

IP5020

Internet Access Server

User's Guide

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

Copyright © 2000. All Rights Reserved.

Document Version: 1.1

All trademarks and trade names are the properties of their respective owners.

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION	1
IP5020 Features	1
LAN Features	1
Internet Access Features.....	1
Configuration & Management	2
Advanced Functions.....	2
Security Features	2
Package Contents	3
IP5020 Internet Access Server	3
Components.....	3
LED Table.....	4
DIP Switches.....	4
CHAPTER 2 INSTALLATION	6
Procedure	6
Requirements.....	6
Procedure	6
CHAPTER 3 CONFIGURATION	7
Overview	7
Configuration Program	8
Preparation	8
Connecting to the IP5020.....	8
Home Screen	9
LAN Port Configuration	10
Data - LAN Port	10
WAN Port Configuration	12
Direct Connection Screen.....	12
PPPoE Screen.....	14
Status Screens	15
WAN Status – Direct Connection	15
WAN Status – PPPoE	16
Device/LAN Status Screen.....	18
CHAPTER 4 PC CONFIGURATION	20
If you have a Router	20
If you use DHCP	20
No Router, no DHCP	20
IP Address	20
Network Mask.....	20
Gateway.....	20
DNS (Domain Name Server) Address	21
Operation - Internet Access	21
Accessing AOL	21
CHAPTER 5 DHCP	22
Overview	22
What DHCP Does	22
Checking if your PC uses DHCP	23
Checking your DHCP Server	24
Using the IP5020's DHCP Server	25
To Configure your PCs to use DHCP	25
CHAPTER 6 ROUTING	27
Overview	27
IP5020 Configuration	27
Routing Table Data	27

Router Configuration	28
Local Router.....	28
Other Routers on the Local LAN	28
Routing Example.....	29
For the IP5020's Routing Table.....	29
For Router A's Default Route.....	29
For Router B's Default Route	29
CHAPTER 7 DEVICE OPTIONS	30
Overview	30
Device Password.....	30
NAT (Network Address Translation).....	31
CHAPTER 8 ADVANCED INTERNET	32
Overview	32
Advanced Internet Screen.....	32
Special Applications.....	33
Special Applications Screen.....	33
Using a Special Application.....	33
Configuration Data (from Service Provider).....	34
Virtual Servers	35
IP Address seen by Internet Users.....	35
Types of Virtual Servers	35
Virtual Server Configuration.....	36
User Defined Virtual Servers	37
Connecting to the Virtual Servers	38
Using this Device as a Virtual Web Server.....	38
Exposed Computer.....	39
Configuring the Exposed Computer.....	39
Data	39
CHAPTER 9 ACCESS CONTROL	41
Overview	41
Security Groups	42
Operations	42
Data	43
Workstations	44
Operations	44
Data	44
Administrator Defined Filters.....	45
Data	45
APPENDIX A TROUBLESHOOTING.....	47
Overview	47
General Problems.....	47
Internet Access	47
APPENDIX B SPECIFICATIONS	49
IP5020 Internet Access Server	49



Chapter I

Introduction

This Chapter provides an overview of the IP5020's features and capabilities.

Congratulations on the purchase of your new IP5020 Internet Access Server. The IP5020 will allow multiple LAN users to share an Internet user account, via an DSL or Cable modem. Once the IP5020 is installed and configured, the Internet is just a click away.

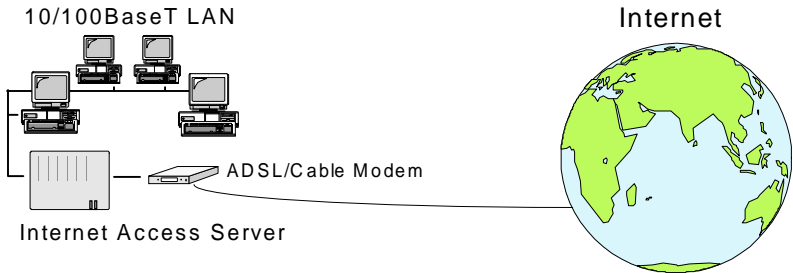


Figure 1: Office to Internet

Alternatively, the IP5020 Internet Access Server can be used to connect your local LAN to a remote LAN or WAN, via the IP5020's WAN port.

IP5020 Features

The IP5020 incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

LAN Features

- **Dual Ethernet ports.** The IP5020 has 2 Ethernet ports. One (the LAN port) is used to connect to your local LAN. The other (the WAN port) is used to connect to an external LAN, WAN or the Internet. (Internet access requires an DSL or Cable modem.)
- **DHCP Server Support.** Dynamic Host Configuration Protocol provides a dynamic IP address to PCs and other devices upon request. The IP5020 can act as a **DHCP Server** for devices on your local LAN.
- **DHCP Client Support.** On the WAN port, the IP5020 can act as a **DHCP Client**. This allows the use of dynamic IP Addresses on the "External LAN" or WAN.
- **Multi Segment LAN Support.** LANs containing one or more segments are supported, via the IP5020's built-in static routing table. If NAT (Network Address Translation) is disabled, the IP5020 will function as a static router.

Internet Access Features

- **Shared Internet Access.** All users on the LAN can access the Internet through the IP5020, 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).

- **PPPoE Support.** Connect to your ISP using PPPoE (PPP over Ethernet), if your ISP uses this method.

Configuration & Management

- **Easy Setup.** Use your WEB browser from anywhere on the LAN for configuration.
- **Remote Management.** The IP5020 can be managed from a workstation anywhere on the LAN, using a WEB browser.

Advanced 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.
- **Exposed Computer.** One (1) PC on your local LAN can be exposed to the Internet. This allows unrestricted 2-way communication between this PC and servers or 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 and E-Mail access by individual workstations.
- **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.)

Firewall Protection

The firewall protection provided by the IP5020 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 IP5020 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 IP5020 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 IP5020 Unit
- Power Adapter
- Quick Installation Guide
- CD-ROM containing the on-line manual.

