to restore Default IP Address and clear Password (See below)
1=on 2=on	Normal Operation.

Restore Default IP Address and Clear Password

If the CNWR-811P's IP Address or password is lost, the following procedure can be used to recover from this situation.

1. Turn the power to the CNWR-811P OFF.
2. Set DIP switch 1 ON.
3. Turn the power to the CNWR-811P ON.
4. Operate DIP switch 1 in the following sequence (you have 15 seconds to complete the sequence):
    - OFF
    - ON
    - OFF
5. The CNWR-811P will now reset, and the Red Status LED flash. The following changes will have been made. (Other configuration data is unchanged.)
    - *IP Address* set to its default value of 192.168.0.1
    - *Network Mask* set to 255.255.255.0
    - *DHCP Server* is enabled, and will allocate IP Addresses in the range 192.168.0.2 to 192.168.0.51.
    - The password cleared (no password).
6. You can now connect to the CNWR-811P and make any configuration changes required.

Chapter 2
Installation

This Chapter covers the physical installation of the CNWR-811P.

Requirements

- Ethernet LAN (10/100BaseTX) and the TCP/IP protocol.
- For Internet Access, an ADSL or Cable modem, and an Internet Access account with an ISP.
- To use the Wireless Access Point, all Wireless devices must be compliant with the IEEE802.11b specifications.

The CNWR-811P's PCMCIA slot is designed to use ONLY 3.3V PCMCIA Wireless cards.

Procedure

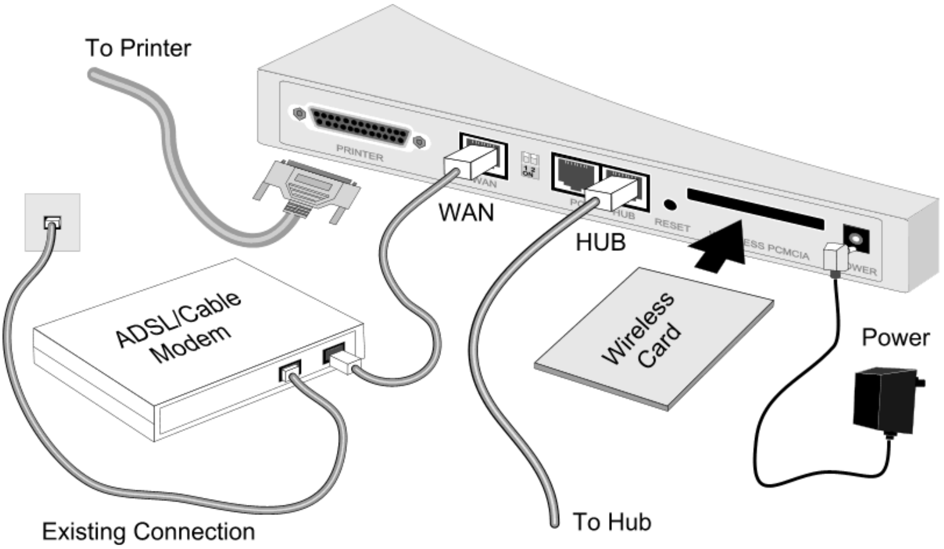


Figure 4: Installation Diagram

1. Choose an Installation Site

Select a suitable physical location. Ensure the CNWR-811P and the ADSL/Cable modem are powered OFF.

2. Insert Wireless PCMCIA card

Ensuring the Wireless PCMCIA card is the right way up, insert it into the slot on the rear. Push it firmly until it clicks into position.

3. Connect LAN Cable

Connect a standard LAN cable from a 10BaseT or 100BaseTX Hub on your LAN to the "HUB" port on the CNWR-811P.

4. Connect WAN Cable

Connect the ADSL or Cable modem to the WAN port on the CNWR-811P. Use the cable supplied with your modem. If no cable was supplied, use a standard LAN cable.

5. Connect Printer Cable

Use a standard parallel printer cable to connect your printer to the Printer port on the CNWR-811P.

6. Power Up

Connect the supplied power adapter and power up.
Use only the power adapter provided.

7. Check the LEDs

- The *Status* LED should flash, then turn Off. If it stays on, there is a hardware error.
- The *Power* LED should be ON.
- One (1) of the LAN LEDs (*10* or *100*) should be ON.
- The *Wireless* LED should be ON.
- If the printer is On and On-line, the *Print Act* LED should be ON.

For more information, refer to LEDs in Chapter 1.

Chapter 3
Configuration

3

This Chapter provides details of the configuration process.

Overview

This chapter describes the procedure for:

- LAN setup
- WAN port configuration for Internet Access
- Wireless access point configuration

PCs on your local LAN may also require configuration. For details, see *Chapter 4 - PC Configuration*.

Other configuration may also be required, depending on which features and functions of the CNWR-811P you wish to use. Use the table below to locate detailed instructions for the required functions.

To Do this:	Refer to:
Configure PCs on your LAN.	Chapter 4: PC Configuration
Learn more about using DHCP on the internal LAN	Chapter 5: DHCP
Configure the CNWR-811P and routers for a LAN which has 1 or more routers.	Chapter 6: Routing
Set a password for the CNWR-811P, or disable NAT (Network Address Translation).	Chapter 7: Options
Use any of the following features: • Special Internet Applications • Virtual Servers • DMZ	Chapter 8: Advanced Internet Features
Limit Internet Access by individual workstations	Chapter 9: Access Control

Note!

Where use of a certain feature requires that PCs or other LAN devices be configured, this is also explained in the relevant chapter.

Configuration Program

The CNWR-811P contains a HTTP server. This enables you to connect to it, and configure it, using your Web Browser.

Most Browsers should work, provided they support HTML tables and forms.

Preparation

Before attempting to configure the CNWR-811P, please ensure that:

- Your PC can establish a physical connection to the CNWR-811P. The PC and the CNWR-811P must be directly connected (using the “PC” port on the CNWR-811P) or on the same LAN segment.
- The CNWR-811P must be installed and powered ON.
- If the CNWR-811P's default IP Address (192.168.0.1) is already used by another device, the other device must be turned OFF until the CNWR-811P is allocated a new IP Address during configuration.

Connecting to the CNWR-811P

To establish a connection from your PC to the device:

1. After installing the CNWR-811P in your LAN, start your PC. If your PC is already running, restart it.
2. Start your WEB browser.
3. In the *Address* box, enter "HTTP://" and the IP Address of the CNWR-811P, as in the following example, which uses the CNWR-811P’s default IP Address:

   ```
   HTTP://192.168.0.1
   ```
4. You should then see the *LAN* screen.

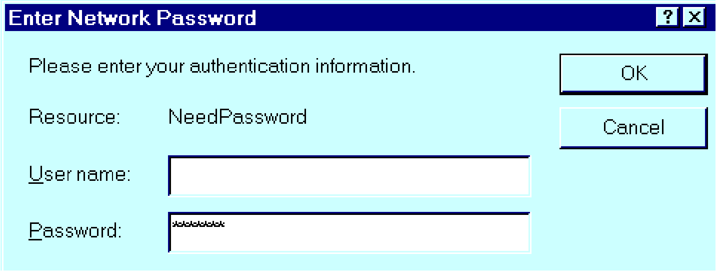
If you can't connect

If the CNWR-811P does not respond, check the following:

- The CNWR-811P is properly installed, LAN connection is OK, and it is powered ON.
- Ensure that your PC and the CNWR-811P are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.0.2 to 192.168.0.254 to be compatible with the CNWR-811P's default IP Address of 192.168.0.1. Also, the *Network Mask* must be set to 255.255.255.0. See *Chapter 4 – PC Configuration* for details on checking your PC’s TCP/IP settings.

Password

If you have assigned a password to the CNWR-811P you will be prompted for the password, as shown below.



Enter Network Password

Please enter your authentication information.

Resource: NeedPassword

User name:

Password: *******

Figure 5: Password Dialog

- Leave the "User Name" blank.
- Enter the password for this device, if one has been set.

If no password has been set, this dialog will not appear.

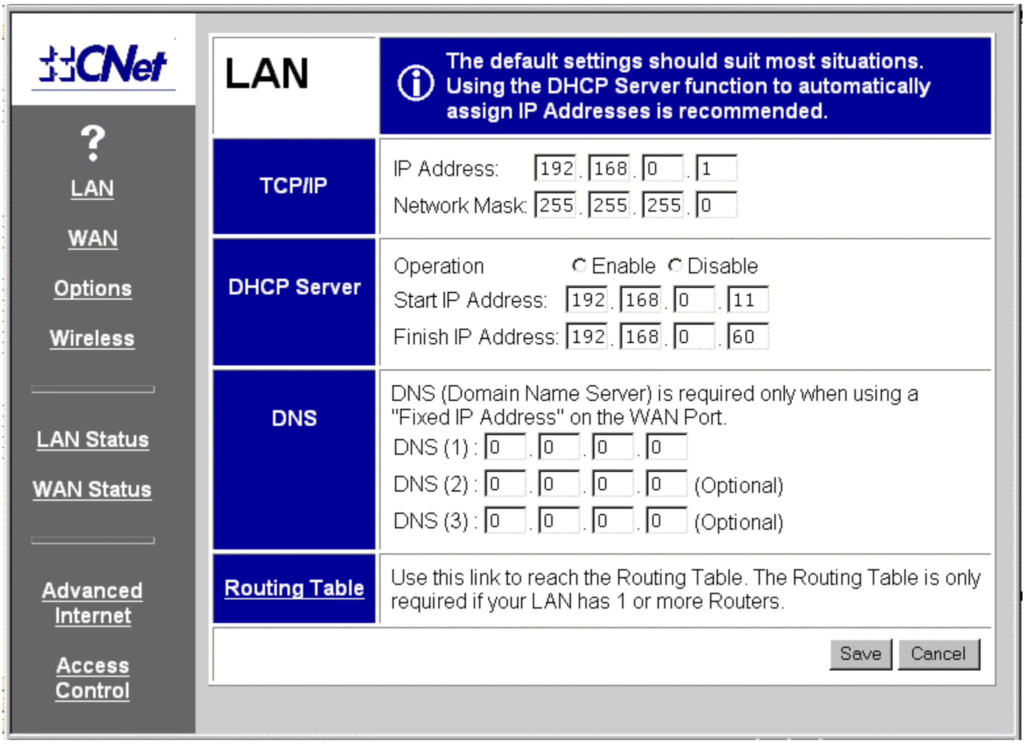
Navigation & Data Input

- Use the menu bar on the left of the screen, and the "Back" button on your Browser, for navigation.
- Changing to another screen without clicking "Save" does NOT save any changes you may have made. You must “Save” before changing screens or your data will be ignored.

ⓘ **On each screen, clicking this icon will display help for that screen.**

LAN Screen

The LAN screen, like the example below, will be displayed when you first connect.



LAN

The default settings should suit most situations. Using the DHCP Server function to automatically assign IP Addresses is recommended.

TCP/IP

IP Address: 192 . 168 . 0 . 1

Network Mask: 255 . 255 . 255 . 0

DHCP Server

Operation ○ Enable ○ Disable

Start IP Address: 192 . 168 . 0 . 11

Finish IP Address: 192 . 168 . 0 . 60

DNS

DNS (Domain Name Server) is required only when using a "Fixed IP Address" on the WAN Port.

DNS (1) : 0 . 0 . 0 . 0

DNS (2) : 0 . 0 . 0 . 0 (Optional)

DNS (3) : 0 . 0 . 0 . 0 (Optional)

Routing Table

Use this link to reach the Routing Table. The Routing Table is only required if your LAN has 1 or more Routers.

Figure 6: LAN Screen

LAN Configuration.

For most users, the default values for these fields should be satisfactory, and no changes will be required.

If your LAN contains an existing Router or Routers, refer to *Chapter 6 - Routing*.

Data – LAN Screen

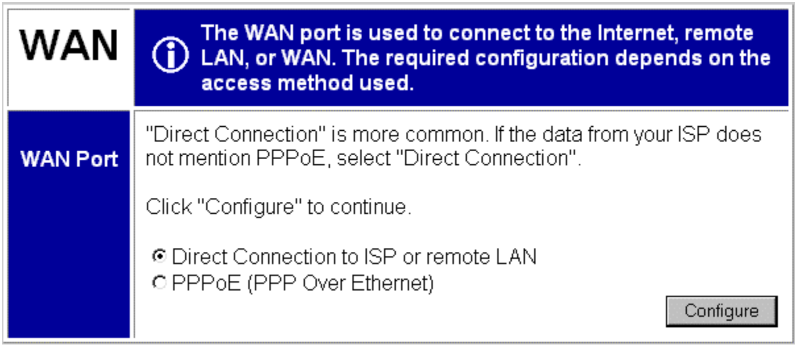
TCP/IP	
IP Address	IP address for the CNWR-811P. Use the default value of 192.168.0.1 unless the address is already in use or your LAN is using a different IP address range. In the latter case, enter an unused IP Address from within the range used by your LAN.
Network Mask	The default value 255.255.255.0 is standard for small (class "C") networks. For other networks, use the Network Mask for the LAN segment to which the CNWR-811P is attached. i.e. the same value as the PCs on that LAN segment.
DHCP Server	
Operation	If Enabled, the CNWR-811P will allocate IP Addresses to PCs on your LAN. The default and recommended value is Enabled. If you are already using a DHCP Server, this setting must be

	DISABLED, and the existing DHCP server must be re-configured. See Chapter 5 for further details.
Start IP Address **Finish IP Address**	The *IP Start Address* and *IP Finish Address* fields set the values used by the DHCP server. This range also determines the number of DHCP clients supported. (Maximum 253.)
DNS (Domain Name Server)	
DNS (Domain Name Server) IP Addresses	If your ISP uses a "Dynamic IP Address", then the DNS is also provided dynamically. Any DNS values entered here will be used instead of the dynamically-obtained DNS addresses. If using a "Fixed IP Address", your ISP should recommend a DNS. Multiple DNS entries should be entered in the order you want them accessed. (The first available DNS will be used.)
Routing Table	
Routing Table	If your LAN contains an existing Router or Routers, refer to *Chapter 6 - Routing*.

WAN Configuration

To configure the WAN port:

- Select ***WAN*** from the menu.
- Select the appropriate connection type (*Direct Connection* or *PPPoE*) on the screen below, then Click the "Configure" button.



WAN

The WAN port is used to connect to the Internet, remote LAN, or WAN. The required configuration depends on the access method used.

WAN Port

"Direct Connection" is more common. If the data from your ISP does not mention PPPoE, select "Direct Connection".

Click "Configure" to continue.

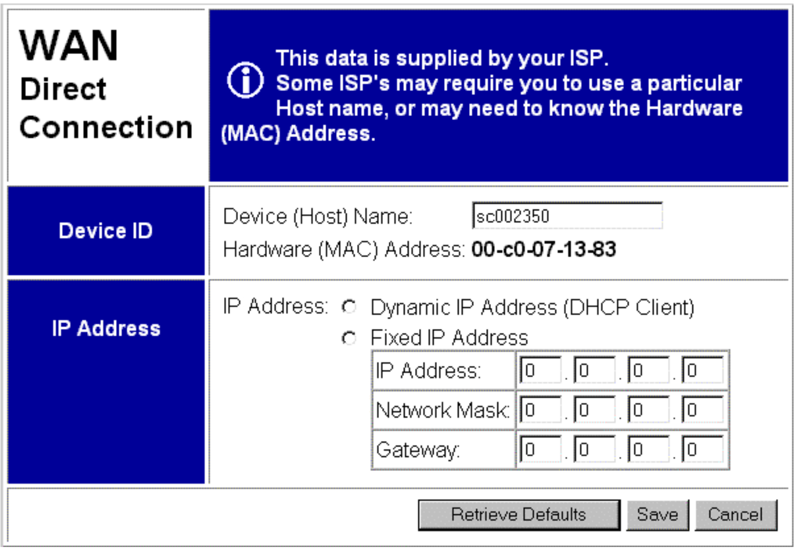
● Direct Connection to ISP or remote LAN
○ PPPoE (PPP Over Ethernet)

Figure 7: WAN Screen

Tip:

If your connection documentation does not refer to *PPPoE*, select ***Direct Connection***.

