



xDSL/Cable Broadband Router

DC-202

---

***Full manual***

---

**Copyright**

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission.

**Trademarks**

All products, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

**FCC Interference Statement**

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

**CE Declaration of Conformity**

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B.

The specification is subject to change without notice.

# Table of Contents

<b>CHAPTER 1 INTRODUCTION.....</b>	<b>5</b>
1.1 FUNCTIONS AND FEATURES .....	5
1.1.1 Router Basic functions .....	5
1.1.2 functions .....	<b>Error! Bookmark not defined.</b>
1.1.3 Security functions .....	6
1.1.4 Advanced functions .....	6
1.1.5 Other functions .....	7
1.2 PACKING LIST .....	8
<b>CHAPTER 2 HARDWARE INSTALLATION.....</b>	<b>9</b>
2.1 PANEL LAYOUT .....	9
2.1.1. Front Panel .....	9
2.1.2. Rear Panel .....	10
2.2 PROCEDURE FOR HARDWARE INSTALLATION .....	11
2.2.1 Decide where to place your Broadband Router.....	11
2.2.2 Setup LAN connection.....	11
2.2.3 Setup WAN connection .....	11
2.2.4 Power on.....	11
<b>CHAPTER 3 NETWORK SETTINGS AND SOFTWARE INSTALLATION .....</b>	<b>13</b>
3.1 MAKE CORRECT NETWORK SETTINGS OF YOUR COMPUTER.....	13
<b>CHAPTER 4 CONFIGURING BROADBAND ROUTER .....</b>	<b>15</b>
4.1 START-UP AND LOG IN .....	16
4.2 STATUS .....	17
4.3 SETUP WIZARD.....	18
4.4 BASIC SETTING .....	20
4.4.1 Setup – Manual configuration and Virtual Computers .....	20
4.4.1.1 Static IP Address.....	21
4.4.1.2 Dynamic IP Address.....	22
4.4.1.3 Dynamic IP Address with Road Runner Session Management .....	22
4.4.1.4 PPP over Ethernet.....	22
4.4.1.5 PPTP.....	22
4.4.2 DHCP Server.....	23
4.4.4 Change Password .....	24
4.5 ADVANCED SETTINGS .....	25
4.5.1 Virtual Server.....	25

4.5.2	<i>Special AP</i>	26
4.5.3	<i>Miscellaneous Items</i>	27
4.5.4	<i>Logs</i>	28
4.5.5	<i>Dynamic DNS</i>	29
4.5.6	<i>SNMP Setting</i>	30
4.5.7	<i>Routing Table</i>	31
	Configuration on NAT Router	32
4.5.8	<i>Schedule</i>	33
4.6	SECURITY SETTINGS	34
4.6.1	<i>Packet Filter</i>	34
4.6.1.1	Inbound Filter:	34
4.6.1.2	Outbound Filter	36
4.6.2	<i>Domain Filter</i>	39
4.6.3	<i>URL Blocking</i>	41
4.6.4	<i>MAC Address Control</i>	43
4.6.5	<i>Miscellaneous Items</i>	45
4.7	TOOLBOX	46
4.7.1	<i>System Log</i>	46
4.7.2	<i>Firmware Upgrade</i>	46
4.7.3	<i>Miscellaneous Items</i>	47
4.7.4	<i>System Time</i>	48
4.7.5	<i>Backup Setting</i>	49
4.7.6	<i>Reset to default</i>	49
4.7.7	<i>Reboot</i>	49
<b>APPENDIX A TCP/IP CONFIGURATION FOR WINDOWS 95/98</b>		<b>50</b>
<b>APPENDIX B FAQ AND TROUBLESHOOTING</b>		<b>57</b>
	RESET TO FACTORY DEFAULT	57

# **Chapter 1 Introduction**

Congratulations on your purchase of this outstanding Broadband Router. This product is specifically designed for Small Office and Home Office needs. It provides a complete SOHO solution for Internet surfing, and is easy to configure and operate even for non-technical users. Instructions for installing and configuring this product can be found in this manual. Before you install and use this product, please read this manual carefully for fully exploiting the functions of this product.

## **1.1 Functions and Features**

### **1.1.1 Router Basic functions**

- **Auto-sensing Ethernet Switch**

Equipped with a 4-port auto-sensing Ethernet switch.

- **WAN type supported**

The router supports some WAN types, Static, Dynamic, PPPoE , PPTP , Dynamic IP with Road Runner.

- **Firewall**

All unwanted packets from outside intruders are blocked to protect your Intranet.

- **DHCP server supported**

All of the networked computers can retrieve TCP/IP settings automatically from this product.

- **Web-based configuring**

Configurable through any networked computer's web browser using Netscape or Internet Explorer.

- **Virtual Server supported**

Enable you to expose WWW, FTP and other services on your LAN to be accessible to Internet users.

- **User-Definable Application Sensing Tunnel**

User can define the attributes to support the special applications requiring multiple connections, like Internet gaming, video conferencing, Internet telephony and so on, then this product can sense the application type and open multi-port tunnel for it.

- **DMZ Host supported**

Lets a networked computer be fully exposed to the Internet; this function is used when special application sensing tunnel feature is insufficient to allow an application to function correctly.

- **Statistics of WAN Supported**

Enables you to monitor inbound and outbound packets

### 1.1.2 Security functions

- **Packet filter supported**

**Packet Filter** allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.

- **Domain Filter Supported**

Let you prevent users under this device from accessing specific URLs.

- **URL Blocking Supported**

URL Blocking can block hundreds of websites connection by simply a keyword.

- **VPN Pass-through**

The router also supports VPN pass-through.

- **SPI Mode Supported**

When SPI Mode is enabled, the router will check every incoming packet to detect if this packet is valid.

- **DoS Attack Detection Supported**

When this feature is enabled, the router will detect and log the DoS attack comes from the Internet.

### 1.1.3 Advanced functions

- **System time Supported**

Allow you to synchronize system time with network time server.

- **E-mail Alert Supported**

The router can send its info by mail.

- **Dynamic dns Supported**

At present, the router has 3 ddns.dyndns, TZO.com and dhs.org.

- **SNMP Supported**

The router supports basic SNMP function.

- **Routing Table Supported**

Now, the router supports static routing.

- **Schedule Rule supported**

Customers can control some functions, like virtual server and packet filters when to access or when to block.

#### **1.1.4 Other functions**

- **UPNP (Universal Plug and Play) supported**

The router also supports this function. The applications: X-box, Msn Messenger.

## 1.2 Packing List

- broadband router unit
- Installation CD-ROM
- Power adapter
- CAT-5 UTP Fast Ethernet cable



## Chapter 2 Hardware Installation

### 2.1 Panel Layout

#### 2.1.1. Front Panel

LEDs:

LED	Function	Color	Status	Description
POWER	Power indication	Green	On	Power is being applied to this product.
M1	System status indicators	Green	Blinking	M1 is flashed once per second to indicate system is alive.
WAN	WAN port activity	Green	On	The WAN port is linked.
			Blinking	The WAN port is sending or receiving data.
Link/Act. 1~4	Link status	Green	On	An active station is connected to the corresponding LAN port.
			Blinking	The corresponding LAN port is sending or receiving data.
10/100	Data Rate	Green	On	Data is transmitting in 100Mbps on the corresponding LAN port.