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

IP5020 Internet Access Server

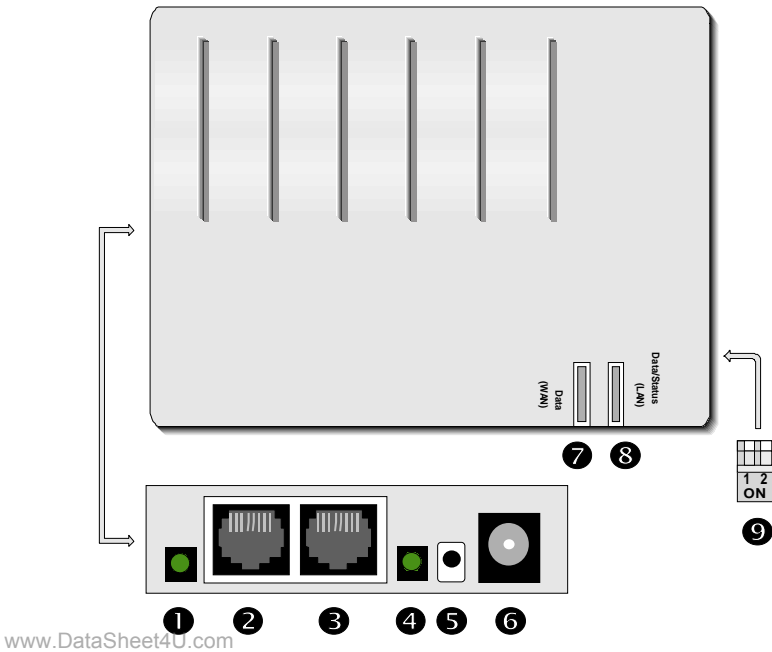


Figure 2: IP5020 Internet Access Server

Components

① LED Link Indicator (WAN Port)	Flashes when data is transmitted or received.
② WAN port (10BaseT)	Connect the 10BaseT cabling (RJ45 connector) for the External LAN, WAN, or DSL/Cable Modem here.
③ LAN port (Auto-sensing 10/100BaseT)	Connect the LAN cable (RJ45 connectors) from this port to a 10BaseT or 100BaseT hub.
④ LED Link Indicator (LAN Port)	Flashes when data is transmitted or received.
⑤ Reset Button	Used to reset (reboot) the IP5020.





6 Power port (12V)	Connect the power adapter here.
7 WAN Data LED	This will flash during normal operation, when data is transmitted or received through the WAN port.
8 LAN Data/Status LED	During normal operation, this will flash in Green. Orange indicates an error. See the following <i>LED Table</i> for more information.
9 DIP switches	Refer to <i>DIP Switches</i> on page 4.

LED Table

The *Data/Status* LED will flash in GREEN during normal operation, as data is transmitted or received through the *LAN* port. YELLOW indicates an error. Possible LED states are shown below.

LAN Data/Status LED	WAN Data LED	Description
On (Orange, then Green)	On	Normal start up (power ON) sequence.
On (Green)	On	Idle.
Flashing (Green)	Flashing	Normal Operation. The <i>Data/Status</i> LED will flash when data is transmitted or received through the <i>LAN</i> port. The <i>Data</i> LED will flash when data is transmitted or received through the <i>WAN</i> port.
Flashing Orange, Green, Orange, Green, ...		Hardware error. Contact your dealer for technical support.

DIP Switches

DIP Switch Setting	Description
A  1=off 2=off	Normal Operation
B  1=off 2=on	DHCP Server function disabled.
C  1=on 2=off	Restore Default IP Address and clear Password (See below)
D  1=on 2=on	Normal Operation.

Restore Default IP Address and Clear Password

If the IP5020's IP Address or password is lost, the following procedure can be used to recover from this situation.

1. Turn the power to the IP5020 OFF.
2. Set the DIP switches to position "C" in the table above.
3. Turn the power to the IP5020 ON.
4. Operate DIP switch 1 in the following sequence (you have 15 seconds to complete the sequence):
 - OFF
 - ON
 - OFF
5. The IP5020 will now reset, and the Yellow 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
 - The password cleared (no password).
6. You can now connect to the IP5020 and make any configuration changes required.



Note! If the DIP switches are simply left at position "C", the IP5020 will function normally.

Chapter 2

Installation

This Chapter explains how to install the IP5020 in your LAN.

Procedure

This section explains how to install the IP5020 Internet Access Server in your existing TCP/IP network.

Requirements

- Ethernet Network employing 10BaseT and the TCP/IP protocol.
- For Internet Access, an DSL or Cable modem, and an Internet Access account with a local ISP (Internet Service Provider).

Procedure

1. Choose an Installation Site

Select a suitable place on the network to install the IP5020.

2. Connect LAN Cable

Connect a 10BaseT cable from a Hub on your LAN to the LAN port on the IP5020.

3. Connect WAN Cable

Connect the 10BaseT cable from the external LAN, WAN, or DSL/Cable modem to the WAN port on the IP5020.

4. Connect Power Adapter

Connect the IP5020's power adapter to the IP5020 and power it ON.



Only use the power adapter provided. Using a different one may cause hardware damage.

5. Check the LEDs

When the IP5020 is powered On, the *Data/Status* LED should flash Orange, then turn Green. If it stays Orange, there is a hardware problem. For more information on the LEDs, refer to

LED on page 4.

Chapter 3

Configuration

This Chapter provides details of the configuration process.

Overview

This chapter describes the configuration and checking of the LAN and WAN ports.

PCs on your local LAN may also require configuration. For details, see *Chapter 4 - PC Configuration*. Also, if you are using DHCP, please read *Chapter 5 - DHCP*.

Other IP5020 configuration may also be required, depending on which features and functions of the IP5020 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 internal LAN.	Chapter 4: PC Configuration
Use DHCP on the internal LAN	Chapter 5: DHCP
Configure the IP5020 and routers for a LAN which has 1 or more routers.	Chapter 6: Routing
Set a password for the IP5020, or disable NAT (Network Address Translation).	Chapter 7: Device Options
Use any of the following features: <ul style="list-style-type: none"> • Special Internet Applications • Virtual Servers • Exposed Computer 	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 IP5020 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 IP5020, please check the following:

- Since configuration uses the LAN connection, the IP5020 must be installed and powered ON.
- If the IP5020's default IP Address (192.168.0.1) is already used by another device, the other device must be turned OFF until the IP5020 is allocated a new IP Address during configuration.

Connecting to the IP5020

To establish a connection from your PC to the device:

1. Start your WEB browser.
2. In the *Address* box, enter "HTTP://" and the IP Address of the IP5020, as in the following example:

HTTP://192.168.0.1

3. You should then see the *Home* screen. Select the desired option from the navigation bar.

If you can't connect

If the IP5020 does not respond, check the following:

- The IP5020 is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the IP5020 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 IP5020's default IP Address of 192.168.0.1. Also, check that the *Network Mask* is set to 255.255.255.0

In Windows, the IP Address can be checked by using *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

Password

If a password has been set for the device, you will be prompted for the password, as shown below.