WAN - Direct Connection



WAN Direct Connection

This data is supplied by your ISP. Some ISP's may require you to use a particular Host name, or may need to know the Hardware (MAC) Address.

Device ID

Device (Host) Name: sc002350
Hardware (MAC) Address: **00-c0-07-13-83**

IP Address

IP Address: ○ Dynamic IP Address (DHCP Client)
○ Fixed IP Address

IP Address:	0	0	0	0
Network Mask:	0	0	0	0
Gateway:	0	0	0	0

Figure 8: WAN - Direct Connection

Data - WAN (Direct Connection)

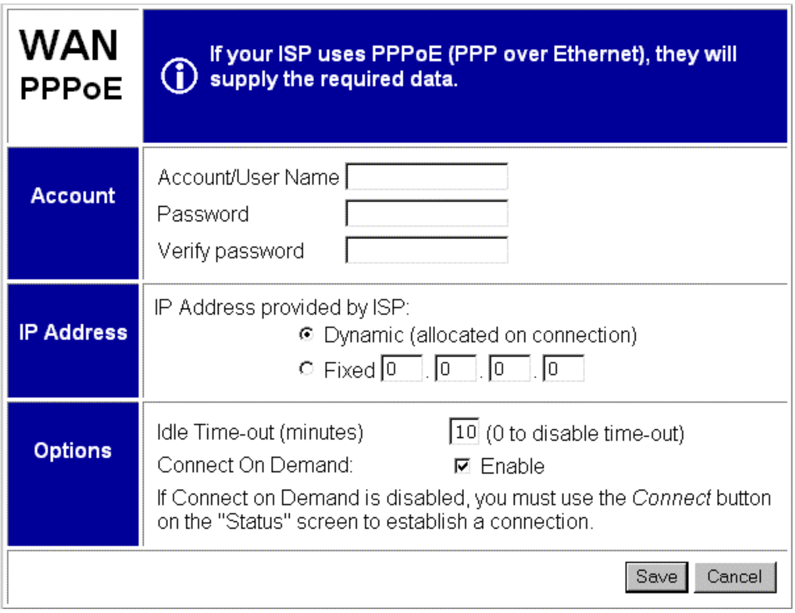
Device ID	
Device (Host) Name	Normally, there is no need to change the default name, but if your ISP requests that you use a particular "Hostname", enter it here. This name will be provided to, and recorded by, the remote DHCP Server.

Hardware (MAC) Address	Also called *Network Adapter Address* or *Physical Address*. Provide this value to your ISP if requested. If you did not provide this value when first connected, there is no need to provide it now.
IP Address	
Dynamic IP Address (DHCP Client)	Leave this enabled if you want your ISP to allocate an IP Address to the CNWR-811P upon connection.
Fixed IP Address	Select this if using a fixed IP Address. If this option is selected, the following data must be entered. • **IP Address**. If connecting to an ISP, this is the address allocated by the ISP. If connecting to another LAN, this must be a valid address on the external LAN. • **Network Mask** This must be compatible with the IP Address above • **Gateway IP Address** The address of the router or gateway, either on the external LAN, or supplied by your ISP. **DNS IP Address** At least 1 DNS IP Address is required, and should be provided by your ISP. DNS settings are on the LAN screen.
Buttons	
Retrieve Defaults	Get the default *Device Name* and clear the other items. No changes are made to the configuration until you click the *Save* button.
Save	Save any data you have entered on this screen. Remember to save before changing to another screen.
Cancel	Cancel any data you have entered since the last "Save" operation.

Note:

If using *Dynamic IP Address*, the IP Address, Network Mask, and Gateway fields may display the values obtained dynamically.

WAN - PPPoE



WAN PPPoE

If your ISP uses PPPoE (PPP over Ethernet), they will supply the required data.

Account

Account/User Name [ ]

Password [ ]

Verify password [ ]

IP Address

IP Address provided by ISP:

● Dynamic (allocated on connection)

○ Fixed 0 . 0 . 0 . 0

Options

Idle Time-out (minutes) 10 (0 to disable time-out)

Connect On Demand: ☑ Enable

If Connect on Demand is disabled, you must use the *Connect* button on the "Status" screen to establish a connection.

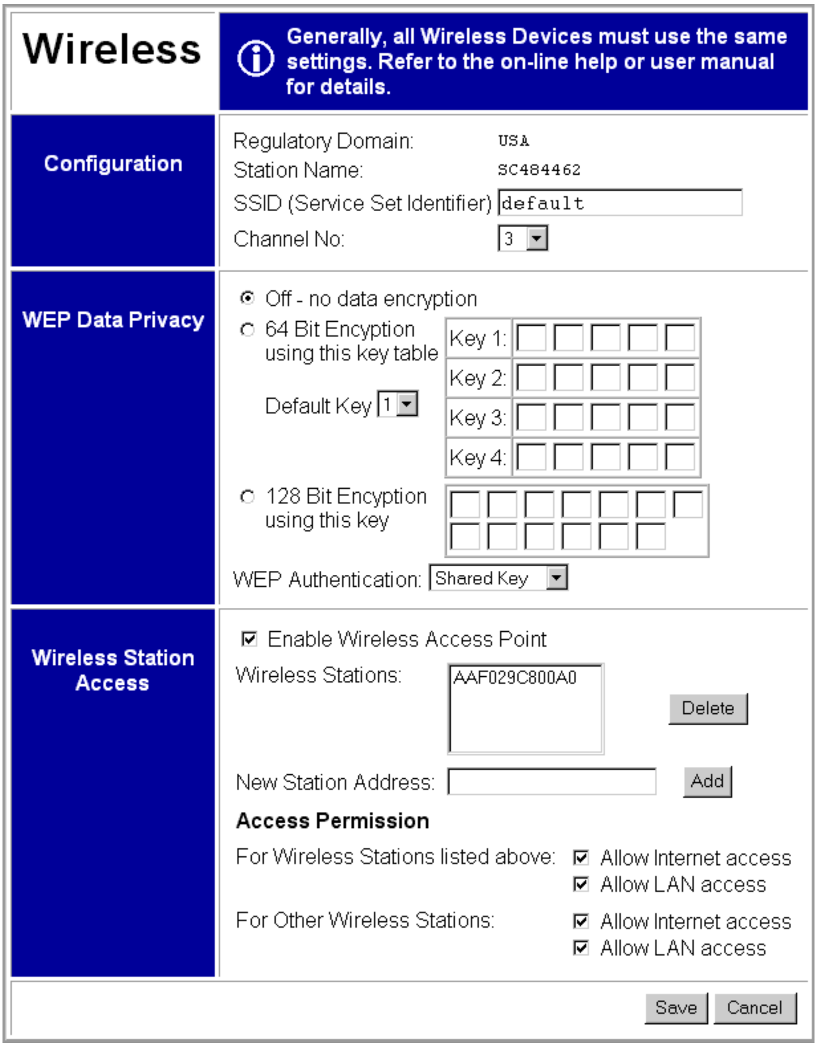
Figure 9: WAN Port - PPPoE

Data – WAN (PPPoE)

Account	
Account/User Name	The name of the Internet account provided by your ISP.
Password & Verify	Enter the password for the above account. Re-enter the password in the *Verify* field, to ensure it is correct.
IP Address	
IP Address provided by ISP	Normally, this is *Dynamic*; use this setting if your ISP did not provide an IP Address. If your ISP did provide an IP Address, select *Fixed* and enter the value they provided.
Options	
Idle Time-out	If an connection is inactive for longer than this time period, it will be terminated. If zero (0), then the connection will never be terminated.
Connect on Demand	Normally, this should be Enabled. If disabled, you must use the *Connect* button on the ***Status*** screen to establish a connection.
Buttons	
Save	Save any data you have entered on this screen. Remember to save before changing to another screen.
Cancel	Cancel any data you have entered since the last "Save" operation.

Wireless Configuration

The CNWR-811P settings must match the other Wireless stations. An example ***Wireless*** screen is shown below.



Wireless

ⓘ Generally, all Wireless Devices must use the same settings. Refer to the on-line help or user manual for details.

Configuration

Regulatory Domain: USA
Station Name: SC484462
SSID (Service Set Identifier) default
Channel No: 3

WEP Data Privacy

● Off - no data encryption
○ 64 Bit Encyption using this key table
Default Key 1
Key 1: □ □ □ □ □
Key 2: □ □ □ □ □
Key 3: □ □ □ □ □
Key 4: □ □ □ □ □
○ 128 Bit Encyption using this key
□ □ □ □ □ □ □
□ □ □ □ □ □
WEP Authentication: Shared Key

Wireless Station Access

☑ Enable Wireless Access Point
Wireless Stations: AAF029C800A0
Delete
New Station Address:
Add

Access Permission

For Wireless Stations listed above: ☑ Allow Internet access ☑ Allow LAN access
For Other Wireless Stations: ☑ Allow Internet access ☑ Allow LAN access

Save Cancel

Figure 10: Wireless Screen

Data – Wireless Screen

Configuration	
Regulatory Domain	It is illegal to use this device in any location outside of the regulatory domain.
Station name	This is the same as the *Device (Host) Name* on the WAN screen. On your PC, some Wireless status screens may display this name as the Access Point in use.
SSID (ESSID)	To communicate, all Wireless stations MUST use the same SSID/ESSID. The default value is `default` **Note! The SSID is case sensitive.**

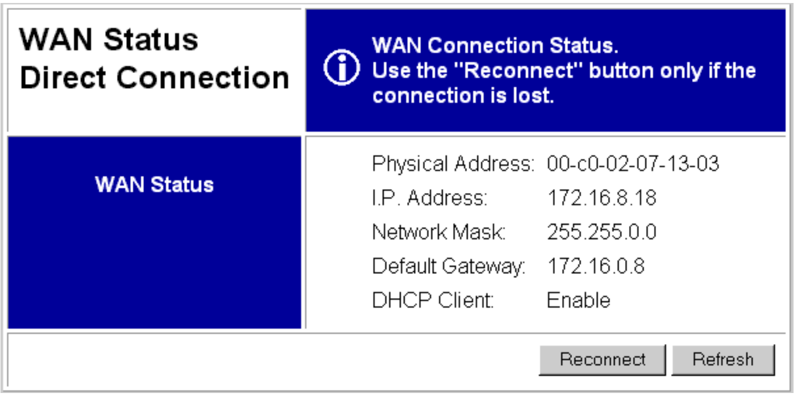
Channel No.	Select the value you wish to use on your Wireless LAN. If you experience lost connections and/or slow data transfers you may need to experiment with different channels to see which is the best.
WEP Data Privacy	
Off	If OFF (default), data is NOT encrypted before being transmitted.
64 Bit Encryption	• If selected, data is encrypted, using the default key, before being transmitted. The receiving station must be set to 64 Bit Encryption, and have the same Key value in the same position in its key table. Otherwise, it will not be able to decrypt the data. • **Default Key** Select the key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only. • **Key Table** • This table is used when Encrypting and Decrypting data. All stations, including this Access Point, always transmit data encrypted using their default key. The key number (1, 2, 3, 4) is also transmitted. The receiving station will use the key number (1, 2, 3, 4) to determine which key value to use for decryption. If the key value does not match the transmitting station, decryption will fail. • The easiest way to ensure there are no problems is to have every Station, including the Access Point, use the same key table (all entries identical). Then, it does not matter which key is used as the default key.
128 Bit Encryption	• If selected, data is encrypted using the key before being transmitted. The receiving station must be set to use 128 Bit Encryption, and have the same Key value. Otherwise, it will not be able to decrypt the data. • **Key** Enter the key value you wish to use. Other stations must have the same key.
WEP Authentication	Select the appropriate value - "Open System" or "Shared Key". Check your Wireless card's documentation to see what method to use. Some Wireless cards do not support both methods.
Wireless Station Access	
Enable Wireless Access Point	• If enabled (default), this device can act as a Wireless Access Point. • If not enabled, no Wireless stations can use this device as a Wireless Access Point.
Existing Stations	• This lists the Wireless stations you have entered. If you have not entered any stations, this list will be empty. • To delete an entry, select it, and click the "Delete" button. Multiple entries may be selected by hold down the CTRL key while selecting. (On the Macintosh, use SHIFT instead of CTRL.)

New station Address	• Use this field to add a new station to the list. Just enter its address here, and click the "Add" button. • Use the software supplied with your Wireless unit to determine its address. The address consists of 12 letters (A..F) and digits (0..9) like this example: `10F810A81091` The address may be shown with separators (: or -) between each pair of characters. Do NOT enter the separators (: or -) in this field.
Access Permission	• **For Wireless Stations listed above** This setting determines what type of access is available to Wireless stations whose address has been entered in the "Wireless Stations" list. • **For Other Wireless Stations** This setting determines what type of access is available to Wireless stations whose address is NOT in the "Wireless Stations" list. • For either category, if neither "Internet" nor "LAN" access is enabled, Wireless stations are unable to use this Access Point.
Buttons	
Delete	**Delete** will delete the selected entry or entries in the list.
Add	**Add** will add the *New Station* data to the list.
Save	**Save** will save the other data on the screen. This has no effect on the contents of the ***Wireless Stations*** list.

WAN Status

Clicking ***WAN Status*** on the menu bar will take you to the ***WAN Status*** screen. The screen shown will depend on whether you are using a **Direct Connection** or **PPPoE**.

WAN Status – Direct Connection



WAN Status
Direct Connection

WAN Connection Status.
Use the "Reconnect" button only if the connection is lost.

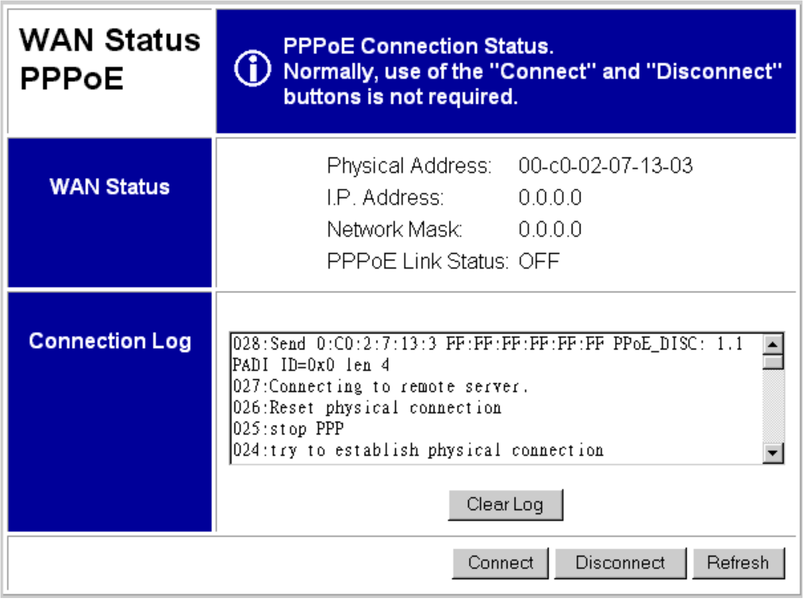
Physical Address: 00-c0-02-07-13-03
I.P. Address: 172.16.8.18
Network Mask: 255.255.0.0
Default Gateway: 172.16.0.8
DHCP Client: Enable

Figure 11: WAN Status – Direct Connection

Data

WAN Status	
Physical Address	The "Hardware" address of this device, as seen by other devices on the WAN.
IP Address	The IP Address of this device, as seen by devices on the WAN. (This device has 2 IP Addresses; one for the local LAN, and another for the WAN port.)
Network Mask	The Network Mask for the above IP Address.
Default Gateway	IP address of the Router/Gateway on the WAN port.
DHCP Client	Displays "Enabled" or "Disabled", indicating whether this device is acting as a DHCP client on the external LAN or WAN.
Buttons	
Reconnect	Use this button if the connection seems to have been lost, and no data is being transferred. (This button has no effect unless acting as a DHCP Client.)
Refresh	Update the data on screen.