## 2.1.2. Rear Panel

Ports:

<b>Port</b>	<b>Description</b>
<b>PWR</b>	Power inlet
<b>WAN</b>	the port where you will connect your cable (or DSL) modem or Ethernet router.
<b>Port 1-4</b>	the ports where you will connect networked computers and other devices.
<b>Reset</b>	To reset system settings to factory defaults

## 2.2 Procedure for Hardware Installation

### 2.2.1 Decide where to place your Broadband Router

You can place your Broadband Router on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your Broadband Router in the center of your office (or your home) in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to power and network connection.

### 2.2.2 Setup LAN connection

- a. Wired LAN connection: connects an Ethernet cable from your computer's Ethernet port to one of the LAN ports of this product.
- b. LAN connection: locate this product at a proper position to gain the best transmit performance.

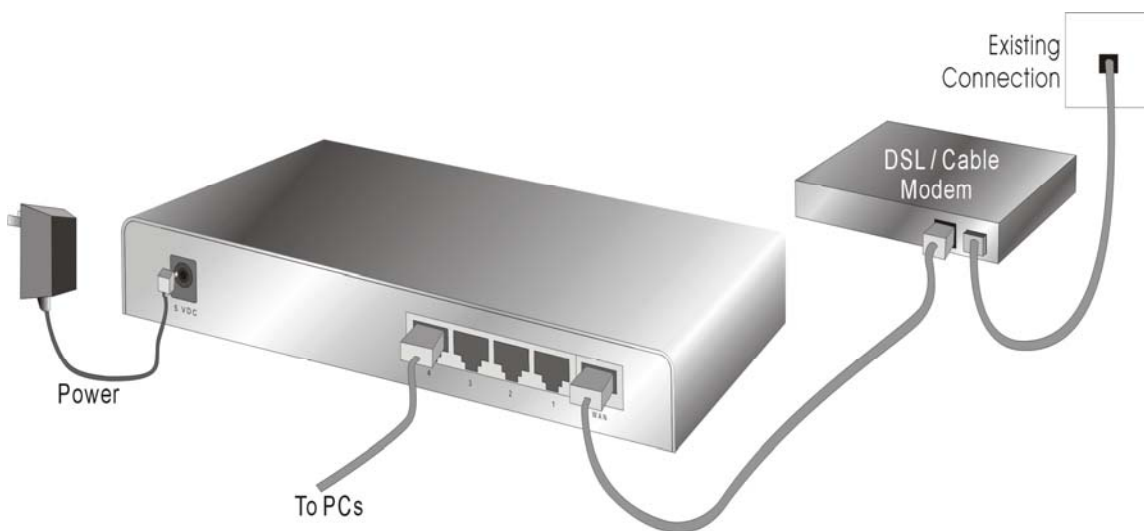


Figure 2-3 Setup of LAN and WAN connections for this product.

### 2.2.3 Setup WAN connection

Prepare an Ethernet cable for connecting this product to your cable/xDSL modem or Ethernet backbone. Figure 2-3 illustrates the WAN connection.

### 2.2.4 Power on

Connecting the power cord to power inlet and turning the power switch on, this product will automatically enter the self-test phase. When it is in the self-test phase, the indicators M1 will be lighted ON for about 10 seconds, and then M1 will be flashed 3 times to indicate that the self-test operation has finished. Finally, the M1 will be continuously flashed once

per second to indicate that this product is in normal operation.

## **Chapter 3 Network Settings and Software**

### **Installation**

To use this product correctly, you have to properly configure the network settings of your computers and install the attached setup program into your MS Windows platform (Windows 95/98/NT/2000).

#### **3.1 Make Correct Network Settings of Your Computer**

The default IP address of this product is 192.168.123.254, and the default subnet mask is 255.255.255.0. These addresses can be changed on your need, but the default values are used in this manual. If the TCP/IP environment of your computer has not yet been configured, you can refer to **Appendix A** to configure it. For example,

1. configure IP as 192.168.123.1, subnet mask as 255.255.255.0 and gateway as 192.168.123.254, or more easier,
2. configure your computers to load TCP/IP setting automatically, that is, via DHCP server of this product.

After installing the TCP/IP communication protocol, you can use the **ping** command to check if your computer has successfully connected to this product. The following example shows the ping procedure for Windows 95 platforms. First, execute the **ping** command

```
ping 192.168.123.254
```

If the following messages appear:

```
Pinging 192.168.123.254 with 32 bytes of data:
```

```
Reply from 192.168.123.254: bytes=32 time=2ms TTL=64
```

a communication link between your computer and this product has been successfully established. Otherwise, if you get the following messages,

```
Pinging 192.168.123.254 with 32 bytes of data:
```

```
Request timed out.
```

There must be something wrong in your installation procedure. You have to check the following items in sequence:

1. Is the Ethernet cable correctly connected between this product and your computer?

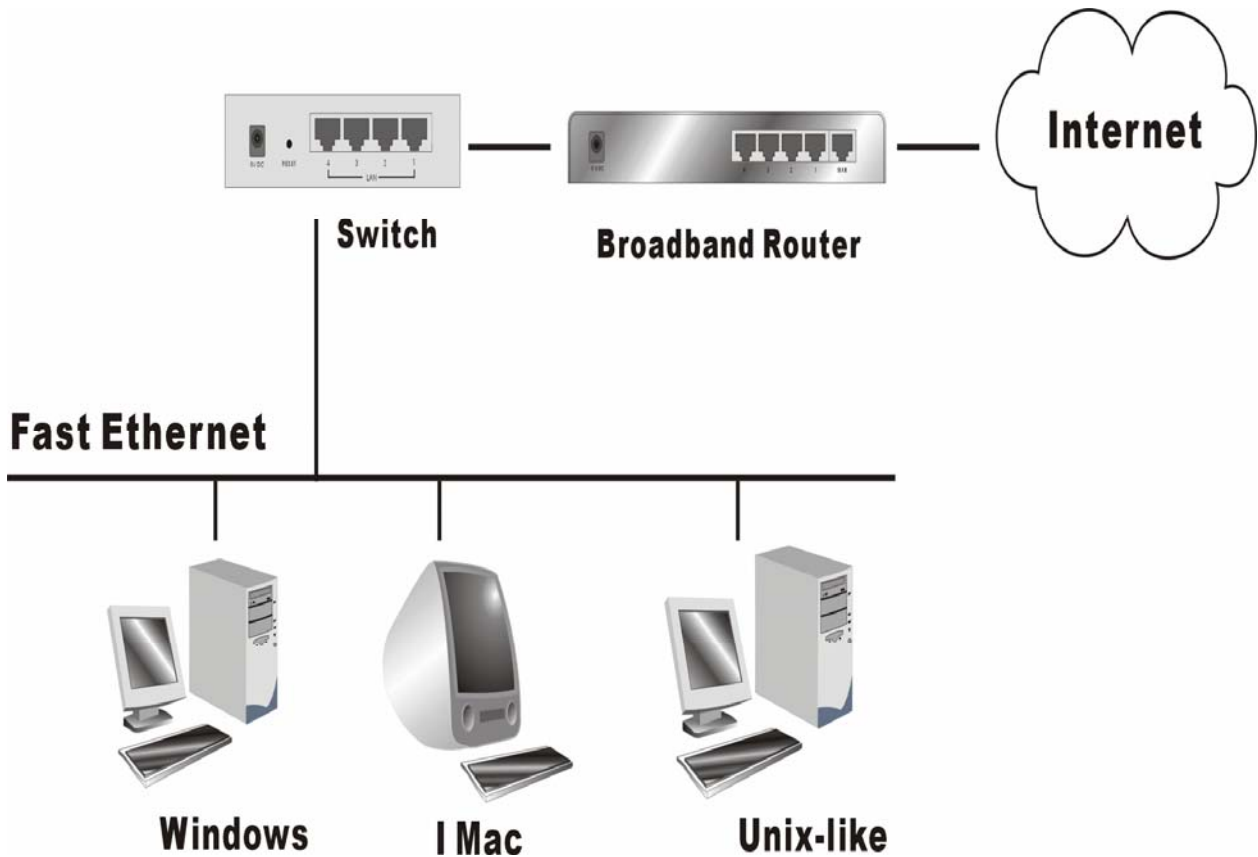
**Tip:** The LAN LED of this product and the link LED of network card on your computer must be lighted.