Figure 3: 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. Instead, you will immediately see the **Home** screen, which contains helpful information for first-time users.

Navigation & Data Input

Most screens contain a navigation bar on the left of the screen allows you to move about. You can also use the "Back" button on your Browser.



***Note!** Changing to another screen without clicking "Save" does NOT save any changes you may have made. HTML uses "forms based input"; you must submit (save) the form or your data will be ignored.*

Home Screen

www.DataSheet4U.com

The **Home** screen is shown below. No data can be input from this screen.

Figure 4: Home Screen

Note that the navigation bar contains a **Help** button. Context-sensitive help is available from each screen. From this screen, the **Help** file provides links to all help files.

LAN Port Configuration

To configure the LAN port, select *Device - LAN Port*. You will see a screen like the example below.

LAN Port	
Internal LAN	Device IP Address <input style="width: 30px;" type="text" value="192"/> . <input style="width: 30px;" type="text" value="168"/> . <input style="width: 30px;" type="text" value="0"/> . <input style="width: 30px;" type="text" value="1"/> Network Mask <input style="width: 30px;" type="text" value="255"/> . <input style="width: 30px;" type="text" value="255"/> . <input style="width: 30px;" type="text" value="255"/> . <input style="width: 30px;" type="text" value="0"/>
DHCP Server	Operation <input checked="" type="radio"/> Enable <input type="radio"/> Disable Start IP Address <input style="width: 30px;" type="text" value="192"/> . <input style="width: 30px;" type="text" value="168"/> . <input style="width: 30px;" type="text" value="0"/> . <input style="width: 30px;" type="text" value="2"/> Finish IP Address <input style="width: 30px;" type="text" value="192"/> . <input style="width: 30px;" type="text" value="168"/> . <input style="width: 30px;" type="text" value="0"/> . <input style="width: 30px;" type="text" value="51"/> DNS (Domain Name Server) IP Addresses DNS (1) (Required) <input style="width: 30px;" type="text" value="0"/> . <input style="width: 30px;" type="text" value="0"/> . <input style="width: 30px;" type="text" value="0"/> . <input style="width: 30px;" type="text" value="0"/> DNS (2) (Optional) <input style="width: 30px;" type="text" value="0"/> . <input style="width: 30px;" type="text" value="0"/> . <input style="width: 30px;" type="text" value="0"/> . <input style="width: 30px;" type="text" value="0"/> DNS (3) (Optional) <input style="width: 30px;" type="text" value="0"/> . <input style="width: 30px;" type="text" value="0"/> . <input style="width: 30px;" type="text" value="0"/> . <input style="width: 30px;" type="text" value="0"/> (The first available DNS will be used.)
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 5: LAN Port

Data - LAN Port

For most users, the default values for these fields should be satisfactory.

Data - Internal LAN

Device IP Address	IP address for the IP5020. 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, use an 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 IP5020 is attached. i.e. the same value as the PCs on that LAN segment.

Data - DHCP Server

A DHCP (Dynamic Host Configuration Protocol) server provides a valid IP address (and the Gateway and DNS addresses) to a DHCP client (PC or device) upon request. The IP5020 can act as a **DHCP server**.

To use this feature:

- The IP5020 must be configured with the following data.
- The PCs must be configured to act a DHCP **clients**. This procedure is explained in *Chapter 5 - DHCP*.

Operation	<p>If Enabled, the IP5020 will function as a DHCP server. The default value is Enabled.</p> <p>If you already have a DHCP Server, this must be DISABLED.</p>
Start IP Address Finish IP Address	<p>The <i>IP Start Address</i> and <i>IP Finish Address</i> fields set the values used by the DHCP server.</p> <p>This range also determines the number of DHCP clients supported. (Maximum number of clients is 253.)</p>
DNS (Domain Name Server) IP Addresses	<p>Enter at least 1 DNS. Your ISP should recommend a DNS.</p> <p>If they don't, you can copy the public DNS entry from DNS (3) to DNS (1)</p> <p>Multiple DNS entries should be entered in the order you want them accessed. (The first available DNS will be used.)</p>

WAN Port Configuration

Data on the WAN port screen is used to identify this device to the remote LAN. The IP Address seen by the remote LAN is different to the IP Address on the local LAN.

To configure the WAN port, first select the appropriate connection type (*Direct Connection* or *PPPoE*) on the *Device* screen (below) and then click the “Configure” button.

<u>Device Options</u>	Set Password, NAT (Network Address Translation).
<u>LAN Port</u>	Configure the port used to connect this device to your local LAN, including the DHCP Server function.
<u>WAN Port</u>	<p>The WAN port is used to connect to the external LAN, WAN, or the Internet. Select the connection method used by the remote Server:</p> <p><input checked="" type="radio"/> Direct Connection to ISP or remote LAN (Fixed IP Address or DHCP Client)</p> <p><input type="radio"/> PPPoE (PPP Over Ethernet)</p> <p style="text-align: right;"><input type="button" value="Configure"/></p>

Figure 6: Device Screen

Tip:

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

Direct Connection Screen

www.DataSheet4U.com

WAN Port - Direct Connection

Device Name:

Hardware (MAC) Address:

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

IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Network Mask	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Gateway IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>

Figure 7: WAN Port – Fixed Connection

- Note that if IP Address entries are shown when *DHCP Client* is selected, then these values were supplied by the DHCP server on the remote LAN.
- The *Retrieve Defaults* button will recover the default *Device Name* and clear the other items. After clicking this button, you must click *Save* to restore the default values to the IP5020.

Data - WAN Port

Device Name	Used for identification. Normally, there is no need to change the default name, but if your ISP requests that you use a particular name, enter it here. This name will be provided to, and recorded by, the remote DHCP Server.
Hardware (MAC) Address	If your ISP asks for the <i>Network Adapter Address</i> , <i>Physical Address</i> , <i>Hardware Address</i> , or <i>MAC Address</i> for the PC the DSL/Cable modem is connected to, provide this value.
DHCP Client	Leave this enabled if you want the IP5020 to be allocated an IP Address by the DHCP server on the remote LAN, WAN, or ISP account. If this is enabled, the IP Address information below is NOT required.
Fixed IP Address	Select this if using a fixed IP Address. If this option is selected, the following data must be entered. <ul style="list-style-type: none"> • 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.