WAN Status – PPPoE



WAN Status PPPoE

PPPoE Connection Status.
Normally, use of the "Connect" and "Disconnect" buttons is not required.

Physical Address: 00-c0-02-07-13-03
I.P. Address: 0.0.0.0
Network Mask: 0.0.0.0
PPPoE Link Status: OFF

```
028:Send 0:C0:2:7:13:3 FF:FF:FF:FF:FF:FF PPoE_DISC: 1.1
PADI ID=0x0 len 4
027:Connecting to remote server.
026:Reset physical connection
025:stop PPP
024:try to establish physical connection
```

Figure 12: WAN Status – PPPoE

Status Data

WAN Status	
Physical Address	The "Hardware" address of this device, as seen by other devices on the WAN.
IP Address	The IP Address of this device, as seen by devices on the WAN. (This device has 2 IP Addresses; one for the local LAN, and another for the WAN port.)
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.
PPPoE Link Status	This indicates whether or not the connection is currently established. If the connection does not exist, the ***Connect*** button can be used to establish a connection. If the connection currently exists, the ***Disconnect*** button can be used to break the connection.
Connection Log	
Log Data	The Connection Log shows status messages relating to the existing connection. The most common messages are listed in the following table.
Buttons	
Connect	If not connected, establish a connection to your ISP
Disconnect	If connected to your ISP, hang up the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.

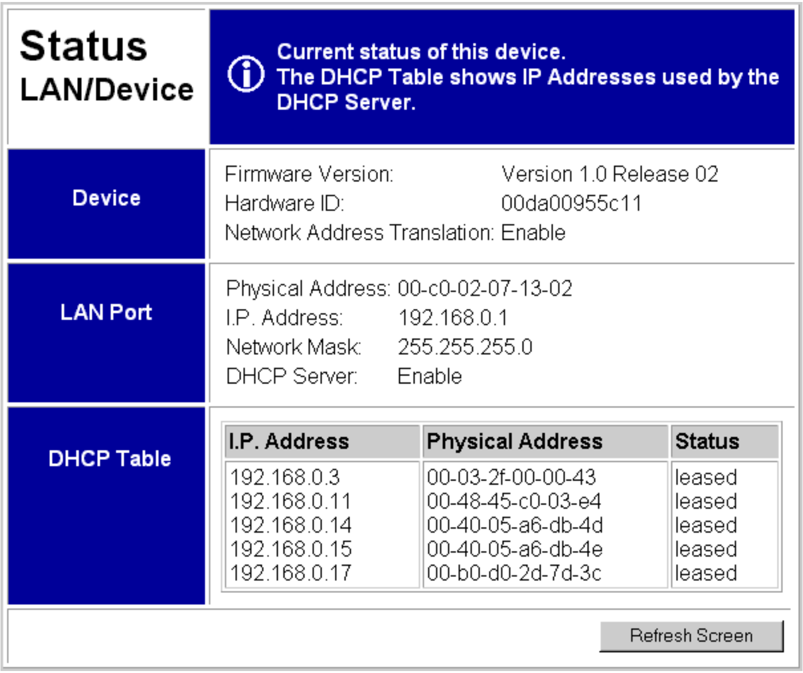
Refresh	Contact this device and update the Log data.

Connection Log Messages

Message	Description
Connect on Demand	Connection attempt has been triggered by the "Connect on Demand" setting.
Manual connection	Connection attempt started by the "Connect" button.
Reset physical connection	Preparing line for connection attempt.
Connecting to remote server	Attempting to connect to the the ISP's server.
Remote Server located	ISP's Server has responded to connection attempt.
Start PPP	Attempting to login to ISP's Server and establish a PPP connection.
PPP up successfully	Able to login to ISP's Server and establish a PPP connection.
Idle time-out reached	The connection has been idle for the time period specified in the "Idle Time-out" field. The connection will now be terminated.
Disconnecting	The current connection is being terminated, due to either the "Idle Time-out" above, or "Disconnect" button being clicked.
Error: Remote Server not found	ISP's Server did not respond. This could be a Server problem, or a problem with the link to the Server.
Error: PPP Connection failed	Unable to establish a PPP connection with the ISP's Server. This could be a login problem (name or password) or a Server problem.
Error: Connection to Server lost	The existing connection has been lost. This could be caused by a power failure, link failure, or Server failure.
Error: Invalid or unknown packet type	The data received from the ISP's Server could not be processed. This could be caused by data corruption (from a bad link), or the Server using a protocol which is not supported by this device.

LAN/Device Status

The ***LAN Status*** link on the menu will result in a screen like the example below.



Status
LAN/Device

Current status of this device.
The DHCP Table shows IP Addresses used by the DHCP Server.

Device

Firmware Version: Version 1.0 Release 02
Hardware ID: 00da00955c11
Network Address Translation: Enable

LAN Port

Physical Address: 00-c0-02-07-13-02
I.P. Address: 192.168.0.1
Network Mask: 255.255.255.0
DHCP Server: Enable

DHCP Table

I.P. Address	Physical Address	Status
192.168.0.3	00-03-2f-00-00-43	leased
192.168.0.11	00-48-45-c0-03-e4	leased
192.168.0.14	00-40-05-a6-db-4d	leased
192.168.0.15	00-40-05-a6-db-4e	leased
192.168.0.17	00-b0-d0-2d-7d-3c	leased

Figure 13: Status Screen

Data – LAN/Device Status

Device	
Firmware Version	Version of the firmware (embedded software, including this program) which is currently installed.
Hardware ID	The hardware ID of this device, used by the manufacturer.
Network Address Translation	This will display "Enabled" (NAT is On) or "Disabled" (NAT is Off)
LAN Port	
Physical Address	The "Hardware" address of this device, as seen by other devices on the Internal LAN.
IP Address	The IP Address of this device, as seen by other devices on the Internal LAN.
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.
DHCP Server	This shows the status of the DHCP Server function. The value will be "Enabled" or "Disabled".
DHCP Table	
IP Address	The IP Address which has been allocated by the DHCP server to the other device.
Physical Address	The Physical Address (Hardware Address) of the device which has been allocated a IP Address.

Status	Possible Status values are "Leased" (the IP Address is allocated to the device shown) or "Reserved" (the IP Address is not available).

Note:

The DHCP table will be empty unless the DHCP Server function is being used. If not empty, this table lists the devices on the LAN which have been allocated IP Addresses by the DHCP server function.

Chapter 4
PC Configuration

4

This Chapter details the PC Configuration required on the local ("Internal") LAN.

Overview

For each PC, the following may to be configured:

- TCP/IP network settings
- Internet Access configuration
- Network printer
- Wireless configuration

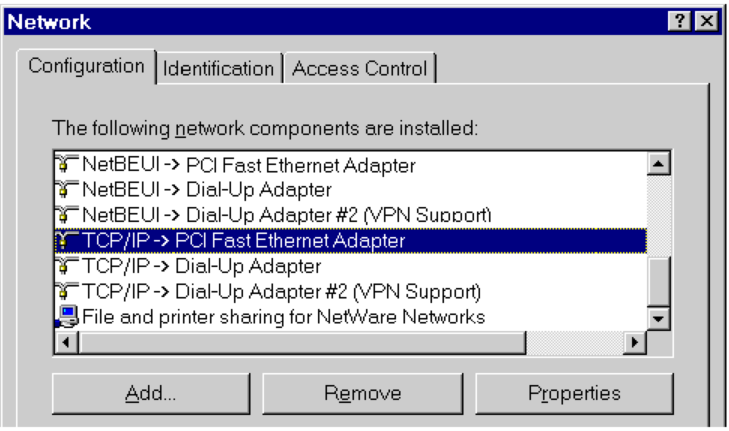
TCP/IP Settings

If using the default CNWR-811P settings, and the default Windows 95/98 TCP/IP settings, no changes need to be made.

- By default, the CNWR-811P will act as a DHCP Server, automatically providing a suitable IP Address to each PC when the PC boots.
- The default Windows 95/98 TCP/IP setting is to act as a DHCP client.

To check your PC's TCP/IP Settings:

1. Select *Control Panel - Network*. You should see a screen like the following:

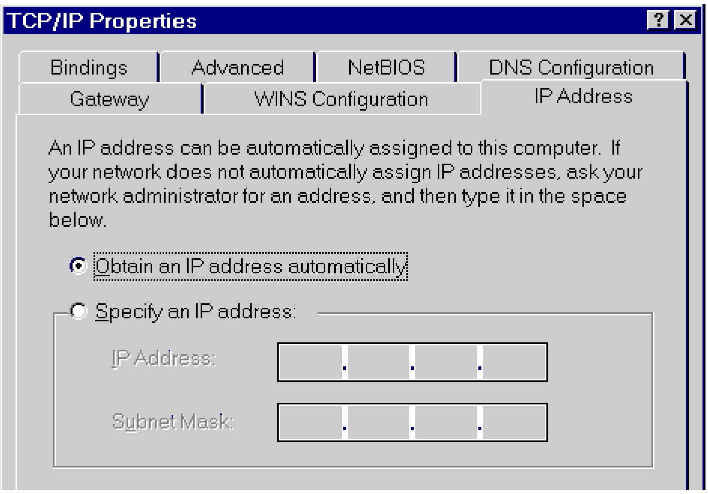


The following network components are installed:

NetBEUI -> PCI Fast Ethernet Adapter
NetBEUI -> Dial-Up Adapter
NetBEUI -> Dial-Up Adapter #2 (VPN Support)
TCP/IP -> PCI Fast Ethernet Adapter
TCP/IP -> Dial-Up Adapter
TCP/IP -> Dial-Up Adapter #2 (VPN Support)
File and printer sharing for NetWare Networks

Figure 14: Network Configuration

2. Select the *TCP/IP* protocol for your network card.
3. Click on the *Properties* button. You should then see a screen like the following.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

Figure 15: IP Address (Win 95)

Ensure your TCP/IP settings are correct, as follows:

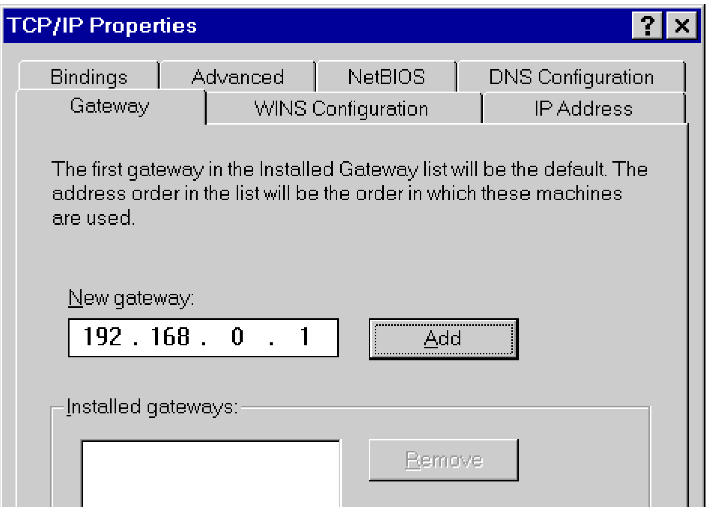
Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows settings.

Restart your PC to ensure it obtains an IP Address from the CNWR-811P.

Using "Specify an IP Address"

- If your PC is already configured, do NOT change the settings on the IP Address tab shown in Figure 15 above.
- On the *Gateway* tab, enter the CNWR-811P's IP address in the *New Gateway* field and click *Add*. Your LAN administrator can advise you of the IP Address they assigned to the CNWR-811P.



The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

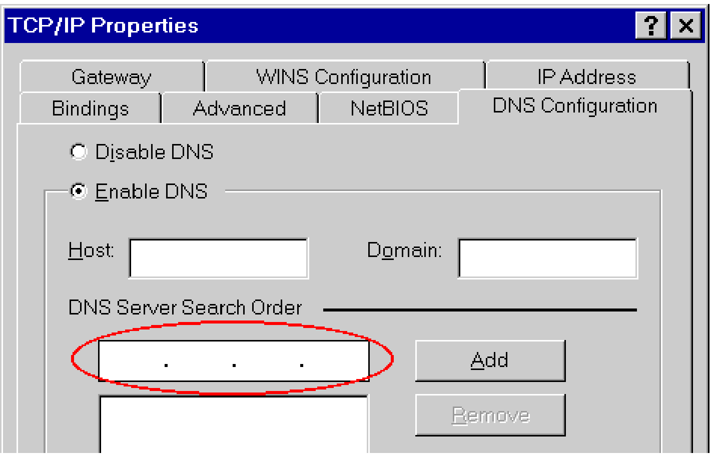
New gateway:

192 . 168 . 0 . 1

Installed gateways:

Figure 16: Gateway Tab (Win 95/98)

- On the *DNS Configuration* tab, ensure *Enable DNS* is selected. If the *DNS Server Search Order* list is empty, enter the DNS address provided by your ISP in the fields beside the *Add* button, then click *Add*.



○ Disable DNS

● Enable DNS

Host:

Domain:

DNS Server Search Order

. . .

Figure 17: DNS Tab (Win 95/98)

Note!

If your LAN has a Router, the LAN Administrator must re-configure the Router itself. Refer to *Chapter 6 - Routing* for details.

Internet Access Configuration

If you are using the CNWR-811P for Internet access:

- Ensure that the DSL modem, Cable modem, or other permanent connection is functional.
- Use the following procedure to configure your Browser to access the Internet via the LAN, rather than by a Dial-up connection.

1. Select *Start Menu - Settings - Control Panel - Internet Options*.
2. Select the *Connection* tab, and click the *Setup* button.
3. Select "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" and click "Next".
4. Select "I connect through a local area network (LAN)" and click "Next".
5. Ensure all of the boxes on the following *Local area network Internet Configuration* screen are **unchecked**.
6. Check the "No" option when prompted “Do you want to set up an Internet mail account now?”.
7. Click "Finish" to close the Internet Connection Wizard.
8. Then simply use your Browser, FTP client, or other Internet client to connect to the desired Internet site.

Accessing AOL

To access AOL (America On Line) through the CNWR-811P, the *AOL for Windows* software must be configured to use TCP/IP network access, rather than a dial-up connection. The configuration process is as follows:

- Start the *AOL for Windows* communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.
- Click the *Setup* button.
- Select *Create Location*, and change the location name from "New Locality" to "CNWR-811P".
- Click *Edit Location*. Select *TCP/IP* for the *Network* field. (Leave the *Phone Number* blank.)
- Click *Save*, then *OK*.
  Configuration is now complete.
- Before clicking "Sign On", always ensure that you are using the "CNWR-811P" location.