2. Is the TCP/IP environment of your computers properly configured?

**Tip:** If the IP address of this product is 192.168.123.254, the IP address of your computer must be 192.168.123.X and default gateway must be 192.168.123.254.

## **Chapter 4 Configuring Broadband Router**

This product provides Web based configuration scheme, that is, configuring by your Web browser, such as Netscape Communicator or Internet Explorer. This approach can be adopted in any MS Windows, Macintosh or UNIX based platforms.



## 4.1 Start-up and Log in

Activate your browser, and **disable the proxy** or **add the IP address of this product into the exceptions**. Then, type this product's IP address in the Location (for Netscape) or Address (for IE) field and press ENTER. For example: **http://192.168.123.254**.

After the connection is established, you will see the web user interface of this product. There are two appearances of web user interface: for general users and for system administrator.

To log in as an administrator, enter your login name and password (default: *admin/admin*) and click **OK**. If the password is correct, the web appearance will be changed into administrator configure mode. As listed in its main menu, there are several options for system administration.



## 4.2 Status

This option provides the function for observing this product's working status:

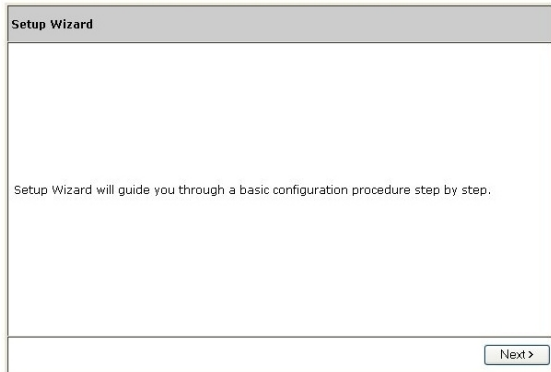
A. **WAN Port Status.**

If the WAN port is assigned a dynamic IP, there may appear a "**Renew**" or "**Release**" button on the Side note column. You can click this button to renew or release IP manually.

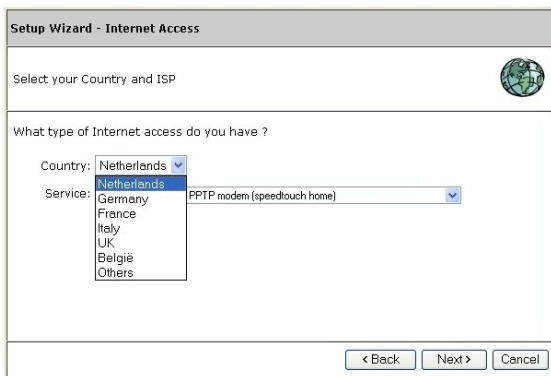
B. **Statistics of WAN:** enables you to monitor inbound and outbound packets

## 4.3 Setup wizard

1. Click **Wizard** to configure the router.
2. The **Setup wizard** will now be displayed; check that the modem is connected and click on **Next**.



3. Select your country from the **Country** list.



4. From **Service**, select your internet provider. Click **Next**.



5. Depending on the chosen provider, you may need to enter your user name and password and MAC address or hostname in the following window. Then click on **Next**.

The image shows two side-by-side screenshots of the 'Setup Wizard' configuration window. Both windows have a title bar 'Setup Wizard' and a globe icon. The left window is titled 'Check the data supplied by your ISP.' and shows the 'Login method' set to 'PPTP'. It includes input fields for 'Username', 'Password', 'Server IP Address' (10.0.0.138), 'IP Address' (10.0.0.150), and 'Subnet Mask' (255.255.255.0). The 'DNS' section has 'Automatic(Obtain from Server)' selected. The right window also has the title 'Check the data supplied by your ISP.' and shows the 'Login method' set to 'Dynamic IP Address'. It includes a 'WAN's MAC Address' field (00-50-18-21-B6-DB) with a 'Clone MAC' button. The 'DNS' section has 'Automatic(Obtain from Server)' selected. Both windows have '< Back', 'Next >', and 'Cancel' buttons at the bottom.

6. Click **Reboot** to complete the configuration.

The image shows a 'Setup Wizard' window with a grey title bar. The main content area contains the text 'Configuration is complete.' in bold, followed by 'The changes will not take effect until rebooting. Please click Reboot.' in a smaller font. At the bottom right, there are two buttons: '< Back' and 'Reboot'.

7. The configuration is now completed.  
8. Click **OK** to reboot the router and commit the changes.



9. Wait for about 10 seconds to see if the Internet connection is available otherwise, if you are using a PPTP or PPPoE connection please click **Connect** in the following window.

## System Status

Item	WAN Status	Sidenote
IP Address	0.0.0.0	PPTP
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	Unreachable
Domain Name Server	0.0.0.0	
Connection Time	-	<a href="#">Connect</a>

Statistics of WAN	Inbound	Outbound
Octets	0	0
Unicast Packets	0	0
Non-unicast Packets	0	0

10. The router will now connect to the Internet.

## 4.4 Basic Setting

### 4.4.1 Setup – Manual configuration

Home Wizard Basic Settings Security Settings Advanced Settings Toolbox DC-202

## Basic Settings

Set-up DHCP Password

Item	Setting
LAN IP Address	192.168.123.254
WAN Type	Dynamic IP Address <a href="#">Change...</a>
Host Name	<input type="text"/> (optional)
WAN's MAC Address	00-50-18-21-B8-1D <a href="#">Clone MAC</a>
Renew IP Forever	<input type="checkbox"/> Enable (Auto-reconnect)

Save Undo Virtual Computers... Help

INTERNET

ROUTER

Broadband xDSL/Cable Router

INTERNET NETWORK CONNECTIVITY

**SITECOM**  
EXPANDING POSSIBILITIES

Press "Change"



Home Wizard Basic Settings Security Settings Advanced Settings Toolbox DC-202

# Basic Settings

Set-up DHCP Password


Type	Usage
<input type="radio"/> Static IP Address	ISP assigns you a static IP address.
<input type="radio"/> Dynamic IP Address	Obtain an IP address from ISP automatically.
<input type="radio"/> Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond)	
<input type="radio"/> PPP over Ethernet	Some ISPs require the use of PPPoE to connect to their services.
<input checked="" type="radio"/> PPTP	Some ISPs require the use of PPTP to connect to their services.
<input type="radio"/> L2TP	Some ISPs require the use of L2TP to connect to their services.