PPPoE Screen

WAN Port - PPPoE

Account/User Name

Password

Verify password

IP Address provided by ISP: Dynamic (allocated on connection)
 Fixed

Idle Time-out (minutes) (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 8: WAN Port - PPPoE

These settings must be correct in order to complete the remote connection. This data is provided by your ISP (Internet Service Provider).

Data – PPPoE Screen

Account/User Name	The name of the Internet account provided by your ISP.
Password	Enter the password for the above account.
Verify Password	Re-enter the password, to ensure it is correct.
IP Address provided by ISP <small>www.DataSheet4U.com</small>	Normally, this is Dynamic; use this setting if your ISP's data does not mention an IP Address. If your ISP did provide an IP Address, select Fixed and enter the value they provided.
Connect on Demand	Normally, this should be Enabled. If disabled, you must use the Connect button on the Status screen to establish a connection.
Idle Time-out	If an connection is inactive for longer than this time period, it will be terminated.
Buttons	<ul style="list-style-type: none"> • 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.

Status Screens

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

In either case the screen contains a hyperlink to jump to the *Device/LAN Status* screen.

WAN Status – Direct Connection

WAN Status - Direct Connection	
Physical Address	00-c0-02-99-99-77
I.P. Address	0.0.0.0
Network Mask	0.0.0.0
Default Gateway	0.0.0.0
DHCP Client	Enable
<input type="button" value="Reconnect"/> <input type="button" value="Refresh"/>	
<input type="button" value="Device/LAN Status"/>	

Figure 9: WAN Status – Direct Connection

Data

Physical Address	The "Hardware" address of this device, as seen by other devices on the external LAN or 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 External LAN or WAN.
DHCP Client	Displays "Enabled" or "Disabled", indicating whether this device is acting as a DHCP client on the external LAN or WAN.
Buttons	<ul style="list-style-type: none"> 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	
Status	Physical Address 00:C0:04:AA:00:06
	I.P. Address 172.3.1.4.23
	Network Mask 255.255.255.0
	PPPoE Link Status Connected
Log	PPP up successfully
<input type="button" value="Connect"/> <input type="button" value="Disconnect"/> <input type="button" value="Clear Log"/> <input type="button" value="Refresh"/>	
<input type="button" value="Device/LAN Status"/>	

Figure 10: WAN Status – PPPoE

Data

Physical Address	The hardware address of this device.
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.
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.

Log

- The Connection Log shows status messages relating to the existing connection.
- The most common messages are listed in the table below.
- The **Clear Log** button will restart the Log, while the **Refresh** button will update the messages shown on screen.

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.

Buttons and Links

- **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.
- **Device/LAN Status** - Use this link to jump to the "Device/LAN Status" screen.

Device/LAN Status Screen

The *Device/LAN Status* screen can be reached via the *Device/LAN status* hyper-link on the *WAN Status* screen. An example screen is shown below.

Device/LAN Status			
Device	Firmware Version	Version 6.0	
	Hardware ID	4f0007000000	
	Network Address Translation	Enable	
LAN Port	Physical Address	00-c0-02-99-99-76	
	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-c0-02-99-99-76	leased
	192.168.0.2	00-80-c8-44-25-1c	leased
	192.168.0.10	00-c0-a8-35-dd-f3	leased
Refresh			

Figure 11: Status Screen

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" or "Disabled".

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 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

This table will be empty unless the DHCP Server function is being used. If it is being used, this table lists the devices on the local LAN which have been allocated IP Addresses by the DHCP server function. Only IP Addresses in use will be listed.

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).

Chapter 4

PC Configuration

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

If you have a Router

If your If your LAN contains 1 or more Routers, do NOT change any TCP/IP settings on your PCs unless advised to do so by your LAN Administrator.



Note! *The Router itself must be configured. Refer to **Chapter 6 - Routing** for details.*

If you use DHCP

If you are already using DHCP, no PC configuration is required. However, you should check the DHCP Server configuration, as described in *Checking your DHCP Server* on page 24. Also, the DHCP Server function in the IP5020 should be turned OFF. This setting is on the *Internal LAN Port* screen.

If you are not using DHCP, but wish to do so, refer to *Using the IP5020's DHCP Server* on page 25.

No Router, no DHCP

If **your LAN is NOT using DHCP** and **does NOT contain a router**, check the following settings for each PC:

IP Address

Ensure that the IP Address for each PC is unique, and is from the same address range as the IP5020's *Device IP Address*, as set on the *LAN Port* screen.

For example, if the IP5020 uses the default IP Address (192.168.0.1) and Network Mask (255.255.255.0), the PCs must use addresses from 192.168.0.2 to 192.168.0.254.

Network Mask

All PCs, and the IP5020, need to be using the same value for the *Network Mask*. The default value is 255.255.255.0. On the IP5020, this value is set on the *LAN Port* screen.

Gateway

Set the *Default Gateway Address* to the IP5020's IP address (*Device IP Address*, as set on the *LAN Port* screen). The default IP Address is 192.168.0.1.

DNS (Domain Name Server) Address

This should match the DNS address entered into the *DNS IP Address* field on the *LAN Port* screen.

Operation - Internet Access

If you are using the IP5020 for Internet access:

- Ensure that the DSL modem, Cable modem, or other permanent connection is functional.
- Configure your Browser and E-Mail client to use Internet Access via the LAN, rather than a Dial-up connection. In Windows 95, select *Start Menu - Accessories - Internet Tools*. The Wizard called *Get on the Internet* or *Connection Wizard* can be used to set or change your Internet access method.
- 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 IP5020, 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 "IP5020".
- 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 "IP5020" location.



Chapter 5

DHCP

This Chapter covers the use of DHCP, using either an existing DHCP Server or the IP5020's DHCP Server function.

Overview

If your (internal) 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 normally 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 includes all the software required to act as a DHCP **client**.
- The IP5020 can act as a **DHCP server**.

Checking if your PC uses DHCP

Under Windows 95, you can check if your PC is acting as a DHCP client by using the following procedure. For other operating systems, check your system documentation.