Printing Setup

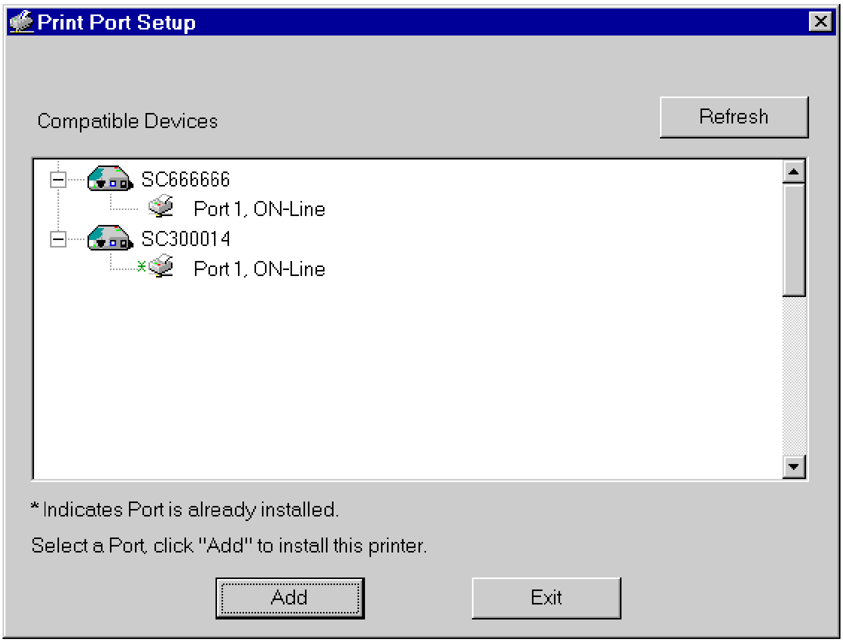
The CNWR-811P provides printing support for 2 methods of printing from Windows:

- **Print Port Driver.** After installing the Print Port Driver, Windows users can print directly to the CNWR-811P. Print jobs are spooled (queued) on each PC.
  The supplied Print Port Driver supports Windows 95/98, Windows ME, Windows NT4.0, and Windows 2000.
- **LPD/LPR Printing.** If using Windows NT 4.0 Server or Windows 2000 Server, LPD/LPR printing can be used. No software needs to be installed on either the Windows Server or each client PC. Print jobs will be spooled (queued) on the Windows Server, and can be managed using the standard Windows Server tools.

Print Port Driver Setup

The following procedure is for Windows 95/98, Windows ME, Windows NT4.0, and Windows 2000.

1. Insert the supplied CD-ROM into your drive. If the setup program does not start automatically, run SETUP.EXE in the root folder.
2. At the *Setup Type* screen, select the correct model.
3. At the *Select Components* screen, select the ***Print Port Driver*** option.
4. Follow the prompts to complete the installation.
5. The *Print Port Setup* will then run, and the following screen will be displayed.



SC666666
Port 1, ON-Line
SC300014
Port 1, ON-Line

* Indicates Port is already installed.

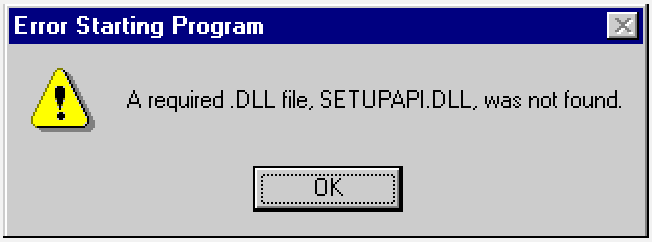
Select a Port, click "Add" to install this printer.

Figure 18: Print Port Setup

6. Select the desired device and port, and then click the "Add" button.

Note!

If you see the following error message, either install Internet Explorer 4 or later, or follow the procedure in the "Trouble Shooting - Printing" section of Appendix A.



Error Starting Program

A required .DLL file, SETUPAPI.DLL, was not found.

7. A pop-up message will inform you if the port has been created successfully, and then the Windows *Add Printer* wizard will start.
   - Select the correct Printer Manufacturer and Model, or use the "Have Disk" option if appropriate.
   - If desired, change the Printer name so it indicates the device used (e.g. HP2100 on SCA43600)
   - If prompted about Sharing, do NOT enable Sharing.
8. Installation is now complete. You can now print using this printer.
   - To install additional Printers, repeat steps 6 and 7.
   - Use the ***Start*** menu to run this program in future. The default installation is *Start - Programs - Broadband Internet Router - Add Port*.

Management

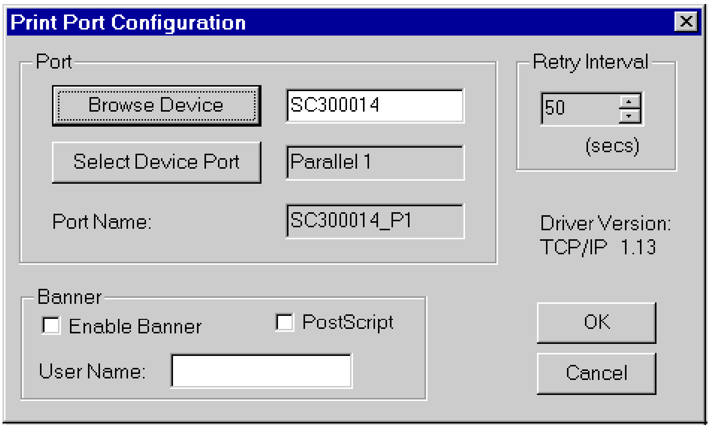
- Print jobs can be managed like any Windows printer. Open the *Printers* folder (*Start - Settings - Printers*) and double-click any printer to see the current print jobs.
- If the printer attached to the CNWR-811P is changed, just run this program again, and select the correct printer.
- To delete a port created by this setup program, use the Windows *Delete Port* facility:
  - Right-click any printer in the *Printers* folder, and select *Properties*.
  - Locate the *Delete Port* button. This button is on the *Details* or *Ports* tab, depending on your version or Windows.
- If the CNWR-811P's IP Address is changed, and you can no longer print, delete the port (see procedure above) and re-install it.

Port Options

The options for the *Print Port Driver* are accessed via the Windows *Port Settings* button.

Use *Start* - *Settings* - *Printers* to open the Printers folder, then right-click the Printer, and select *Properties*. The *Port Settings* button is on the *Details* or *Port* tab, depending on your version of Windows.

An example screen is shown below:



SC300014

Parallel 1

Port Name: SC300014_P1

50

Driver Version:
TCP/IP 1.13

□ Enable Banner

□ PostScript

User Name:

Figure 19: Print Port Configuration

Items shown on this screen are as follows:

Port	If desired, click *Browse* to select a different device. (The *Select Device Port* button is provided to allow this software to work with multi-port models.) The *Port Name* is shown in the Printer's *Properties*.
Banner	Check this option to print a banner page before each print job. • If using a PostScript Printer, check the *PostScript* box. • The *User Name* will be printed on the banner page.
Retry Interval	Sets how often Windows will poll the CNWR-811P to establish a connection when the printer is busy. Increase this value if you get too many warning messages.

LPD/LPR Printing

LPD/LPR printing can be used with Windows NT 4.0 Server or Windows 2000. No software needs to be installed.

Windows NT 4.0 Server Configuration

To use LPD printing, **Microsoft TCP/IP Printing** must be installed and enabled. This can be checked using *Start-Settings-Control Panel-Network - Services*.

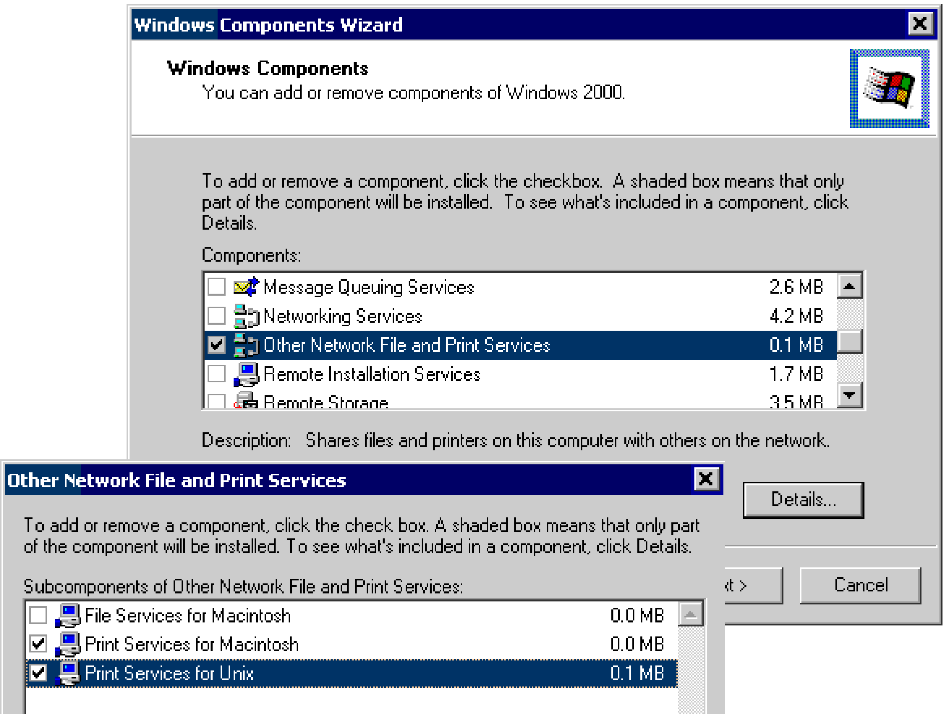
To install LPD printing using the CNWR-811P, follow this procedure:

1. Go to *Start-Settings-Printer* and invoke the *Add Printer* wizard.
2. When prompted with "This printer will be managed by..", select **My Computer** and click Next.
3. Select **Add Port…**, then select **LPR Port** and click **New Port**.
4. In the Dialog requesting *Name of Address of server providing lpd*, enter the IP address of the CNWR-811P.
5. For *Name of printer or print queue on that server*, enter L1
6. Click OK. When returned to the Printer Ports window, simply select *Close* and then install your printer driver as usual.
7. When prompted whether or not the printer will be shared, select the **Sharing** radio button.
8. In the *Shared* dialog box, enter the shared printer name. The shared name is how other users will see this printer. You should advise client PCs of the Server name and this printer name.
9. Click OK to save and exit.

Windows 2000 Server Configuration

The *LPD/LPR Port* is not enabled by default. To enable it, use this procedure:

1. In *Control Panel*, select *Add/Remove Programs*, then *Windows Components*.
2. Select *Other Network File and Print Services*, then click the *Details* button.



Windows Components Wizard

Windows Components
You can add or remove components of Windows 2000.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

□	Message Queuing Services	2.6 MB
□	Networking Services	4.2 MB
☑	Other Network File and Print Services	0.1 MB
□	Remote Installation Services	1.7 MB
□	Remote Storage	3.5 MB

Description: Shares files and printers on this computer with others on the network.

Other Network File and Print Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Other Network File and Print Services:

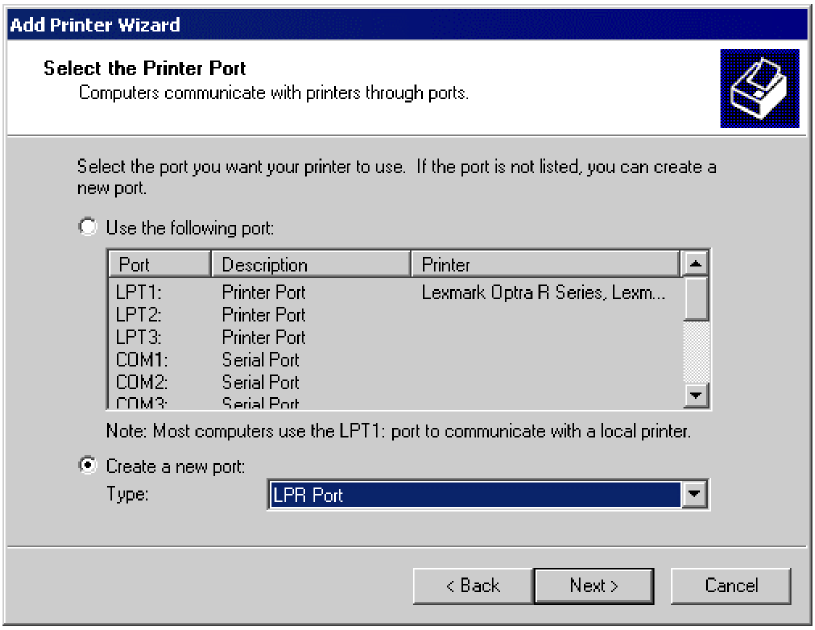
□	File Services for Macintosh	0.0 MB
☑	Print Services for Macintosh	0.0 MB
☑	Print Services for Unix	0.1 MB

Figure 20: Adding LPD/LPR Port (Win 2000)

3. Enable *Print Services for Unix*, and click OK.
4. Click *Next* and complete the Wizard.

Adding the Printer

1. Open your *Printers* folder, and start the *Add Printer* Wizard.
2. When prompted, select *Local Printer*.
3. On the *Select the Printer Port* screen, select *LPR Port*, as shown below. Click *Next* to continue.



Add Printer Wizard

Select the Printer Port

Computers communicate with printers through ports.

Select the port you want your printer to use. If the port is not listed, you can create a new port.

○ Use the following port:

Port	Description	Printer
LPT1:	Printer Port	Lexmark Optra R Series, Lexm...
LPT2:	Printer Port	
LPT3:	Printer Port	
COM1:	Serial Port	
COM2:	Serial Port	
COM3:	Serial Port	

Note: Most computers use the LPT1: port to communicate with a local printer.

● Create a new port:

Type: LPR Port

Figure 21: Windows 2000: Select Port

4. In the Dialog requesting *Name of Address of server providing lpd*, enter the IP address of the CNWR-811P.
5. For *Name of printer or print queue on that server*, enter L1.
6. Click OK, and then *Next*, and continue the Wizard.
7. At the *Select Sharing* screen, select the Radio Button for *Share As*, and enter the shared printer name. The shared name is how other users will see this printer. You should advise client PCs of the Server name and this printer name.
8. Complete the *Add Printer* wizard.

Client PC Setup for LPD/LPR Printing

After configuring the Windows Server, client PCs on the LAN can install the new printer.

The following procedure is for Windows 95/98/ME, Windows NT4.0, and Windows 2000 workstation.

1. Open your *Printers* folder, and start the *Add Printer* Wizard.
2. When prompted, select *Network Printer*.
3. When prompted for *Network Path or Queue Name*, click the *Browse* button, and locate the Server and Printer which your Network Administrator advised you to use.
4. Click OK, then *Next*.
5. Select the correct printer Manufacturer and Model, as advised by your Network Administrator, and click *Next*.
6. Follow the prompts to complete the Wizard.
7. The new printer will be listed with any other installed printers, and may be selected when printing from any Windows application.

Macintosh Configuration

The CNWR-811P currently does not support printing from the Macintosh, but you can access the Internet via the CNWR-811P. The procedure is as follows.

1. Open the TCP/IP Control Panel.
2. Select *Ethernet* from the *Connect via* pop-up menu.
3. Select *Using DHCP Server* from the *Configure* pop-up menu. The DHCP Client ID field can be left blank.
4. Close the TCP/IP panel, saving your settings.

Note:

If using manually assigned IP addresses instead of DHCP, the only change required is to set the *Router Address* field to the CNWR-811P's IP Address.

Wireless Configuration

To use the Wireless Access Point in the CNWR-811P, each Wireless Station must have compatible settings, as follows:

Mode	The mode must be set to ***Infrastructure***.
SSID (ESSID)	This must match the value used on the CNWR-811P. The default value is **`default`** **Note! The SSID is case sensitive.**
WEP	By default, WEP on the CNWR-811P is **disabled**. • If WEP remains disabled on the CNWR-811P, all stations must have WEP disabled. • If WEP was enabled on the CNWR-811P, each station must use the same WEP settings as the CNWR-811P.