Save Cancel

Broadband xDSL/Cable Router

INTERNET NETWORK CONNECTIVITY



EXPANDING POSSIBILITIES

This option is primary to enable this product to work properly. The setting items and the web appearance depend on the WAN type. Choose correct WAN type before you start.

1. **LAN IP Address:** the local IP address of this device. The computers on your network must use the LAN IP address of your product as their Default Gateway. You can change it if necessary.
2. **WAN Type:** WAN connection type of your ISP. You can click **Change** button to choose a correct one from the following four options:
  - A. **Static IP Address:** ISP assigns you a static IP address.
  - B. **Dynamic IP Address:** Obtain an IP address from ISP automatically.
  - C. **Dynamic IP Address with Road Runner Session Management.**(e.g. Telstra BigPond)
  - D. **PPP over Ethernet:** Some ISPs require the use of PPPoE to connect to their services.
  - E. **PPTP:** Some ISPs require the use of PPTP to connect to their services.

#### 4.4.1.1 Static IP Address

WAN IP Address, Subnet Mask, Gateway, Primary and Secondary DNS: enter the proper setting provided by your ISP.

#### 4.4.1.2 Dynamic IP Address

1. Host Name: optional. Required by some ISPs, for example, @Home.
2. Renew IP Forever: this feature enables this product to renew your IP address automatically when the lease time is expiring-- even when the system is idle.

#### 4.4.1.3 Dynamic IP Address with Road Runner Session Management

1. LAN IP Address is the IP address of this product. It must be the default gateway of your computers.
2. WAN Type is Dynamic IP Address. If the WAN type is not correct, change it!
3. Host Name: optional. Required by some ISPs, e.g. @Home.
4. Renew IP Forever: this feature enable this product renew IP address automatically when the lease time is being expired even the system is in idle state.

#### 4.4.1.4 PPP over Ethernet

1. PPPoE Account and Password: the account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it empty.
2. PPPoE Service Name: optional. Input the service name if your ISP requires it. Otherwise, leave it blank.
3. Maximum Idle Time: the amount of time of inactivity before disconnecting your PPPoE session. Set it to zero or enable Auto-reconnect to disable this feature.
4. **Maximum Transmission Unit (MTU)**: Most ISP offers MTU value to users. The most common MTU value is 1492.

#### 4.4.1.5 PPTP

1. My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned to you.
2. Server IP Address: the IP address of the PPTP server.
3. PPTP Account and Password: the account and password your ISP assigned to you. If you don't want to change the password, keep it empty.
4. Connection ID: optional. Input the connection ID if your ISP requires it.
5. Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will connect to ISP automatically, after system is restarted or connection is dropped.

Home Wizard Basic Settings Security Settings Advanced Settings Toolbox DC-202

## Basic Settings

Set-up DHCP Password

Item	Setting
▶ LAN IP Address	192.168.123.254
▶ WAN Type	PPTP <span>Change...</span>
▶ My IP Address	0.0.0.0
▶ My Subnet Mask	255.255.255.0
▶ Server IP Address	
▶ PPTP Account	
▶ PPTP Password	
▶ Connection ID	(optional)
▶ Maximum Idle Time	600 seconds <input type="checkbox"/> Auto-reconnect

Save Undo Help Reboot

Saved! The change doesn't take effective until rebooting!

Broadband xDSL/Cable Router

INTERNET
 NETWORK
 CONNECTIVITY

### 4.4.2 DHCP Server

Home Wizard Basic Settings Security Settings Advanced Settings Toolbox DC-202

## Basic Settings

Set-up DHCP Password

Item	Setting
▶ DHCP Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
▶ IP Pool Starting Address	100
▶ IP Pool Ending Address	199
▶ Domain Name	
▶ Primary DNS	0.0.0.0
▶ Secondary DNS	0.0.0.0
▶ Primary WINS	0.0.0.0
▶ Secondary WINS	0.0.0.0
▶ Gateway	0.0.0.0 (optional)

Save Undo Clients List... Fixed Mapping... Help

Broadband xDSL/Cable Router

INTERNET
 NETWORK
 CONNECTIVITY

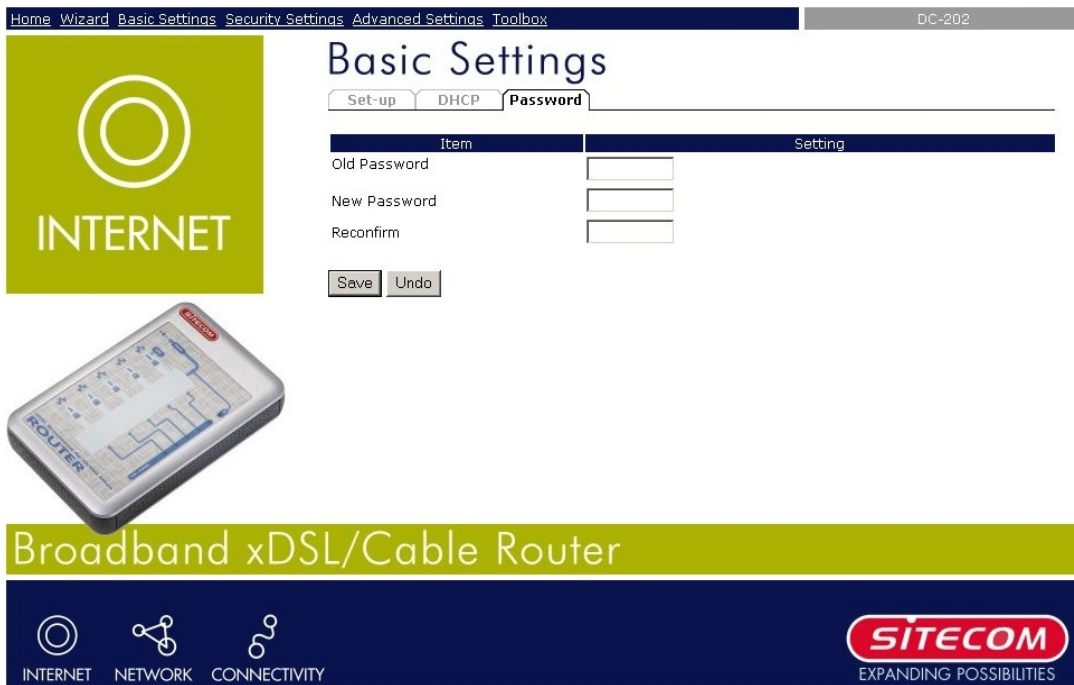
Press **"More>>"**

The settings of a TCP/IP environment include host IP, Subnet Mask, Gateway, and DNS configurations. It is not easy to manually configure all the computers and devices in your network. Fortunately, DHCP Server provides a rather simple approach to handle all these settings. This product supports the function of DHCP server. If you enable this product's DHCP server and configure your computers as "automatic IP allocation" mode, then when

your computer is powered on, it will automatically load the proper TCP/IP settings from this product. The settings of DHCP server include the following items:

1. **DHCP Server:** Choose "Disable" or "Enable."
2. **Lease Time:** this feature allows you to configure IP's lease time (DHCP client).
3. **IP pool starting Address/ IP pool starting Address:** Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.
4. **Domain Name:** Optional, this information will be passed to the client.
5. **Primary DNS/Secondary DNS:** This feature allows you to assign DNS Servers
6. **Primary WINS/Secondary WINS:** This feature allows you to assign WINS Servers
7. **Gateway:** The Gateway Address would be the IP address of an alternate Gateway. This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.