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

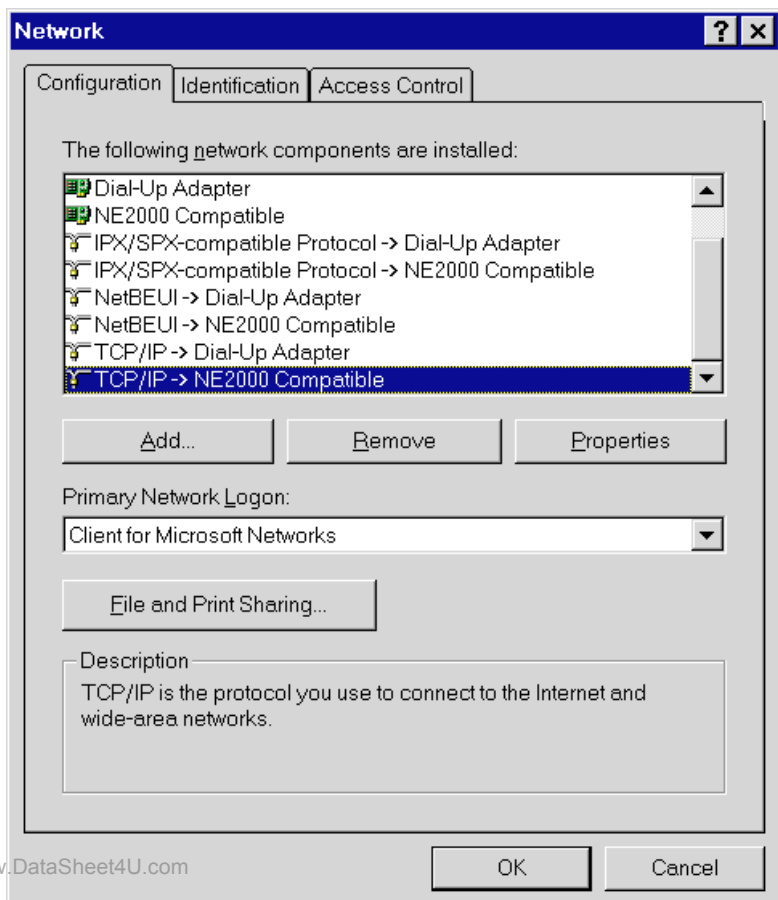


Figure 12: Network Configuration

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.

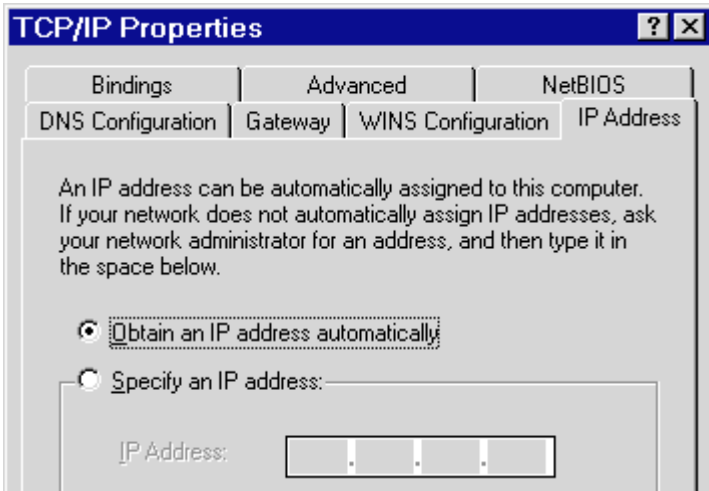


Figure 13: IP Address (Win 95)

4. If the radio button for "Obtain an IP address automatically" is checked, as shown above, then your PC is acting as a DHCP client.

Checking your DHCP Server

If you already have a DHCP Server:

- Check that the DHCP Server function in the IP5020 is **Disabled**. This setting is on the *LAN Port* screen.
- Check your DHCP Server, and ensure that:
 - **IP Address** assigned to the IP5020 (*Device IP Address*, set on the *LAN Port* screen) is compatible with the Address range used by the DHCP Server.
 - **Network Mask** matches the value entered on the IP5020's *LAN Port* screen.
 - **DNS IP Address** matches the value entered on the IP5020's *LAN Port* screen.
 - **Gateway** is set correctly. This depends on whether or not you have a router installed on your LAN, as shown by the following table.

www.DataSheet4U.com

No Router	Set the <i>Default Gateway Address</i> to the IP address (<i>Device IP Address</i> , set on the <i>LAN Port</i> screen) assigned to the IP5020. The default IP Address is 192.168.0.1.
Router	Do not change the <i>Default Gateway Address</i> . Instead, the router must be configured as explained in <i>Chapter 6 - Routing</i> .

Using the IP5020's DHCP Server

To use the IP5020's built-in DHCP Server function:

- Ensure that the IP5020's *DHCP Server* is **Enabled**, and the other DHCP data is correct. (Check the *Internal LAN Port* screen).
- Configure your PCs to act as DHCP clients, as described below.

To Configure your PCs to use DHCP

Your PCs must be configured to act as DHCP clients. For Windows 95, the procedure is detailed below. For other operating systems, check your system documentation.