Chapter 5

DHCP

This Chapter covers the use of DHCP, using either an existing DHCP Server or the CNWR-811P's DHCP Server function.

Overview

If your LAN does not use DHCP, and you do not wish to use DHCP, you can ignore this chapter.

What DHCP Does

A DHCP (Dynamic Host Configuration Protocol) **server** allocates a valid IP address to a DHCP **client** (PC or device) upon request.

- The client request is made when the client device boots.
- The DHCP Server provides the *Gateway* and *DNS* addresses to the client, as well as allocating an IP Address.
- Windows 95/98/ME include all the software required to act as a DHCP **client**. This is the default Windows setting for TCP/IP. However, Windows uses the term *Obtain an IP Address automatically* instead of "DHCP Client".
- The CNWR-811P can act as a **DHCP server**.

Using the CNWR-811P's DHCP Server

This is the default setting. The DHCP Server settings are on the ***LAN*** screen. On this screen, you can:

- Enable or Disable the CNWR-811P's *DHCP Server* function.
- Set the range of IP Addresses allocated to PCs by the DHCP Server function.

Note!

You can assign Fixed IP Addresses to some devices while using DHCP, provided that the Fixed IP Addresses are NOT within the range used by the DHCP Server.

Using another DHCP Server

You can only use one (1) DHCP Server. If you wish to use another DHCP Server, rather than the CNWR-811P's, the following procedure is required.

1. Disable the DHCP Server feature in the CNWR-811P. This setting is on the LAN screen.
2. Configure the DHCP Server to provide the CNWR-811P's IP Address as the *Default Gateway*.

To Configure your PCs to use DHCP

This is the default setting for TCP/IP under Windows 95/98/ME. See *Chapter 4 – Client Configuration* for the procedure to check these settings.

Chapter 6
Routing

This Chapter explains the Routing features of the CNWR-811P.

Overview

While the CNWR-811P includes a standard (static) routing table, this feature can be completely ignored if you do not have a router in your LAN.

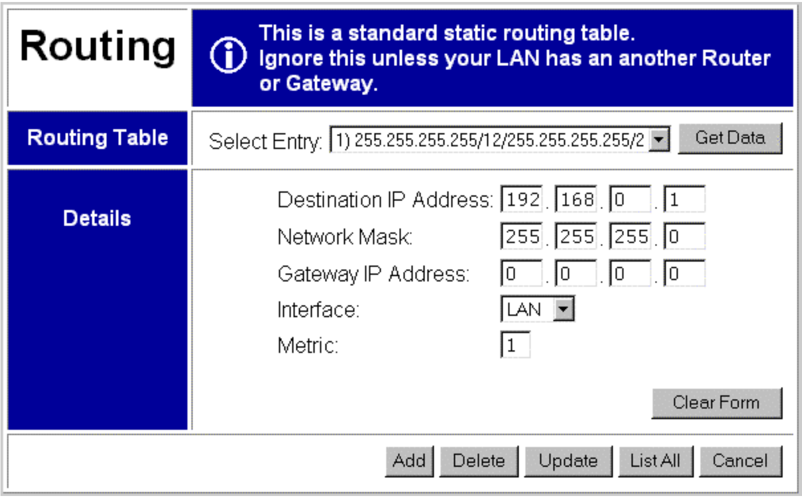
If you DO have a router, it is necessary to configure BOTH the Router and the Routing table in the CNWR-811P correctly, as described in the following sections.

Note!

See *Routing Example* on page 40 for an example of configuring both the CNWR-811P and the Router.

CNWR-811P Configuration

The routing table is accessed by the *Routing* link on the LAN screen. An example screen is shown below.



Routing

This is a standard static routing table. Ignore this unless your LAN has an another Router or Gateway.

Routing Table

Select Entry: 1) 255.255.255.255/12/255.255.255.255/2

Details

Destination IP Address: 192 . 168 . 0 . 1

Network Mask: 255 . 255 . 255 . 0

Gateway IP Address: 0 . 0 . 0 . 0

Interface: LAN

Metric: 1

Figure 22: Routing Screen

Using this Screen

Any existing entries are listed. To view and edit the details of an existing entry, select it, and click "Get Data". After making any changes, click the "Update" button to save your changes.

To add a new entry, click "Clear Form", enter your data, then click the "Add" button.

Routing Table Data

An entry in the routing table is required for each LAN segment on your Network, other than the segment to which this device is attached. The data in the Routing Table is as follows.

Destination IP Address	The network address of the remote LAN segment. For standard class "C" LANs, the network address is the first 3 fields of this *Destination IP Address*. The 4th (last) field can be left at 0.
Network Mask	The Network Mask used on the remote LAN segment. For class "C" networks, the standard Network Mask is 255.255.255.0
Gateway IP Address	The IP Address of the Router on the LAN segment to which this device is attached. (NOT the router on the remote LAN segment.)
Interface	Select the appropriate interface - LAN (Internal LAN) or WAN (External LAN or WAN) from the drop-down list.
Metric	The number of routers which must be traversed to reach the remote LAN segment. The default value is 1.

Router Configuration

It is essential that all IP packets for devices not on the local LAN be passed to the CNWR-811P, so that they can be forwarded to the external LAN, WAN, or Internet. To achieve this, the local LAN must be configured to use the CNWR-811P as the *Default Route* or *Default Gateway*.

Local Router

The local router is the Router installed on the same LAN segment as the CNWR-811P. This router requires that the *Default Route* is the CNWR-811P itself. Typically, routers have a special entry for the *Default Route*. It should be configured as follows.

Destination IP Address	Normally 0.0.0.0, but check your router documentation.
Network Mask	Normally 0.0.0.0, but check your router documentation.
Gateway IP Address	The IP Address of the CNWR-811P.
Metric	1

Other Routers on the Local LAN

Other routers on the local LAN must use the CNWR-811P's *Local Router* as the *Default Route*. The entries will be the same as the CNWR-811P's local router, with the exception of the *Gateway IP Address*.

- For a router with a direct connection to the CNWR-811P's local Router, the *Gateway IP Address* is the address of the CNWR-811P's local router.
- For routers which must forward packets to another router before reaching the CNWR-811P's local router, the *Gateway IP Address* is the address of the intermediate router.

Routing Example

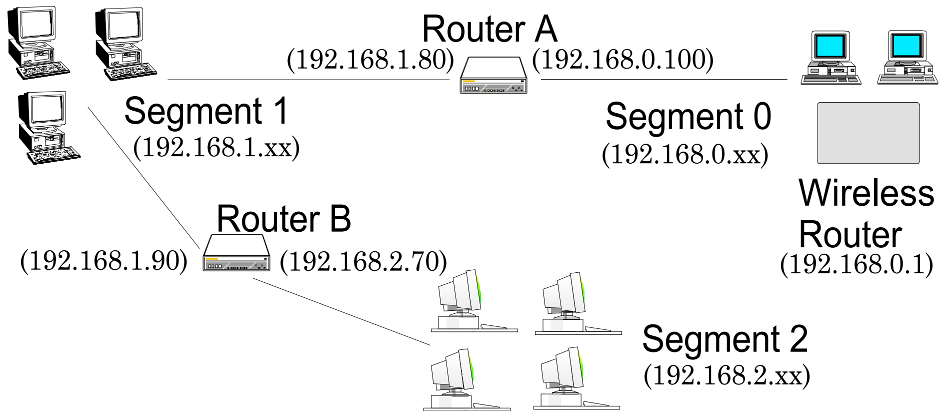


Figure 23: Routing Example

For the LAN shown above, with 2 routers and 3 LAN segments, the required entries would be as follows.

For the CNWR-811P's Routing Table

The CNWR-811P requires 2 entries as follows.

Entry 1 (Segment 1)	
Destination IP Address	192.168.1.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100 (CNWR-811P's local Router)
Interface	LAN
Metric	1
Entry 2 (Segment 2)	
Destination IP Address	192.168.2.0
Network Mask	255.255.255.0
Gateway IP Address	192.168.0.100
Interface	LAN
Metric	2

For Router A's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.0.1 (CNWR-811P's IP Address)

For Router B's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.1.80 (CNWR-811P's local router)

Chapter 7

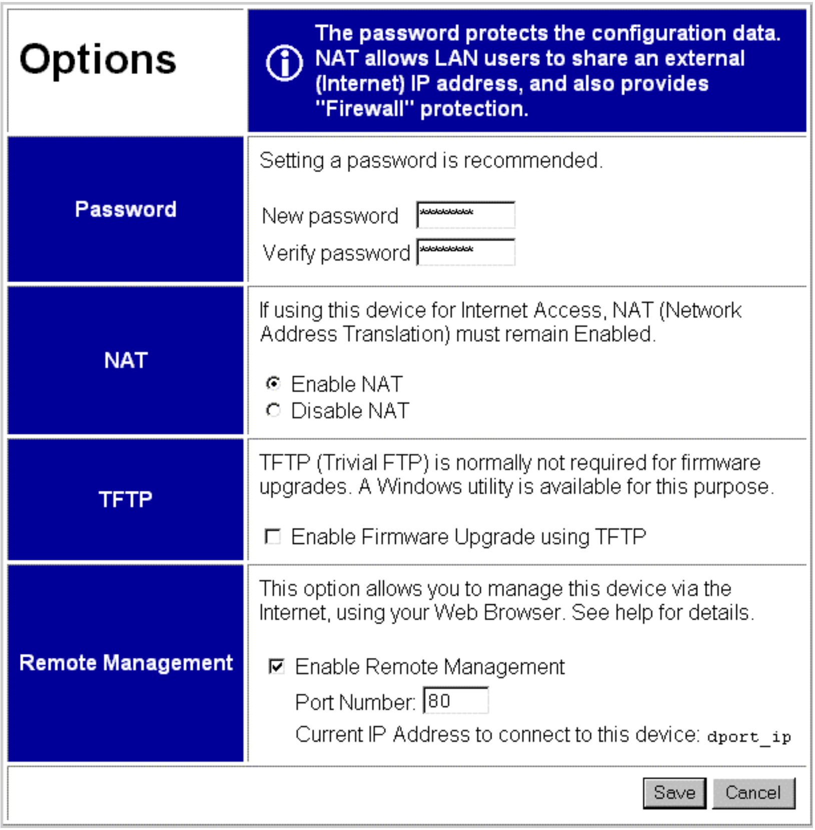
Options

7

This Chapter details the options available on the CNWR-811P's "Options" screen.

Overview

An example Options screen is shown below.



Options

The password protects the configuration data. NAT allows LAN users to share an external (Internet) IP address, and also provides "Firewall" protection.

Password

Setting a password is recommended.

New password ********

Verify password ********

NAT

If using this device for Internet Access, NAT (Network Address Translation) must remain Enabled.

● Enable NAT
○ Disable NAT

TFTP

TFTP (Trivial FTP) is normally not required for firmware upgrades. A Windows utility is available for this purpose.

□ Enable Firmware Upgrade using TFTP

Remote Management

This option allows you to manage this device via the Internet, using your Web Browser. See help for details.

☑ Enable Remote Management

Port Number: 80

Current IP Address to connect to this device: `dport_ip`

Figure 24: Options Screen

Password

Once a password is entered, it is required in order to change the device configuration. Passwords are case sensitive and can be up to 8 alphanumeric characters (no spaces or punctuation).

To create or change the password, enter the required password in both the *New Password* and *Verify Password* input fields.

Note!

When prompted for the password, leave the "User Name" blank.

NAT (Network Address Translation)

NAT allows PCs on your LAN to share a single external (Internet) IP Address. This IP Address is supplied by your ISP. Use the following to determine whether or nor you need NAT.

- For Internet access, NAT **must be left On** unless all PCs on your LAN have valid external IP Addresses.
- In other situations, NAT is not normally required. With NAT disabled, the CNWR-811P will act as a static router.
- If NAT is disabled, the Firewall protection provided by the CNWR-811P is lost, and the *Advanced Internet* features (Virtual Servers, Special Applications, and DMZ) are no longer available.

TFTP

TFTP (Trivial FTP) can be used to upgrade the firmware in the CNWR-811P. However, this is not normally required; there is a Windows utility available for this purpose.

Remote Management

This feature allows you to manage the CNWR-811P via the Internet.

Enable Remote Management	Enable to allow management via the Internet. If Disabled, this device will ignore management connection attempts from the WAN port.
Port Number	Enter a port number between 1024 and 65535 (8080 is recommended). This port number must be specified when you connect (see below). **Note:** The default port number for HTTP (Web) connections is port 80, but using port 80 here will prevent the use of a Web "Virtual Server" on your LAN. (See *Advanced Internet - Virtual Servers*)
Current WAN Port IP Address	You must use this IP Address to connect (see below). This IP Address is allocated by your ISP. But if using a Dynamic IP Address, this value can change each time you connect to your ISP. So it is better if your ISP allocates you a Fixed IP Address.

To connect from a remote PC via the Internet

1. Ensure your Internet connection is established, and start your Web Browser.
2. In the "Address" bar, enter "HTTP://" followed by the WAN IP Address of the CNWR-811P. If the port number is not 80, the port number is also required. (After the IP Address, enter ":" followed by the port number.)
   e.g.

   ```
   HTTP://123.123.123.123:8080
   ```

   This example assumes the WAN IP Address is 123.123.123.123, and the port number is 8080.

Chapter 8
Advanced Internet

This Chapter explains how to use the CNWR-811P's "Advanced Internet" features.

Overview

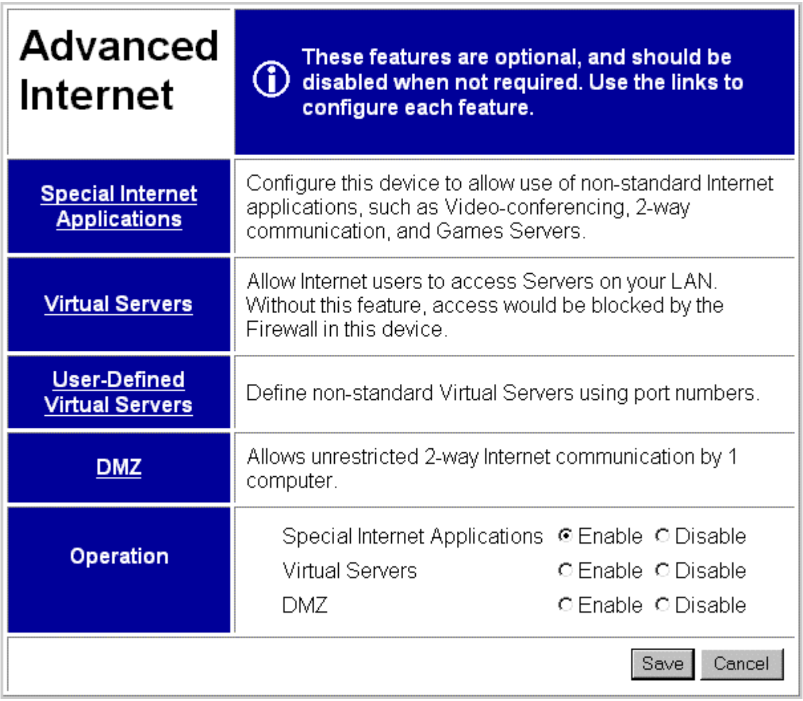
For situations where the CNWR-811P is being used to provide shared Internet access, the following advanced features are provided.

- Special Internet Applications
- Virtual Servers
- DMZ

This chapter contains details of the configuration and use of each of these features.

Advanced Internet Screen

This screen provides access to the advanced Internet features, and provides a convenient overview and control center. An example screen is shown below.