#### 4.4.3 Change Password



The screenshot shows the router's web interface. At the top, there is a navigation menu with links: Home, Wizard, Basic Settings, Security Settings, Advanced Settings, and Toolbox. The current page is titled "Basic Settings" and has three tabs: "Set-up", "DHCP", and "Password". The "Password" tab is selected. Below the tabs is a table with two columns: "Item" and "Setting".

Item	Setting
Old Password	<input type="text"/>
New Password	<input type="text"/>
Reconfirm	<input type="text"/>

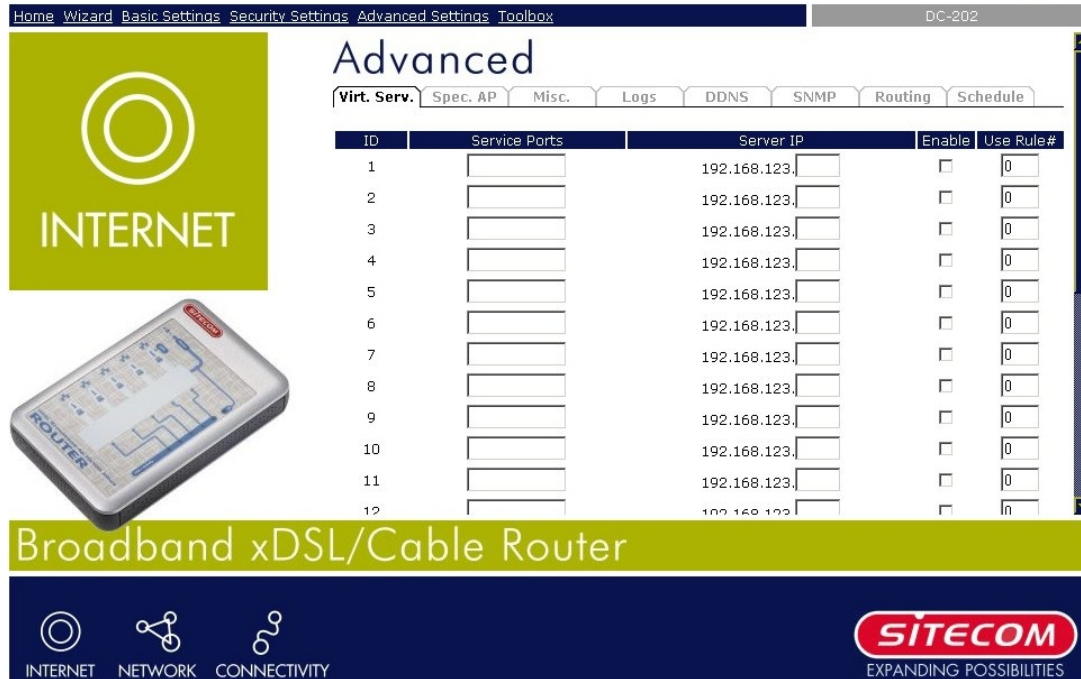
Below the table are "Save" and "Undo" buttons. On the left side of the interface, there is a green square with a white circle icon and the word "INTERNET" below it. Below that is a 3D image of a white broadband router. At the bottom of the interface, there is a green banner with the text "Broadband xDSL/Cable Router". Below the banner is a dark blue bar with three icons: "INTERNET" (a circle), "NETWORK" (a network diagram), and "CONNECTIVITY" (a network diagram). On the right side of this bar is the "SITECOM" logo with the tagline "EXPANDING POSSIBILITIES".

You can change Password here. We strongly recommend you to change the system password for security reason.



## 4.5 Advanced Settings

### 4.5.1 Virtual Server



The screenshot shows the 'Advanced' settings page for a Sitecom router. The 'Virtual Server' tab is selected, displaying a table for mapping service ports to server IPs. The table has columns for ID, Service Ports, Server IP, Enable, and Use Rule#. The 'Enable' column contains checkboxes, and the 'Use Rule#' column contains input boxes. The 'Server IP' column shows the default value 192.168.123.x for each row.

ID	Service Ports	Server IP	Enable	Use Rule#
1		192.168.123.	<input type="checkbox"/>	0
2		192.168.123.	<input type="checkbox"/>	0
3		192.168.123.	<input type="checkbox"/>	0
4		192.168.123.	<input type="checkbox"/>	0
5		192.168.123.	<input type="checkbox"/>	0
6		192.168.123.	<input type="checkbox"/>	0
7		192.168.123.	<input type="checkbox"/>	0
8		192.168.123.	<input type="checkbox"/>	0
9		192.168.123.	<input type="checkbox"/>	0
10		192.168.123.	<input type="checkbox"/>	0
11		192.168.123.	<input type="checkbox"/>	0
12		192.168.123.	<input type="checkbox"/>	0

This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

A virtual server is defined as a Service Port, and all requests to this port will be redirected to the computer specified by the Server IP. Virtual Server can work with Scheduling Rules, and give user more flexibility on Access control. For Detail, please refer to Scheduling Rule.

For example, if you have an FTP server (port 21) at 192.168.123.1, a Web server (port 80) at 192.168.123.2, and a VPN server at 192.168.123.6, then you need to specify the following virtual server mapping table:

Service Port	Server IP	Enable
21	192.168.123.1	V
80	192.168.123.2	V
1723	192.168.123.6	V

## 4.5.2 Special AP

Home Wizard Basic Settings Security Settings **Advanced Settings** Toolbox DC-202

### Advanced

Virt. Serv. **Spec. AP** Misc. Logs DDNS SNMP Routing Schedule

ID	Trigger	Incoming Ports	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Popular applications  Copy to ID

Save Undo Help

Broadband xDSL/Cable Router

INTERNET NETWORK CONNECTIVITY **SITECOM** EXPANDING POSSIBILITIES

Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. The **Special Applications** feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the **DMZ** host instead.

1. **Trigger:** the outbound port number issued by the application..
2. **Incoming Ports:** when the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.

This product provides some predefined settings. Select your application and click **Copy to** to add the predefined setting to your list.

Note! At any given time, only one PC can use each Special Application tunnel.

### 4.5.3 Miscellaneous Items

Home Wizard Basic Settings Security Settings Advanced Settings Toolbox DC-202

## Advanced

Virt. Serv. Spec. AP **Misc.** Logs DDNS SNMP Routing Schedule

Item	Setting	Enable
▶ IP Address of DMZ Host	192.168.123. <input type="text"/>	<input type="checkbox"/>
▶ Non-standard FTP port	<input type="text" value="0"/>	

Save Undo Help

**Broadband xDSL/Cable Router**

INTERNET NETWORK CONNECTIVITY **SITECOM** EXPANDING POSSIBILITIES

#### IP Address of DMZ Host

DMZ (DeMilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

**NOTE:** This feature should be used only when needed.

#### Non-standard FTP port

You have to configure this item if you want to access an FTP server whose port number is not 21. This setting will be lost after rebooting.