Windows 95 DHCP Client Setup

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

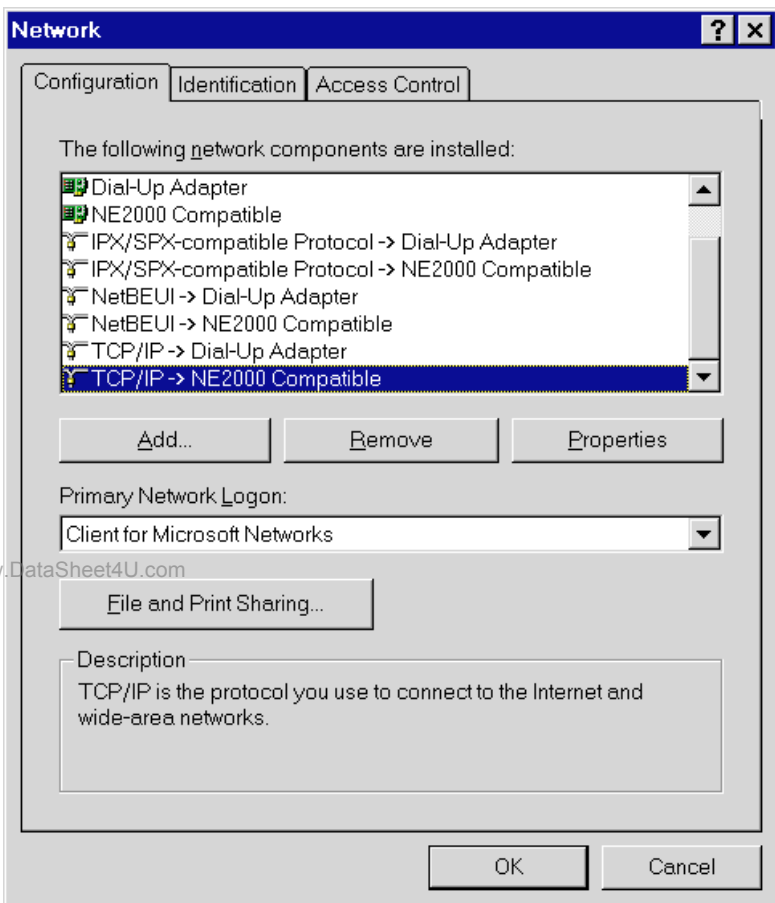


Figure 14: Network Configuration

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.

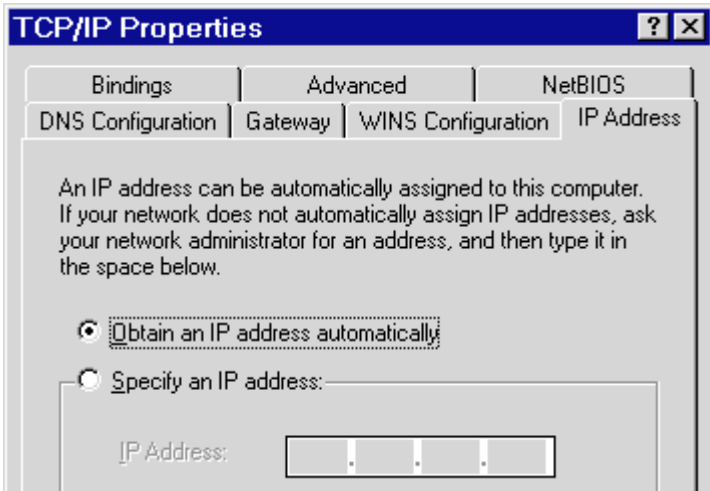


Figure 15: IP Address (Win 95)

4. Click on the radio button "Obtain an IP address automatically", as shown above. This sets the DHCP client ON.
5. Click on the *Gateway* tab.
The *Default Gateway Address* should be left blank. The DHCP server will provide this information.
6. Click on the *DNS Configuration* tab
The DNS (Domain Name Server) should be "Enabled" but the fields can be left blank. The DHCP server will provide this information also.



Note! To reserve an IP Address for a particular DHCP client, so that it always receives the same IP Address, refer to **Workstations** on page 44.

Chapter 6

Routing

This Chapter explains the Routing features of the IP5020.

Overview

While the IP5020 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 IP5020 correctly, as described in the following sections.



See page 29 for an example of configuring both the IP5020 and the Router.

IP5020 Configuration

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

Routing

Existing Entries in Routing Table

1) 172.17.0.0/255.255.0.0/192.168.0.20/1 Get Data

Clear Form

Routing Table

Destination IP Address

Network Mask

Gateway IP Address

Interface

Metric

Add Delete Update List All Cancel

Figure 16: Routing Screen

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 <i>Destination IP Address</i> . The 4 th (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 IP5020, 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 IP5020 as the *Default Route* or *Default Gateway*.

Local Router

The local router is the Router installed on the same LAN segment as the IP5020. This router requires that the *Default Route* is the IP5020 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 www.DataSheet4U.com	Normally 0.0.0.0, but check your router documentation.
Gateway IP Address	The IP Address of the IP5020.
Metric	1

Other Routers on the Local LAN

Other routers on the local LAN must use the IP5020's *Local Router* as the *Default Route*. The entries will be the same as the IP5020's local router, with the exception of the *Gateway IP Address*.

- For a router with a direct connection to the IP5020's local Router, the *Gateway IP Address* is the address of the IP5020's local router.
- For routers which must forward packets to another router before reaching the IP5020's local router, the *Gateway IP Address* is the address of the intermediate router.

Routing Example

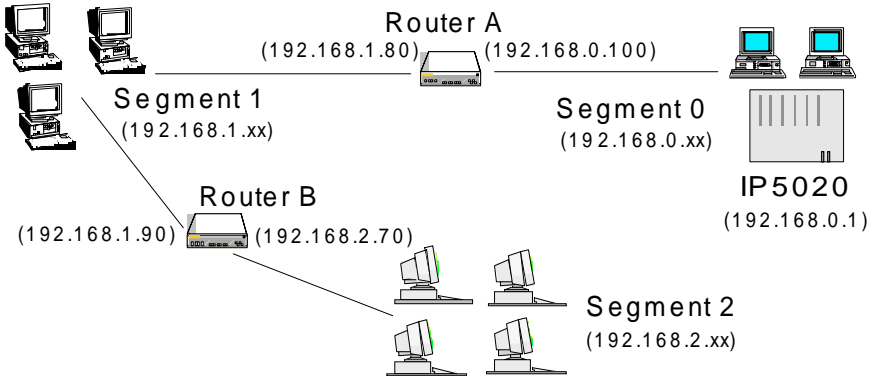


Figure 17: Routing Example

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

For the IP5020's Routing Table

The IP5020 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 (IP5020's local Router)
Entry 2 (Segment 2)	
Destination IP Address	192.168.2.0
Network Mask	255.255.255.0
Gateway IP Address	192.168.0.100

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 (IP5020'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 (IP5020's local router)

Chapter 7

Device Options

This Chapter details the options available on the IP5020's "Device Options" screen.

Overview

The *Device* screen is reached by selecting the *Device* on the navigation bar, then *Device Options*

The options available on this screen are:

- Password
- NAT (Network Address Translation)

An example screen is shown below.

Device Options	
Password	New password <input type="password"/> Verify password <input type="password"/>
NAT	NAT (Network Address Translation) allows LAN users to share the "WAN" (external) IP address, and also provides "Firewall" protection. <input checked="" type="radio"/> Enable NAT <input type="radio"/> Disable NAT
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

www.DataSheet4U.com **Figure 18: Device Options Screen**

Device 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.