Advanced Internet	ⓘ These features are optional, and should be disabled when not required. Use the links to configure each feature.
Special Internet Applications	Configure this device to allow use of non-standard Internet applications, such as Video-conferencing, 2-way communication, and Games Servers.
Virtual Servers	Allow Internet users to access Servers on your LAN. Without this feature, access would be blocked by the Firewall in this device.
User-Defined Virtual Servers	Define non-standard Virtual Servers using port numbers.
DMZ	Allows unrestricted 2-way Internet communication by 1 computer.
Operation	Special Internet Applications ● Enable ○ Disable Virtual Servers ○ Enable ○ Disable DMZ ○ Enable ○ Disable

Figure 25: Advanced Internet Screen

On this screen, you can enable any required feature. By default, all features are disabled.

Special Internet Applications

This feature is only required if you wish to use Internet applications which require 2-way communication, multiple connections, or combined TCP/UDP connections.

Examples of such applications are Internet Videoconferencing, Telephony, Games Servers, and other special-purpose Servers.

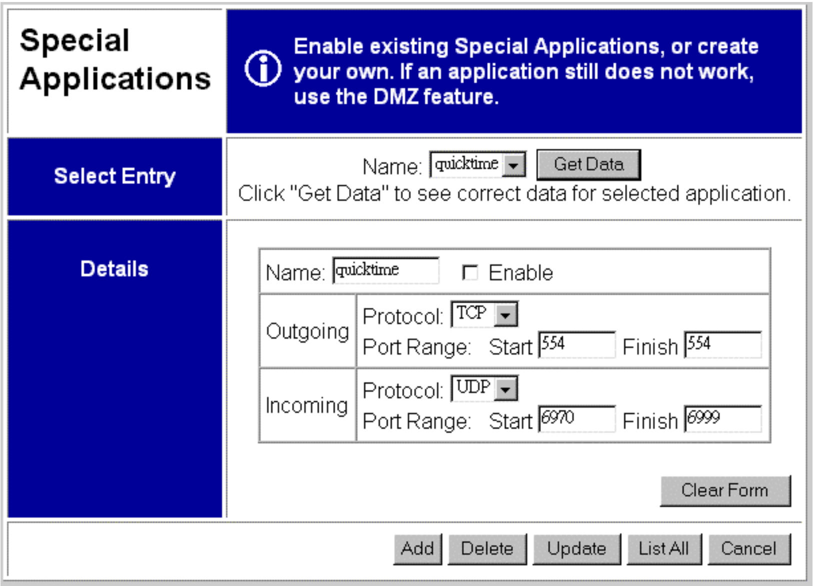
Generally, you will become aware of the need for this feature when an Internet application is unable to function correctly.

Note!

At any time, only one (1) PC can use each Special Application.

Special Applications Screen

This screen can be reached by selecting *Special Internet Applications*. An example screen is shown below.



Special Applications

Enable existing Special Applications, or create your own. If an application still does not work, use the DMZ feature.

Select Entry

Name: quicktime ▾ [Get Data]

Click "Get Data" to see correct data for selected application.

Details

Name: quicktime ☐ Enable

Outgoing	Protocol: TCP ▾	
	Port Range: Start 554	Finish 554
Incoming	Protocol: UDP ▾	
	Port Range: Start 6970	Finish 6999

Figure 26: Special Applications Screen

Using a Special Application

- Ensure that *Special Applications* has been enabled on the *Advanced Internet* screen.
- Configure the *Special Applications* screen as required.

Note!

- **Configuration data must be obtained from the Service/Application provider.**
- **If an application still cannot function correctly, try using the "DMZ" feature.**

Some Special Applications have been defined not enabled.

- **To Enable a defined Application**
  - Select it from the drop-down list
  - Click "Get Data"
  - Check the *Enable* checkbox
  - Click "Update"
- **To Disable a defined Application**
  - As above, but uncheck the *Enable* checkbox.
- **To Delete a defined Application**
  - Select it from the drop-down list,
  - Click "Delete"
- **To Modify (Edit) a defined Application**
  - Select it from the drop-down list,
  - Click "Get Data"
  - Make any desired changes
  - Click "Update"
- **To Create a new Application**
  - Click "Clear Form"
  - Enter the required data, as described below
  - Click "Add"
- **To List all Applications**
  - Click "List All"

Configuration Data (from Service Provider)

This data must be obtained from the service provider.

Name	Enter a descriptive name to identify this application entry.
Enable	Use this to Enable or Disable support for this application, as required.
Outgoing	
Protocol	The protocol (TCP or UDP) used when you connect to the special application service.
Port Range: Start	The beginning of the range of port numbers used by the application server, for data you send to it. If the application uses a single port number, enter it in both the "Start" and "Finish" fields.
Port Range: Finish	The end of the range of port numbers used by the application server, for data you send.
Incoming	
Protocol	The protocol (TCP or UDP) used when the application or service sends data to you.
Port Range: Start	The start of the range of port numbers used by the application server when data is sent to you. If using only one port number, enter it in both the "Start" and "Finish" fields.
Port Range: Finish	The end of the range of port numbers used by the application server, when data is sent to you.

Virtual Servers

This feature allows you to make Servers on your LAN accessible to Internet users. Normally, Internet users would not be able to access a server on your LAN because:

- Your Server does not have a valid external IP Address.
- Attempts to connect to devices on your LAN are blocked by the firewall in this device.

The "Virtual Server" feature solves these problems and allows Internet users to connect to your servers, as illustrated below.

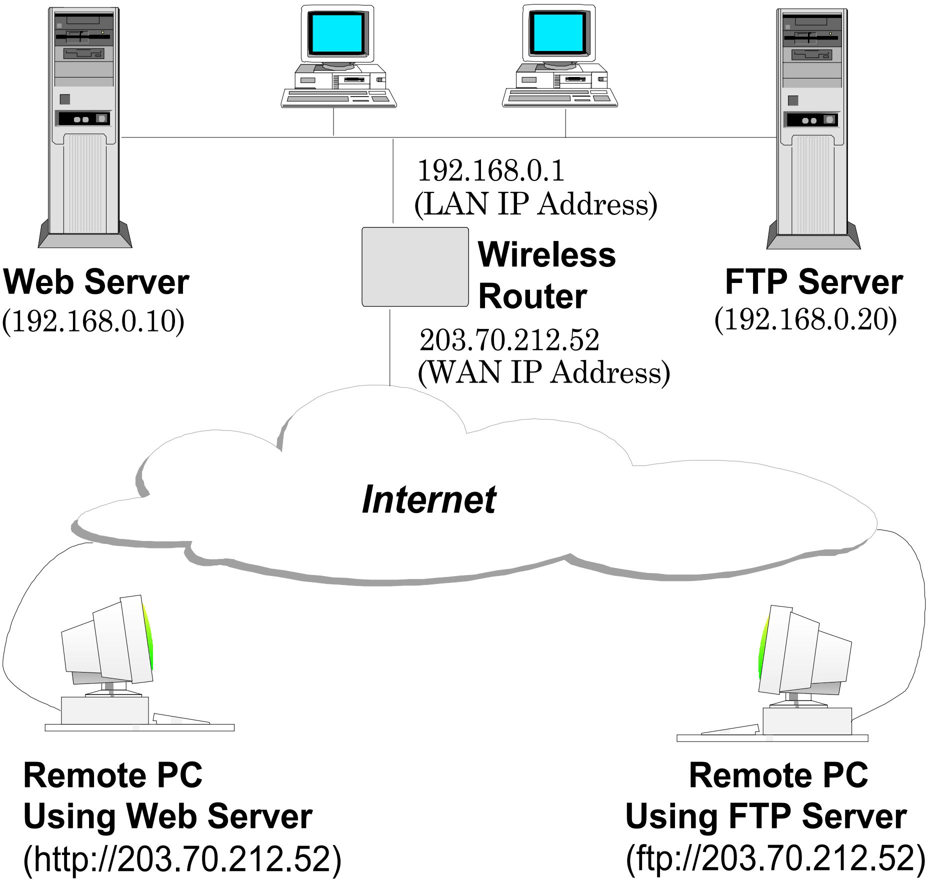


Figure 27: Virtual Servers

IP Address seen by Internet Users

Note that, in this illustration, both Internet users are connecting to the same IP Address, but using different protocols.

To Internet users, all virtual Servers on your LAN have the same IP Address. This IP Address is allocated by your ISP.

This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers. If using a Static IP Address, it is entered on the "WAN" screen.

Types of Virtual Servers

The CNWR-811P supports two (2) types of Virtual Servers:

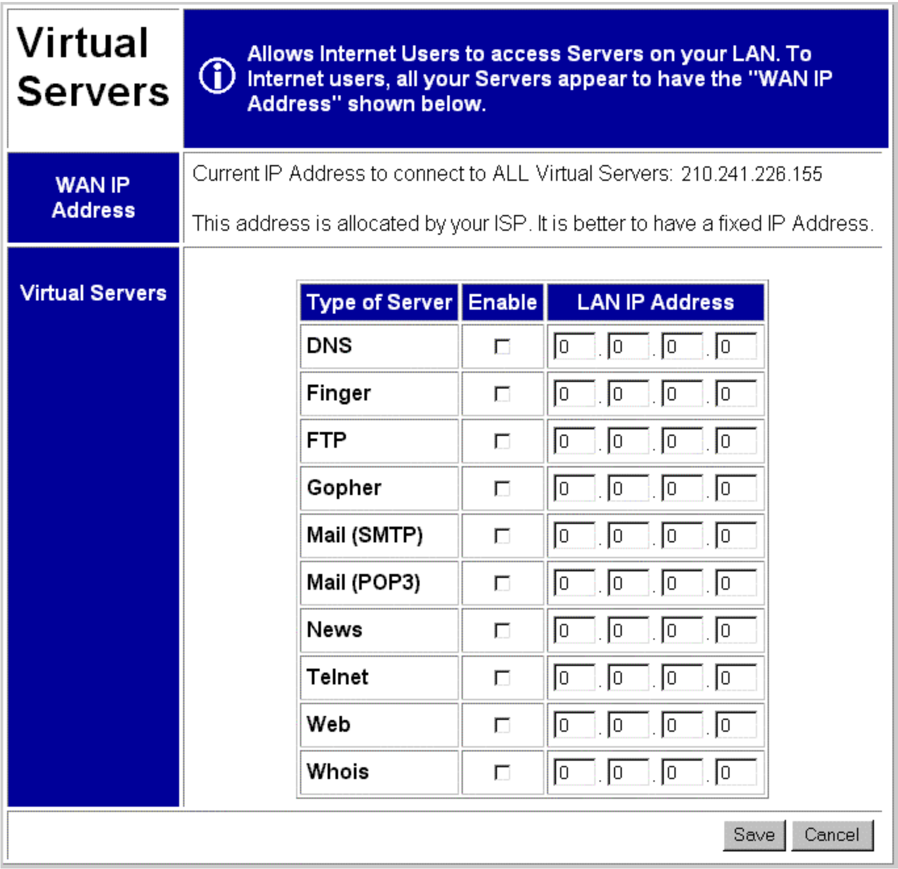
- **Pre-defined** - Standard server types. The only data required is the IP Address of the server on your LAN.
- **User-defined** - Non-standard servers. You must provide additional information about the server.

Note:

The TOTAL number of Virtual Servers which can be used at any time is 10.

Virtual Server Configuration

The *Virtual Servers* screen is reached by the *Advanced Internet - Virtual Servers* link. An example screen is shown below.



Virtual Servers

Allows Internet Users to access Servers on your LAN. To Internet users, all your Servers appear to have the "WAN IP Address" shown below.

WAN IP Address

Current IP Address to connect to ALL Virtual Servers: 210.241.226.155

This address is allocated by your ISP. It is better to have a fixed IP Address.

Virtual Servers

Type of Server	Enable	LAN IP Address
DNS	□	0 . 0 . 0 . 0
Finger	□	0 . 0 . 0 . 0
FTP	□	0 . 0 . 0 . 0
Gopher	□	0 . 0 . 0 . 0
Mail (SMTP)	□	0 . 0 . 0 . 0
Mail (POP3)	□	0 . 0 . 0 . 0
News	□	0 . 0 . 0 . 0
Telnet	□	0 . 0 . 0 . 0
Web	□	0 . 0 . 0 . 0
Whois	□	0 . 0 . 0 . 0

Figure 28: Virtual Server Screen.

Data

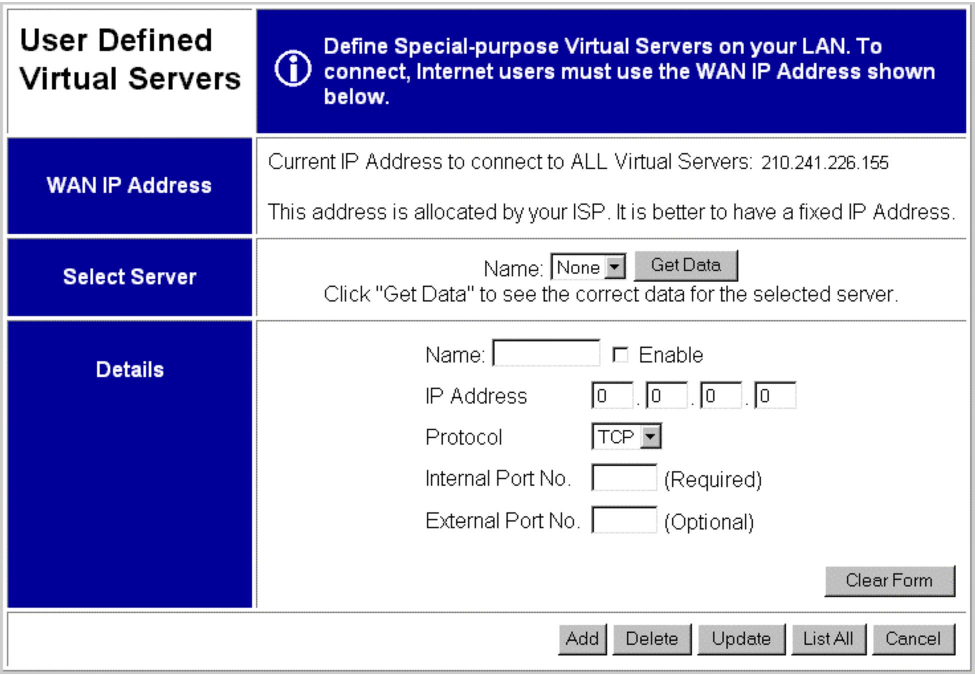
WAN IP Address	• This shows the IP Address which Internet users must use to connect to any of your Virtual Servers. • To Internet Users, ALL your Virtual Servers have the same IP Address. • This IP Address is allocated by your ISP. It is better to have a fixed IP Address.

Type	Select the type of Server you wish to use.
Enable	Check to enable this Server.
LAN IP Address	• Enter the IP Address of a PC on your LAN. • You must install and configure the appropriate Server software on the PC entered here. • If using DHCP, the LAN IP Address of a PC may change. To solve this problem, use either of these methods: • Assign a fixed IP Address to the Server PC, ensuring that its IP Address is NOT within the address range allocated by the DHCP Server. • Reserve an IP Address for the Server PC in the DHCP Server, using the *Access Control - PC* screen.

User Defined Virtual Servers

If the type of Server you wish to use is not listed on the *Virtual Servers* screen, you can define it using this feature.

Select *Advanced Internet - User Defined Virtual Servers* to see a screen like the example below.



User Defined Virtual Servers

Define Special-purpose Virtual Servers on your LAN. To connect, Internet users must use the WAN IP Address shown below.

WAN IP Address

Current IP Address to connect to ALL Virtual Servers: 210.241.226.155

This address is allocated by your ISP. It is better to have a fixed IP Address.

Select Server

Name: None

Click "Get Data" to see the correct data for the selected server.