## 4.5.4 Logs

Home Wizard Basic Settings Security Settings Advanced Settings Toolbox DC-202

### Advanced

Virt. Serv. Spec. AP Misc. **Logs** DDNS SNMP Routing Schedule

Item	Setting	Enable
▶ IP Address for Syslogd	192.168.123.	<input type="checkbox"/>
▶ IP Address of Outgoing Mail Server		<input type="checkbox"/>
• Log or Alert Recipient		<input type="checkbox"/>

View Log... Save Undo Help

INTERNET

Broadband xDSL/Cable Router

INTERNET NETWORK CONNECTIVITY

**SITECOM**  
EXPANDING POSSIBILITIES

This page support two methods to export system logs to specific destination by means of syslog(UDP) and SMTP(TCP). The items you have to setup including:

### IP Address for Syslogd

Host IP of destination where syslogs will be sent to.

Check Enable to enable this function.

### IP address for Outgoing Mail Server

Input the SMTP server IP and port, which are concated with ':'. If you do not specify port number, the default value is 25.

For example, "mail.your\_url.com" or "192.168.1.100:26".

### Log or Alert recipient

The recipients who will receive these logs. You can assign more than 1 recipient, using ';' or ',' to separate these email addresses.

## 4.5.5 Dynamic DNS

The screenshot shows the 'Advanced' settings page for a Sitecom DC-202 router. The 'DDNS' tab is selected, and the 'Enable' radio button is checked. The 'Provider' dropdown menu is set to 'DynDNS.org(Dynamic)'. There are input fields for 'Host Name', 'Username / E-mail', and 'Password / Key'. The 'Save', 'Undo', and 'Help' buttons are visible at the bottom of the configuration area. The page header includes navigation links: Home, Wizard, Basic Settings, Security Settings, Advanced Settings, and Toolbox. The router model 'DC-202' is shown in the top right corner. A green banner at the bottom of the page reads 'Broadband xDSL/Cable Router' and features the Sitecom logo with the tagline 'EXPANDING POSSIBILITIES'.

To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).

So that anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

Before you enable **Dynamic DNS**, you need to register an account on one of these Dynamic DNS servers that we list in **provider** field.

To enable **Dynamic DNS** click the check box next to **Enable** in the **DDNS** field.

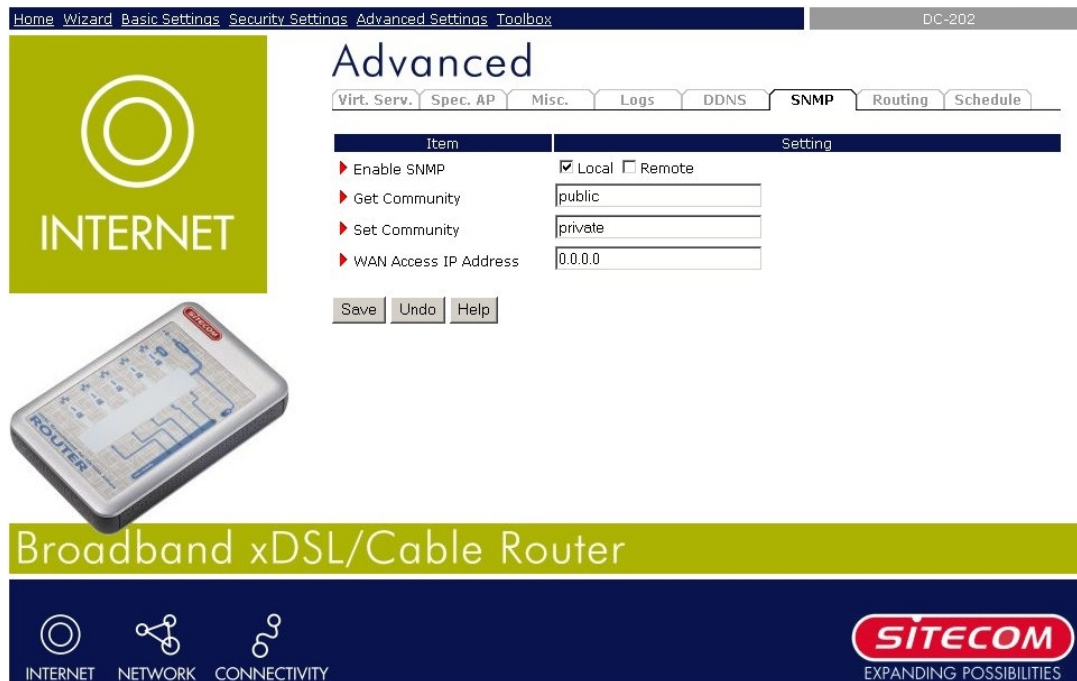
Next you can enter the appropriate information about your Dynamic DNS Server.

You have to define:

- Provider
- Host Name
- Username/E-mail
- Password/Key

You will get this information when you register an account on a Dynamic DNS server.

## 4.5.6 SNMP Setting



The screenshot shows the 'Advanced' settings page for a Sitecom DC-202 router. The 'SNMP' tab is selected, and the configuration table is as follows:

Item	Setting
▶ Enable SNMP	<input checked="" type="checkbox"/> Local <input type="checkbox"/> Remote
▶ Get Community	public
▶ Set Community	private
▶ WAN Access IP Address	0.0.0.0

Buttons for 'Save', 'Undo', and 'Help' are visible below the table. The page also features a navigation bar with 'Home', 'Wizard', 'Basic Settings', 'Security Settings', 'Advanced Settings', and 'Toolbox'. A green 'INTERNET' icon and a 'Broadband xDSL/Cable Router' banner are also present.

In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

### Enable SNMP

You must check either Local or Remote or both to enable SNMP function. If Local is checked, this device will response request from LAN. If Remote is checked, this device will response request from WAN.

### Get Community

Setting the community of GetRequest your device will response.

### Set Community

Setting the community of SetRequest your device will accept.

## 4.5.7 Routing Table

Home Wizard Basic Settings Security Settings Advanced Settings Toolbox DC-202

### Advanced

Virt. Serv. Spec. AP Misc. Logs DDNS SNMP **Routing** Schedule

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Save Undo Help

**Broadband xDSL/Cable Router**

INTERNET NETWORK CONNECTIVITY **SITECOM** EXPANDING POSSIBILITIES

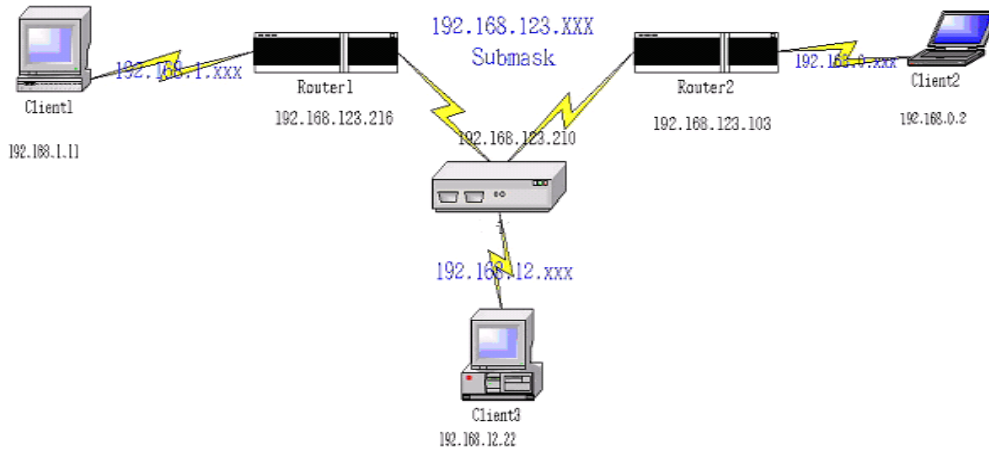
Routing Tables allow you to determine which physical interface address to use for outgoing IP data grams. If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.