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

If the password is lost, a DIP switch setting is available to clear the password. See the DIP Switch table on page 4 for details.

NAT (Network Address Translation)

NAT allows PCs on your LAN to use a local (internal) IP Address which is invalid on the Internet. NAT ensures that the local IP Addresses are invisible to external sources. Use the following to determine whether or not you need NAT.

- If using this device for Internet access, NAT **must be left On** unless PCs on your LAN have valid external IP Addresses.
- If this device is not being used to provide shared Internet access, NAT is not normally required.
- If NAT is disabled, the IP5020 will act as a static router, and the *Advanced Internet* features (Virtual Servers, Special Applications, and Exposed Computer) are no longer available.
- If NAT is disabled, the Firewall protection provided by the IP5020 is lost.

Chapter 8

Advanced Internet

This Chapter explains how to use the IP5020's "Advanced Internet" features.

Overview

For situations where the IP5020 is being used to provide shared Internet access, the following advanced features are provided.

- Special Applications
- Virtual Servers
- Exposed Computer

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 sample screen is shown below.

Advanced Internet Features	
Features - Operational Status	
Special Internet Applications	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Virtual Servers	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Exposed Computer	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	
Special Internet Applications	Configure for non-standard Internet applications.
Virtual Servers	Define servers on your LAN, so that Internet users can access them.
User-Defined Virtual Servers	Define non-standard Virtual Servers using port numbers.
Exposed Computer	Allows unrestricted 2-way Internet connection by 1 computer. Warning! This is a security risk.

Figure 19: Advanced Internet Screen

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

Special 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 *Advanced Internet - Special Applications*. An example screen is shown below.

Special Applications

Existing Special Applications

Name

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

Data for this Application

Name

Enable

Outgoing Control

Protocol:

Port Range: Start Finish

Incoming Data

Protocol:

Port Range: Start Finish

Figure 20: 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 "Exposed Computer" 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 Control

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 Data

Protocol	The protocol (TCP or UDP) used when the application or service sends data to you.
Port Range: Start	The beginning of the range of port numbers used by the application server when data is sent to you. 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, when data is sent to you.

Virtual Servers

This feature allows you to make a server 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.

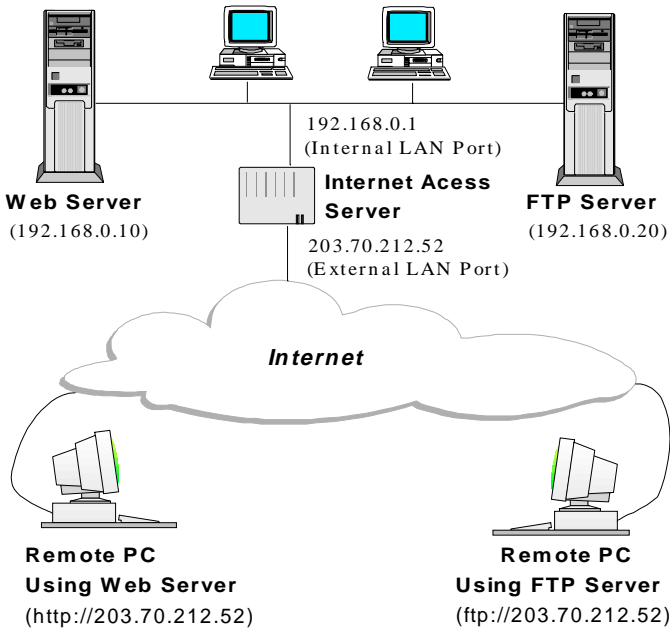


Figure 21: Virtual Servers

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 the *IP Address* on the *External LAN Port* screen. This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers.

Types of Virtual Servers

The IP5020 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 that the TOTAL number of Virtual Servers which can be used is 10.

Virtual Server Configuration

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

On	Type	IP Address			
<input type="checkbox"/>	DNS	0	0	0	0
<input type="checkbox"/>	Finger	0	0	0	0
<input checked="" type="checkbox"/>	FTP	192	168	0	20
<input type="checkbox"/>	Gopher	0	0	0	0
<input type="checkbox"/>	Mail (SMTP)	0	0	0	0
<input type="checkbox"/>	Mail (POP3)	0	0	0	0
<input type="checkbox"/>	News	0	0	0	0
<input type="checkbox"/>	Telnet	0	0	0	0
<input checked="" type="checkbox"/>	WEB Server	192	168	0	10
<input type="checkbox"/>	Whois	0	0	0	0

Save Cancel

Figure 22: Virtual Server Screen.

Simply select the Server type or types you wish to use, enter the IP Address of the server on your LAN, and click "Save".

User Defined Virtual Servers

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

The screen for this function is reached by selecting *Advanced Internet - User Defined Virtual Servers*. An example screen is shown below.

Figure 23: User Defined Virtual Servers

This database operates in the same way as the other databases:

- **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"

Configuration Data

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 <i>Internal Port Number</i> . If it is different, this device will perform a "mapping" or "translation" function, allowing you to configure the server to use one port address, while clients use a different port address

Connecting to the Virtual Servers

Once configured, anyone on the Internet can connect to your Virtual Servers. They must enter the IP Address shown in the *IP Address* on the *External LAN Port* screen as the destination.

e.g.

`http://203.70.212.52`

Using this Device as a Virtual Web Server

It is possible to configure the IP5020 itself as a Virtual Web Server. Once this is done, you can configure this device through the Internet.

For the remote PC, the destination IP Address is the *IP Address* shown on the *External LAN Port* screen.

Upon connecting to the IP5020, you will be prompted for the device password.



Note! Ensure that a password has been set!

To make the IP5020 a Virtual Web Server:

- Enable *Virtual Server* on the *Advanced Internet* screen
- Enable *Web Server* on the *Virtual Servers* screen.
- Enter the *Device IP Address* (from the *Internal LAN Port* screen) as the IP Address of the Web Server.

Exposed Computer

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 "Exposed Computer" and other Internet users or Servers.

- Internet users will see the PC as having the *IP Address* shown on the *External LAN Port* screen of this device. (This is the same IP Address used by the Virtual Servers.)
- Any Internet user who knows this address can connect to the *Exposed Computer*. (What happens after connection depends on what software both computers are using).

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.



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 Exposed Computer

Select *Advanced Internet* from the navigation bar, then *Exposed Computer*. You will see a screen like the following:

Exposed Computer

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

Because of the security risk, this feature should be activated only when required.