Details

Name: □ Enable

IP Address 0 . 0 . 0 . 0

Protocol TCP

Internal Port No. (Required)

External Port No. (Optional)

Figure 29: User Defined Virtual Servers

- **To Create a new Server**
  - Click "Clear Form"
  - Enter the required data (See next section)
  - Click "Add"

- **To Modify (Edit) a defined Server**
  - Select it from the drop-down list,
  - Click "Get Data"
  - Make any desired changes. Note that you can "Enable" and "Disable" a Server using this process.
  - Click "Update"
- **To Delete a defined Server**
  - Select it from the drop-down list,
  - Click "Delete"
- **To List all Servers**
  - Click "List All"

Data

WAN IP Address	• This shows the IP Address which Internet users must use to connect to any of your Virtual Servers. • To Internet Users, ALL your Virtual Servers have the same IP Address. • This IP Address is allocated by your ISP. It is better to have a fixed IP Address.
Select Server	This lists any Servers you have defined. Click the "Get Data" button to view the correct data for the selected Server.
Details	
Name	Enter a descriptive name to identify this Server entry.
Enable	Use this to Enable or Disable support for this Server, as required.
IP Address	The IP Address of the PC on your LAN which is running the Server software.
Protocol	Select the protocol (TCP or UDP) used by the Server.
Internal Port Number	Enter the port number used by the Server to connect to clients.
External Port Number	The port number used by clients when connecting to the Server. This is normally the same as the *Internal Port Number*. If it is different, this device will perform a "mapping" or "translation" function, allowing the server to use one port address, while clients use a different port address.

Note!

From the Internet, ALL Virtual Servers have the IP Address allocated by your ISP, as shown by the "WAN IP Address".

Connecting to the Virtual Servers

Once configured, anyone on the Internet can connect to your Virtual Servers. They must use the WAN Port IP Address (the IP Address allocated to this device by your ISP).
e.g.

```
http://203.70.212.52
ftp://203.70.212.52
```

It is more convenient if you are using a Fixed IP Address from your ISP, rather than Dynamic. If using a Fixed IP Address, it is entered on the *WAN* screen.

DMZ

This feature, if enabled, allows one (1) computer on your LAN to be exposed to all users on the Internet, allowing unrestricted 2-way communication between the "DMZ" PC and other Internet users or Servers.

This allows connection to special-purpose servers which require proprietary client software, or 2-way user connections such as Video-conferencing, which requires both users to run special software.

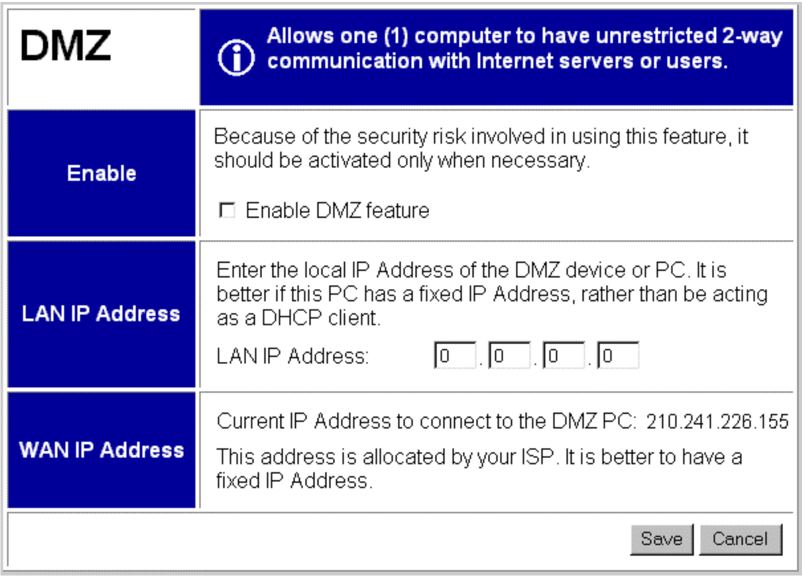
Note!

To allow unrestricted access, the Firewall in this device is disabled, creating a security risk.

You should use this feature only if the "Special Applications" feature is insufficient to allow an application to function correctly. This feature should be turned ON only when needed, and left OFF the rest of the time.

Configuring the DMZ

Select *Advanced Internet* from the navigation bar, then *DMZ* to see a screen like the following:



DMZ

Allows one (1) computer to have unrestricted 2-way communication with Internet servers or users.

Enable	Because of the security risk involved in using this feature, it should be activated only when necessary. □ Enable DMZ feature
LAN IP Address	Enter the local IP Address of the DMZ device or PC. It is better if this PC has a fixed IP Address, rather than be acting as a DHCP client. LAN IP Address: 0 . 0 . 0 . 0
WAN IP Address	Current IP Address to connect to the DMZ PC: 210.241.226.155 This address is allocated by your ISP. It is better to have a fixed IP Address.

Figure 30: DMZ Screen

Data

Enable	
Enable DMZ Feature	Use this to Enable or Disable the DMZ feature. The DMZ feature should be disabled when not required.
LAN IP Address	
LAN IP Address	Enter the IP Address of the PC on your LAN which will become the "DMZ" PC. If using DHCP, the LAN IP Address of a PC may change. To solve this problem, you can use either of these methods: • Assign a fixed IP Address to the DMZ PC, ensuring that its IP Address is NOT within the address range allocated by the DHCP Server. • Reserve an IP Address for the DMZ PC in the DHCP Server, using the *Access Control - PC* screen.
WAN IP Address	
WAN IP Address	This is the IP Address Internet users must use to connect to the "DMZ" PC. This IP Address is allocated by your ISP. It is better if you are using a fixed IP Address, so that it never changes. This will make it easier for Internet users to connect to you. If using a Static IP Address, it is entered on the "WAN" screen.

Note!

To Internet users, the IP Address of the DMZ computer is the IP Address allocated by your ISP, as shown by the "WAN IP Address" value.

Chapter 9

Access Control

9

This Chapter explains how to configure and use the CNWR-811P's "Access Control" feature.

Overview

The Access Control feature allows administrators to restrict Internet Access by individual PCs. The process uses "Packet Filtering" to block or discard data packets. By default, no packets are blocked or discarded.

To use this feature:

- Set the desired restrictions on the "Everyone" group. All PCs are in the "Everyone" group unless explicitly moved to another group, using the *PC* screen.
- Set the desired restrictions on the other groups ("Group 1", "Group 2", etc) as needed.
- For each PC you wish to move from the "Everyone" group, enter their details on the *PCs* screen, and assign them to the desired group

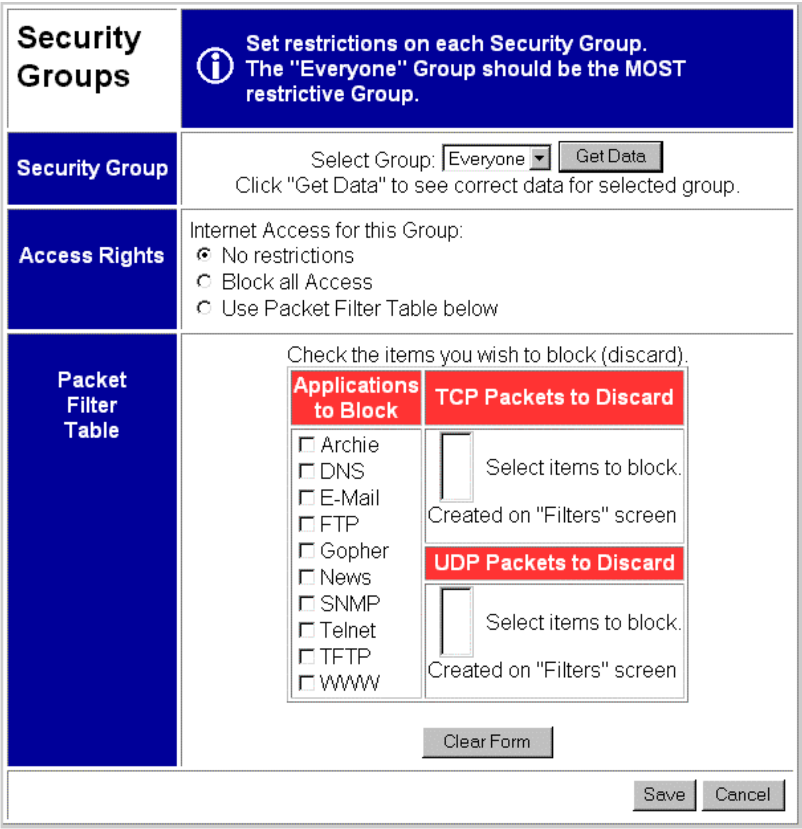
Note!

You can limit Internet access for ALL PCs without entering ANY PC data. Simply apply the desired restrictions to the "Everyone" group.

It is also possible to define your own packet filters, and use these filters in addition to the pre-defined filters. Defining your own filters is optional.

Security Groups

The *Security Groups* screen is reached from the *Access Control* link on the navigation bar. An example screen is shown below.



Security Groups

Set restrictions on each Security Group. The "Everyone" Group should be the MOST restrictive Group.

Security Group

Select Group: Everyone ▾ [Get Data]
Click "Get Data" to see correct data for selected group.

Access Rights

Internet Access for this Group:
● No restrictions
○ Block all Access
○ Use Packet Filter Table below

Packet Filter Table

Check the items you wish to block (discard).

Applications to Block	TCP Packets to Discard
□ Archie □ DNS □ E-Mail □ FTP □ Gopher □ News □ SNMP □ Telnet □ TFTP □ WWW	Select items to block. Created on "Filters" screen **UDP Packets to Discard** Select items to block. Created on "Filters" screen

[Clear Form]

[Save] [Cancel]

Figure 31: Security Groups Screen

Note that the Security groups are pre-named "Everyone", "Group 1", "Group 2", "Group 3", and "Group 4".

Operations

- **To Define a Security Group:**
  Select the group from the drop-down box, then enter the required data. If necessary, click *Clear Form* to remove the existing information shown on screen.
  Click the *Save* button when finished.
- **To Change Access for an Existing Group**:
  Select the group from the drop-down box, click *Get Data* to view their information, then change any fields you wish.
  Click *Save* when finished.
- **To Assign PCs to a Security Group**
  All PCs are initially in the "Everyone" group. Use the *PCs* screen to move individual PCs to other groups as required.

Data

The following data is required.

Access Rights: Internet Access for this Group	
No restrictions	No packets are blocked. Use this to create an "Unlimited Access" group, or to temporarily remove restrictions.
Block all Access	Group members cannot access the Internet at all. Use this to create the most restrictive group.
Use Packet Filter Table below	Use this to define intermediate levels of access. Using the Packet Filter table gives you fine control over Internet access. Simply select the items you wish to block. You can choose from the pre-defined filters in the *Applications to Block* column, or your own filters in the *TCP Packets to Discard* and *UPD Packets to Discard* column.

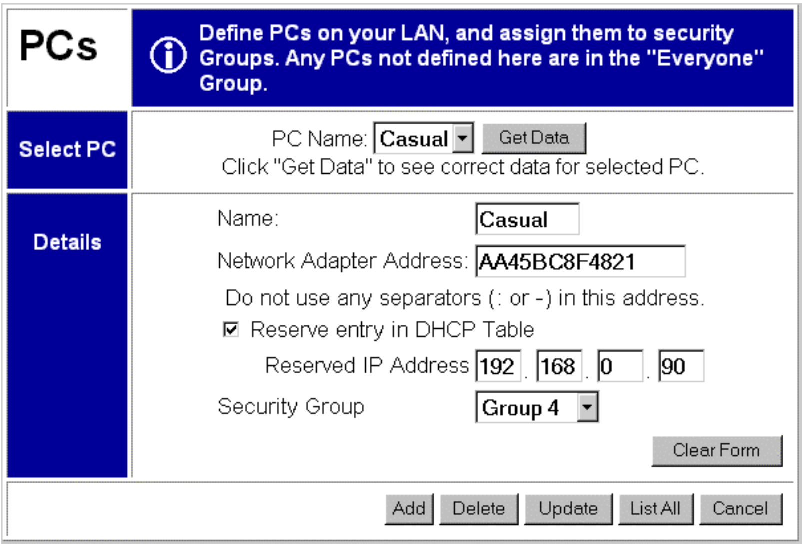
Packet Filter Table	
Applications to Block	Any items checked will be blocked. Users will not be able to use the application.
TCP Packets to Discard	This lists any TCP filters you have defined on the *Filters* screen. If no filters have been defined, this is empty. Multiple items can be selected (or deselected) by holding down the Ctrl key while selecting items. Selected items can NOT be accessed by members of this group.
UDP Packets to Discard	This lists any UDP filters you have defined on the *Filters* screen. If no filters have been defined, this is empty. Multiple items can be selected (or deselected) by holding down the Ctrl key while selecting items. Selected items can NOT be accessed by members of this group.

Note!

If you have not defined your own filters, but wish to do so, refer to "Filters" later in this chapter.

PCs

The *PCs* screen is reached from the *Access Control* link on the navigation bar. An example screen is shown below.



PCs

Define PCs on your LAN, and assign them to security Groups. Any PCs not defined here are in the "Everyone" Group.

Select PC

PC Name: Casual

Click "Get Data" to see correct data for selected PC.

Details

Name: Casual

Network Adapter Address: AA45BC8F4821

Do not use any separators (: or -) in this address.

☑ Reserve entry in DHCP Table

Reserved IP Address 192 . 168 . 0 . 90

Security Group Group 4

Figure 32: PCs Screen

Note that the drop-down box lists all PCs previously entered. If none have been entered, this box will be empty.

Operations

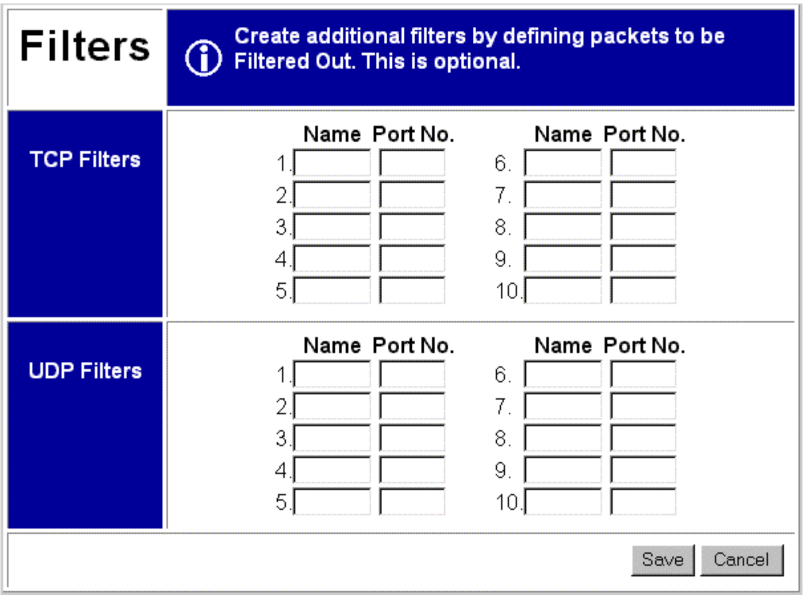
- **To Add a New PC**:
  Ignore the drop-down box, click the *Clear Form* button, and enter the PC details in the fields provided.
  Click *Add* when finished.
- **To Delete an Existing PC:**
  Select the PC from the drop-down box, click *Get Data* to view the information and confirm that this is the correct PC, then click the *Delete* button.
- **To Change an Existing PC's Details**:
  Select the PC from the drop-down box, click *Get Data* to view their information, then change any fields you wish.
  Click *Update* when finished.
- **To Generate a List of all PCs:**
  Just click on the *List All* button.