Routing Table settings are settings used to setup the functions of static.

Static Routing: For static routing, you can specify up to 8 routing rules. You can enter the destination IP address, subnet mask, gateway, hop for each routing rule, and then enable or disable the rule by checking or unchecking the Enable checkbox.



Example:



### Configuration on NAT Router

Destination	SubnetMask	Gateway	Hop	Enabled
192.168.1.0	255.255.255.0	192.168.123.216	1	V
192.168.0.0	255.255.255.0	192.168.123.103	1	V

So if, for example, the client3 wanted to send an IP data gram to 192.168.0.2, it would use the above table to determine that it had to go via 192.168.123.103 (a gateway),

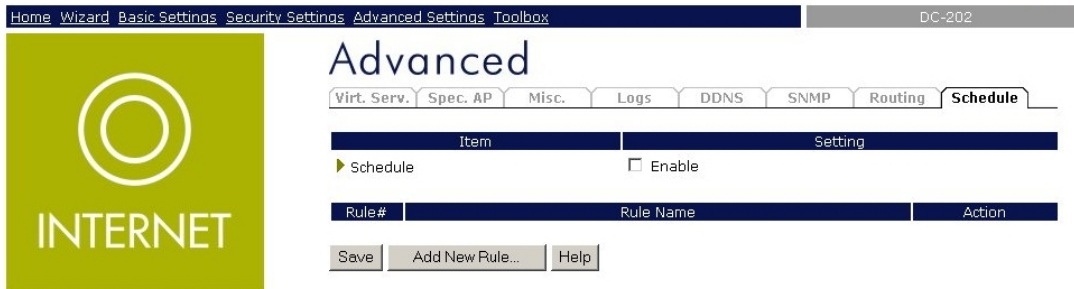
And if it sends Packets to 192.168.1.11 will go via 192.168.123.216

Each rule can be enabled or disabled individually.

After routing table setting is configured, click the save button.



## 4.5.8 Schedule



Home Wizard Basic Settings Security Settings Advanced Settings Toolbox DC-202


### Advanced

Virt. Serv. Spec. AP Misc. Logs DDNS SNMP Routing **Schedule**

Item	Setting
Schedule	<input type="checkbox"/> Enable

Rule#	Rule Name	Action

Save Add New Rule... Help



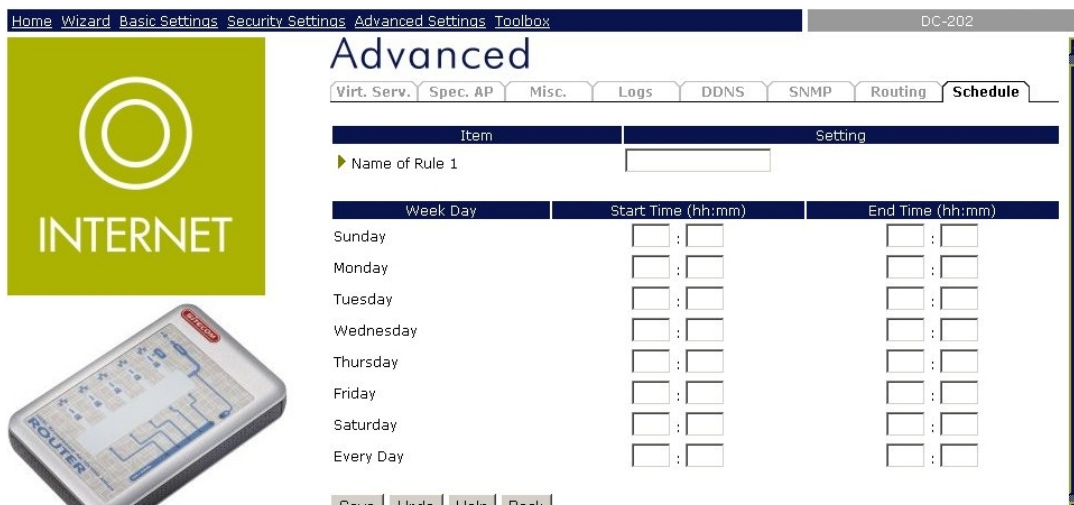
**Broadband xDSL/Cable Router**

INTERNET NETWORK CONNECTIVITY **SITECOM** EXPANDING POSSIBILITIES

You can set the schedule time to decide which service will be turned on or off. Select the “enable” item.

Press **“Add New Rule”**

You can write a rule name and set which day and what time to schedule from “Start Time” to “End Time”.



Home Wizard Basic Settings Security Settings Advanced Settings Toolbox DC-202


### Advanced

Virt. Serv. Spec. AP Misc. Logs DDNS SNMP Routing **Schedule**

Item	Setting
Name of Rule 1	<input type="text"/>

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Sunday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Monday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Tuesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Wednesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Thursday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Friday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Saturday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Every Day	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>

Save Undo Help Back



**Broadband xDSL/Cable Router**

INTERNET NETWORK CONNECTIVITY **SITECOM** EXPANDING POSSIBILITIES

## 4.6 Security Settings

### 4.6.1 Packet Filter

Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, Inbound filter applies on packets that destined to Virtual Servers or DMZ host only. You can select one of the two filtering policies:

- Allow all to pass except those match the specified rules
- Deny all to pass except those match the specified rules

You can specify 8 rules for each direction: inbound or outbound. For each rule, you can define the following:

- Source IP address
- Source port address
- Destination IP address
- Destination port address
- Protocol: TCP or UDP or both.
- Use Rule#

For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.

For source or destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example, T80, U53, U2000-2999. No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. Packet Filter can work with Scheduling Rules, and give user more flexibility on Access control. For Detail, please refer to Scheduling Rule.

Each rule can be enabled or disabled individually.

#### 4.6.1.1 Inbound Filter:

To enable **Inbound Packet Filter** click the check box next to **Enable** in the **Inbound Packet Filter** field.

Suppose you have SMTP Server (25), POP Server (110), Web Server (80), FTP Server (21), and News Server (119) defined in Virtual Server or DMZ Host.

#### Example 1:

Item	Setting
------	---------

▶ Onbound Filter  Enable

Allow all to pass except those match the following rules.

Deny all to pass except those match the following rules.

ID	Source IP : Ports	Destination IP : Ports	Enable	Use Rule#
1	1.2.3.100-1.2.3.149 : <input type="text"/>	<input type="text"/> : 25-100	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
2	1.2.3.10-1.2.3.20 : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>

Schedule rule

- (1.2.3.100-1.2.3.149) They are allow to send mail (port 25), receive mail (port 110), and browse the Internet (port 80)
- (1.2.3.10-1.2.3.20) They can do everything (block nothing)
- Others are all blocked.