Exposed Computer

LAN IP Address . . .

Figure 24: Exposed Computer Screen

Data

The only data required is the *LAN IP Address*. Enter the IP Address of the PC on your LAN which will become the "Exposed Computer".

Checking

Once configured and enabled, the *Exposed Computer* should respond to a "ping" from any PC connected to the Internet. The "ping" command can be entered in the *Run* dialog, as follows:

```
ping ip_address
```

Where *ip_address* is the *IP Address* shown on the *External LAN Port* screen of this device.

Chapter 9

Access Control

This Chapter explains how to configure and use the IP5020's "Access Control" feature.

Overview

The Access Control feature allows administrators to restrict Internet Access by individual workstations. 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. By default, all PCs are in the "Everyone" group unless explicitly moved to another group, using the *Workstation* screen.
- Set the desired restrictions on the other groups ("Group 1", "Group 2", etc) as needed.
- For each Workstation you wish to move from the "Everyone" group, enter their details on the *Workstation* screen, and assign them to the desired group



You can limit Internet access for ALL PCs without entering ANY workstation 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

Group
Get Data
Clear Form

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

Internet Access for this Group

No restrictions
 Block all Access
 Use Packet Filter Table below

Packet Filter Table

Check items you wish to block (discard).

Applications to Block	TCP Packets to Discard
<input type="checkbox"/> Archie <input type="checkbox"/> DNS <input type="checkbox"/> E-Mail <input type="checkbox"/> FTP <input type="checkbox"/> Gopher <input type="checkbox"/> News <input type="checkbox"/> SNMP <input type="checkbox"/> Telnet <input type="checkbox"/> TFTP <input type="checkbox"/> WWW	<div style="border: 1px solid gray; padding: 2px; display: inline-block; margin-bottom: 5px;">6667 Chat</div> <div style="border: 1px solid gray; padding: 2px; display: inline-block; margin-bottom: 5px;">79 Finger</div> <div style="border: 1px solid gray; padding: 2px; display: inline-block; margin-bottom: 5px;">7070 Raudio</div>
	Select items to block.
	Created in "Administrator Defined Filters"
UDP Packets to Discard	
	<div style="border: 1px solid gray; width: 40px; height: 20px; margin-bottom: 5px;"></div>
	Select items to block.
	Created in "Administrator Defined Filters"

Save
Cancel

Figure 25: Security Groups Screen

www.DataSheet4U.com

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 Workstations to a Security Group**
 All Workstations are automatically in the "Everyone" group. Use the *Workstations* screen to move them to another group if required.

Data

The following data is required.

Internet Access for this Group

There are 3 options:

- **No restrictions** - No packets are blocked. Use this to create an "Unlimited Access" group, or to temporarily remove restrictions from a group.
- **Block all Access** - Groups 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.

Packet Filter Table

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 *UDP Packets to Discard* column.

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 <i>Administrator Defined Filters</i> 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 <i>Administrator Defined Filters</i> 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 "Administrator Defined Filters" on page 45.

Workstations

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

The screenshot shows a web interface titled "Workstations". At the top, there is a "Name" dropdown menu with "temp_staff" selected, and two buttons: "Get Data" and "Clear Form". Below this is a text instruction: "Click 'Get Data' to see correct data for selected item." The main form area contains the following fields: "Workstation Name" (text box with "temp_staff"), "Network Adapter Address" (text box with "0000E812E007"), "Reserve entry in DHCP Table" (checkbox, unchecked), "Reserved IP Address" (four text boxes each containing "0"), and "Security Group" (dropdown menu with "Group 1" selected). At the bottom of the form are five buttons: "Add", "Delete", "Update", "List All", and "Cancel".

Figure 26: Workstations Screen

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

Operations

- To Add a New Workstation:**
 Ignore the drop-down box, click the *Clear Form* button, and enter the Workstation details in the fields provided.
 Click *Add* when finished.
- To Delete an Existing Workstation:**
 Select the Workstation from the drop-down box, click *Get Data* to view the information and confirm that this is the correct Workstation, then click the *Delete* button.
- To Change an Existing Workstation's Details:**
 Select the Workstation 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 Workstations:**
 Just click on the *List All* button.

Data

Workstation Name	Enter a name to identify this workstation.
Network Adapter Address	Hardware address for this workstation. 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 workstation. 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 <i>Device - Internal LAN Port</i> screen).
Security Group	Select the security group for this workstation. If you only wish to reserve an IP Address, and are not using the security (access control) features, simply leave this at "Everyone".

Administrator Defined Filters

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

Administrator Defined Filters

Create filters by defining packets to be **Filtered Out**.

TCP Packets		UDP Packets	
Name	Port No.	Name	Port No.
WWW	<input type="text" value="80"/>	DNS	<input type="text" value="53"/>
<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>
<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>
<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>
<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>
<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>
<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>
<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>
<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>
<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>

Figure 27: Administrator Defined Filters

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.

Name	Enter a descriptive name for this entry.
-------------	--

Port No.	Enter an integer representing the Port Number for this type of packet. A Network Analyzer or Packet Sniffer can be used to determine the correct port number.
-----------------	---

UDP Packets

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

Name	Enter a descriptive name for this entry.
Port No.	Enter an integer representing the Port Number for this type of packet. 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 IP5020 and some possible solutions to them. If you follow the suggested steps and the IP5020 still does not function properly, contact your dealer for further advice.

General Problems

Problem 1: Can't connect to the IP5020 to configure it.

Solution 1: Check the following:

- The IP5020 is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the IP5020 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 IP5020's default IP Address of 192.168.0.1. Also, the Network Mask should be set to 255.255.255.0 to match the IP5020.

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 workstations IP settings are correct (IP address, Network Mask, Default gateway and DNS).
- If the PCs are configured correctly, but still not working, check the IP5020. 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 IP5020 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 IP5020.

Solution 2: The IP5020 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 *Exposed Computer* 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 *Exposed Computer* feature is being used, the *Special Applications* and *Virtual Server* features should be disabled.



Appendix B

Specifications

IP5020 Internet Access Server

Model No.:	IP5020
Dimensions	120mm(W) * 93mm(D) * 30mm(H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol:	TCP/IP
Network Interface:	2 Ethernet: 1 * 10/100BaseT (RJ45) 1 * 10BaseT (RJ45)
LEDs	2
External Power Adapter	12 V DC