Data

PC Name	Enter a name to identify this PC.
Network Adapter Address	Hardware address for this PC. You can use the Windows "Winipcfg" program or your LAN management program to find this address.
Reserve entry in DHCP Table	Check this if you wish to reserve an IP address for this PC. This is useful if you have to provide the IP Address for other programs or users. If this is left unchecked, the following entry can be ignored.
Reserved IP Address	This relates to the entry above. Enter the reserved address here. This MUST be within the range used by the DHCP server (set on the *Device - Internal LAN Port* screen).
Security Group	Select the security group for this PC. If you only wish to reserve an IP Address, and are not using the security (access control) features, simply leave this at "Everyone".

Filters

The *Filters* screen is reached from the *Access Control* link on the navigation bar. An example screen is shown below.



Filters

Create additional filters by defining packets to be Filtered Out. This is optional.

Figure 33: Filters Screen

This screen allows you to define packet filters. When you define security groups, on the "Security Groups" screen, you can select from any filters defined here, as well as the pre-defined filters.

Data

TCP Packets

Define the packets you wish to be filtered out, by entering the following data.

TCP Filters	
Name	Enter a descriptive name for this entry.
Port No.	Enter an integer representing the Port Number for this type of packet. This information can normally be provided by the service provider. Otherwise, a Network Analyzer or Packet Sniffer can be used to determine the correct port number.
UDP Filters	
Name	Enter a descriptive name for this entry.
Port No.	Enter an integer representing the Port Number for this type of packet. This information can normally be provided by the service provider. Otherwise, a Network Analyzer or Packet Sniffer can be used to determine the correct port number.

Appendix A
Troubleshooting

This Appendix covers the most likely problems and their solutions.

Overview

This chapter covers some common problems that may be encountered while using the CNWR-811P and some possible solutions to them. If you follow the suggested steps and the CNWR-811P still does not function properly, contact your dealer for further advice.

General Problems

Problem 1: Can't connect to the CNWR-811P to configure it.

Solution 1: Check the following:

- The CNWR-811P is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the CNWR-811P are on the same network segment. (If you don't have a router, this must be the case.)
- Ensure that your PC is using an IP Address within the range 192.168.0.2 to 192.168.0.254 and thus compatible with the CNWR-811P's default IP Address of 192.168.0.1.
  Also, the Network Mask should be set to 255.255.255.0 to match the CNWR-811P.
  In Windows, you can check these settings by using *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

Internet Access

Problem 1: When I enter a URL or IP address I get a time out error.

Solution 1: A number of things could be causing this. Try the following troubleshooting steps.

- Check if other PCs work. If they do, ensure that your PCs IP settings are correct (IP address, Network Mask, Default gateway and DNS).
- If the PCs are configured correctly, but still not working, check the CNWR-811P. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.)
- If the CNWR-811P is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.

Problem 2: Some applications do not run properly when using the CNWR-811P.

Solution 2: The CNWR-811P processes the data passing through it, so it is not transparent.

Use the *Special Applications* feature to allow the use of Internet applications which do not function correctly.

If this does solve the problem you can use the *DMZ* function. This should work with almost every application, but:

- It is a security risk, since the firewall is disabled.
- Only one (1) PC can use this feature.
- When the *DMZ* feature is being used, the *Special Applications* and *Virtual Server* features should be disabled.

Wireless Access

Problem 1: My PC can't locate the Wireless Access Point

Solution 1: Check the following.

- Your PC is set to *Infrastructure Mode*.
- The wireless channel used matches the wireless channel on the Access Point.
- The SSID on your PC and the Wireless Access Point are the same. Remember that the SSID is case-sensitive. So, for example "Workgroup" does NOT match "workgroup".
- Both your PC and the Wireless Access Point must have the same setting for WEP. The default setting for the CNWR-811P is disabled, so your wireless station should also have WEP disabled.
- If WEP is enabled, the key tables must match.
- If the Wireless Station access permission on the CNWR-811P's *Wireless* screen is set to *Only allow access if on this list*, then each Wireless station must have its address correctly entered.
- To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Access Point.
  Remember that the connection range can be as little as 100 feet in poor environments.

Problem 2: Wireless connection speed is very slow.

Solution 2: The wireless system will connect at the highest possible speed, depending on the distance and the environment. To obtain the highest possible connection speed, you can experiment with the following:

- Access Point location.
  Try adjusting the location and orientation of the Access Point.
- Wireless Channel
  If interference is the problem, changing to another channel may show a marked improvement.
- Radio Interference
  Other devices may be causing interference. You can experiment by switching other devices Off, and see if this helps. Any "noisy" devices should be shielded or relocated.
- RF Shielding
  Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the Access Point.

Printing

Problem 1: **When I tried to install the Printing software for Peer-to-Peer printing, I received an error message and the installation was aborted..**

Solution 1: This may be caused by an existing installation of the printer port software. Before attempting another installation:

- Remove the existing installation
- Restart your PC

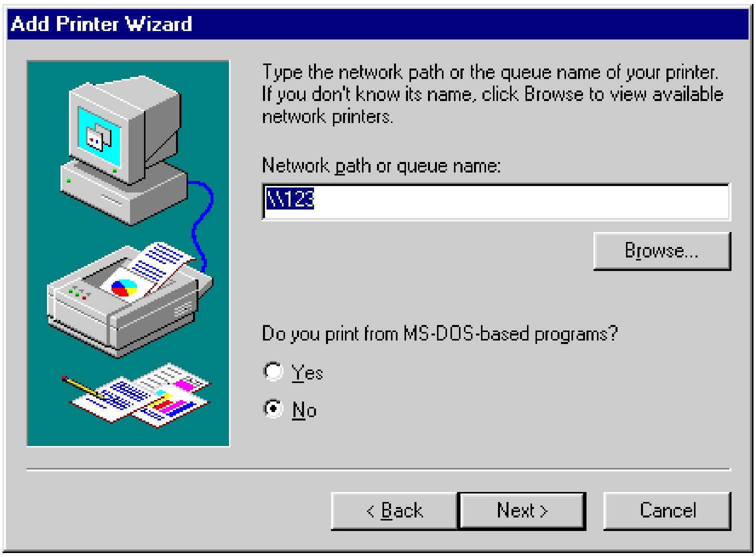
To remove an existing printer port installation:

1. Open Start - Settings - Control Panel - Add/Remove Programs
2. Look for an entry with a name like "Shared Port", "Shared Printer Port", "Print Server Driver" or "Print Server Port".
3. Select this item, click "Add/Remove", and confirm the deletion.

Problem 2: **I am using Windows 95, and the Printing software installed and ran, but when I selected a port on a CNIG907BP and clicked "Add", the printer was not installed.**

Solution 2: Try installing the printer using the standard Windows tools, as follows:

1. Start the *Add Printer* Wizard.
2. Select *Network Printer* when prompted "How is the printer attached to your Computer?", and click Next.
3. When prompted for the Network Path or Queue, enter a dummy value such as \\123, as shown below. (Do NOT select *Yes* for "Do you print for MS-DOS programs?")



Add Printer Wizard

Type the network path or the queue name of your printer. If you don't know its name, click Browse to view available network printers.

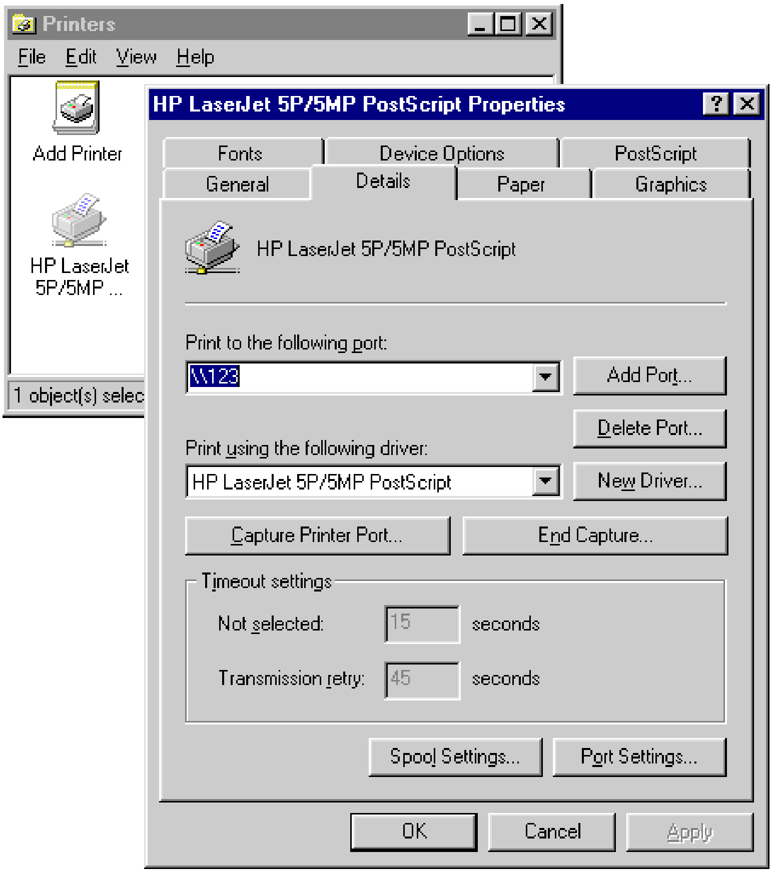
Network path or queue name: \\123

Do you print from MS-DOS-based programs?

○ Yes

● No

4. The printer wizard will display a message stating that “The Network Printer is off-line”. This is OK. Continue the Add Printer Wizard until finished.
5. When finished, go to *Control - Panel-Printers*. The printer icon will be grayed out indicating the printer is not ready.
6. Right-click the Printer, and select *Properties*. Then select the *Details* tab, as shown below. (On Windows NT/2000, select the *Ports* tab.)



Printers

File Edit View Help

Add Printer

HP LaserJet 5P/5MP ...

1 object(s) selec

HP LaserJet 5P/5MP PostScript Properties

Fonts | Device Options | PostScript | General | Details | Paper | Graphics

HP LaserJet 5P/5MP PostScript

Print to the following port: \\123

Add Port...

Delete Port...

Print using the following driver: HP LaserJet 5P/5MP PostScript

New Driver...

Capture Printer Port... | End Capture...

Timeout settings

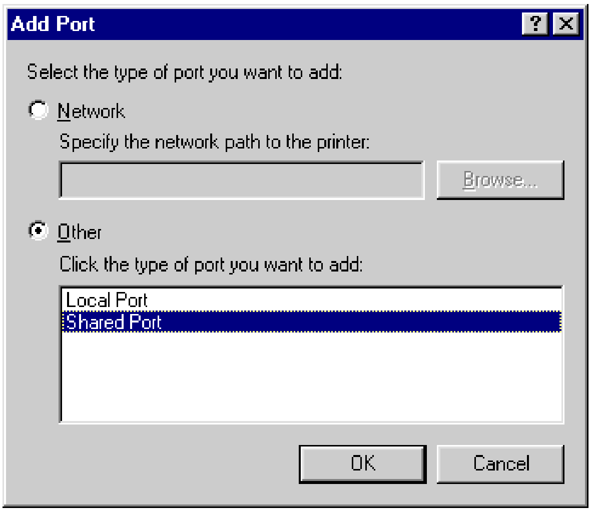
Not selected: 15 seconds

Transmission retry: 45 seconds

Spool Settings... | Port Settings...

OK | Cancel | Apply

7. Click the *Add Port* button. On the resulting screen, select *Other*, then *Shared Port*, as the port to add, as shown below.



Add Port

Select the type of port you want to add:

○ Network

Specify the network path to the printer:

Browse...

● Other

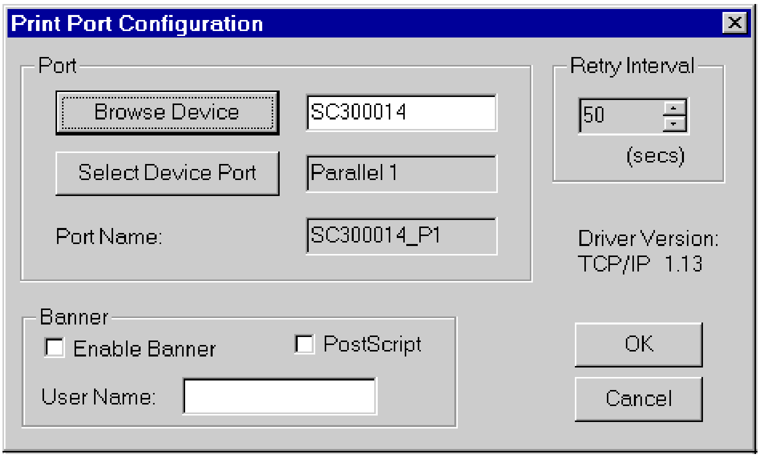
Click the type of port you want to add:

Local Port

Shared Port

OK | Cancel

8. Click OK to see the *Print Port Configuration* screen, as shown below.



SC300014

Parallel 1

Port Name: SC300014_P1

50 (secs)

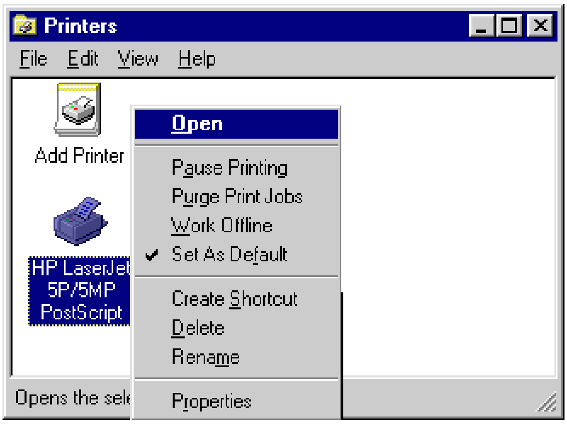
Driver Version:
TCP/IP 1.13

□ Enable Banner □ PostScript

User Name:

9. Click the *Browse Device* button, select the desired Internet Broadband Gateway, and click OK.

10. Click OK to return to the Printers folders, and right-click on the Printer. Ensure that the *Work off-line* option is NOT checked.



The Printer should no longer be grayed out, and is ready for use.

Appendix B
Specifications

B

CNWR-811P Wireless A/P Router

Model No.:	CNWR-811P
Dimensions	240mm(W) * 120mm(D) * 35mm(H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol:	TCP/IP
Network Interface:	3 Ethernet: 2 * 10/100BaseTX (RJ45) for LAN 1 * 10BaseT (RJ45) for WAN
PCMCIA Slot	1 Type II, 16bit bus
Wireless interface	Wireless Access Point via supplied PCMPIA card IEEE 802.11b compatible, WEP security support, roaming support
Printer Port	1 * parallel printer port
LEDs	8
Power Adapter	12 V DC External

FCC Statement:

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.

(2) This device must accept any interference received, including interference that may cause undesired operation.

CE Marking Warning

This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

PCMCIA Wireless Card

Interface	PCMCIA 68pin, 16bit data
Standards	IEEE802.11b WLAN, PCMCIA 2.1, JEIDA 4.2
Frequency	2.4 to 2.4835GHz (Industrial Scientific Medical Band)
Channels	Maximum 14 Channels, depending on regulatory authorities.
Data Rate	11 / 5.5 / 2 / 1 Mbps
Coverage Area	Closed Space : 25m @11Mbps, 100m @5.5Mbps or lower
Power	DC +3.3V / 220mA
Output Power	13dBm (typical)
Receiver Sensitivity	-80dBm Min.
Operating Temperature	0° to 55°C
Storage Temperature	-25° to 70°C
Relative humidity	10% to 90%
PWR LED	ON - power available OFF - no power
ACT LED	OFF - inactive Blinking - Data transmitted or received.