**Example 2:**

Item	Setting			
▶ Onbound Filter	<input checked="" type="checkbox"/> Enable			
	<input type="radio"/> Allow all to pass except those match the following rules. <input checked="" type="radio"/> Deny all to pass except those match the following rules.			
ID	Source IP : Ports	Destination IP : Ports	Enable	Use Rule#
1	1.2.3.100-1.2.3.119 : <input type="text"/>	<input type="text"/> : 21	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
2	1.2.3.100-1.2.3.119 : <input type="text"/>	<input type="text"/> : 119	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>

Schedule rule

- (1.2.3.100-1.2.3.119) They can do everything except read net news (port 119) and transfer files via FTP (port 21)
- Others are all allowed.

After Inbound Packet Filter setting is configured, click the save button.

#### 4.6.1.2 Outbound Filter

To enable **Outbound Packet Filter** click the check box next to **Enable** in the **Outbound Packet Filter** field.

**Example 1:**

Item	Setting
------	---------

▶ Onbound Filter  Enable

Allow all to pass except those match the following rules.

Deny all to pass except those match the following rules.

ID	Source IP : Ports	Destination IP : Ports	Enable	Use Rule#
1	192.168.123.149 : <input type="text"/>	<input type="text"/> : 25-110	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
2	192.168.123.20 : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>

Schedule rule   ID

- (192.168.123.100-192.168.123.149) They are allowed to send mail (port 25), receive mail (port 110), and browse Internet (port 80); port 53 (DNS) is necessary to resolve the domain name.
- (192.168.123.10-192.168.123.20) They can do everything (block nothing)
- Others are all blocked.

**Example 2:**

Item	Setting
▶ Onbound Filter	<input checked="" type="checkbox"/> Enable
	<input checked="" type="radio"/> Allow all to pass except those match the following rules. <input type="radio"/> Deny all to pass except those match the following rules.

ID	Source IP : Ports	Destination IP : Ports	Enable	Use Rule#
1	192.168.123.100 : <input type="text"/>	<input type="text"/> : 25	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
2	192.168.123.119 : <input type="text"/>	<input type="text"/> : 119	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>

Schedule rule   ID

- (192.168.123.100-192.168.123.119) They can do everything except read net news (port 119) and transfer files via FTP (port 21)
- Others are allowed

After Outbound Packet Filter setting is configured, click the save button.

## 4.6.2 Domain Filter

# Security

Packet
  **Domain**
 URL
  MAC
  MISC.

Item	Setting
▶ Domain Filter	<input checked="" type="checkbox"/> Enable
▶ Log DNS Query	<input checked="" type="checkbox"/> Enable
▶ Privilege IP Addresses Range	From <input type="text" value="1"/> To <input type="text" value="20"/>

ID	Domain Suffix	Action	Enable
1	<input type="text" value="www.msn.com"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>

### Domain Filter

Let you prevent users under this device from accessing specific URLs.

### Domain Filter Enable

Check if you want to enable Domain Filter.

### Log DNS Query

Check if you want to log the action when someone accesses the specific URLs.

### Privilege IP Addresses Range

Setting a group of hosts and privilege these hosts to access network without restriction.

### Domain Suffix

A suffix of URL to be restricted. For example, ".com", "xxx.com".

### Action

When someone is accessing the URL met the domain-suffix, what kind of action you want. Check drop to block the access. Check log to log these access.

### Enable

Check to enable each rule.

Example:

# Security

Packet **Domain** URL MAC MISC.

Item	Setting
▶ Domain Filter	<input checked="" type="checkbox"/> Enable
▶ Log DNS Query	<input checked="" type="checkbox"/> Enable
▶ Privilege IP Addresses Range	From <input type="text" value="1"/> To <input type="text" value="20"/>

ID	Domain Suffix	Action	Enable
1	<input type="text" value="www.msn.com"/>	<input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
2	<input type="text" value="www.sina.com"/>	<input type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
3	<input type="text" value="www.google.com"/>	<input checked="" type="checkbox"/> Drop <input type="checkbox"/> Log	<input checked="" type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>

In this example:

- URL include "www.msn.com" will be blocked, and the action will be record in log-file.
- URL include "www.sina.com" will not be blocked, but the action will be record in log-file.
- URL include "www.google.com" will be blocked, but the action will not be record in log-file.
- IP address X.X.X.1 ~ X.X.X.20 can access network without restriction.



### 4.6.3 URL Blocking

Item		Setting
▶ URL Blocking		<input type="checkbox"/> Enable

ID	URL	Enable
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="checkbox"/>

URL Blocking will block LAN computers to connect to pre-defined Websites.

The major difference between "Domain filter" and "URL Blocking" is Domain filter require user to input suffix (like .com or .org, etc), while URL Blocking require user to input a keyword only. In other words, Domain filter can block specific website, while URL Blocking can block hundreds of websites by simply a keyword.

#### URL Blocking Enable

Checked if you want to enable URL Blocking.

#### URL

If any part of the Website's URL matches the pre-defined word, the connection will be blocked.

For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".

#### Enable

Checked to enable each rule.

Item		Setting
▶ URL Blocking		<input checked="" type="checkbox"/> Enable

ID	URL	Enable
1	<input type="text" value="msn"/>	<input checked="" type="checkbox"/>
2	<input type="text" value="sina"/>	<input checked="" type="checkbox"/>
3	<input type="text" value="cnnsi"/>	<input checked="" type="checkbox"/>
4	<input type="text" value="espn"/>	<input checked="" type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="checkbox"/>

In this example:

- URL include "msn" will be blocked, and the action will be record in log-file.
- URL include "sina" will be blocked, but the action will be record in log-file
- URL include "cnnsi" will not be blocked, but the action will be record in log-file.
- URL include "espn" will be blocked, but the action will be record in log-file

## 4.6.4 MAC Address Control

Home Wizard Basic Settings Security Settings Advanced Settings Toolbox DC-202

### Security

Packet Domain URL **MAC** MISC.

Item Setting

MAC Address Control  Enable

Connection control Clients with C checked can connect to this device; and allow unspecified MAC addresses to connect.

ID	MAC Address	IP Address	C
1	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>

DHCP clients - select one - Copy to ID -

Previous page Next page Save Undo Help

Broadband xDSL/Cable Router

INTERNET NETWORK CONNECTIVITY **SITECOM** EXPANDING POSSIBILITIES

MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.

**MAC Address Control** Check "Enable" to enable the "MAC Address Control". All of the settings in this page will take effect only when "Enable" is checked.

**Connection control** Check "Connection control" to enable the controlling of which wired and clients can connect to this device. If a client is denied to connect to this device, it means the client can't access to the Internet either. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect to this device.

### Control table

ID	MAC Address	IP Address	C
1	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>

DHCP clients - select one - Copy to ID -

"Control table" is the table at the bottom of the "MAC Address Control" page. Each row of this table indicates the MAC address and the expected IP address mapping of a client. There are four columns in this table:

<b>MAC Address</b>	MAC address indicates a specific client.
<b>IP Address</b>	Expected IP address of the corresponding client. Keep it empty if you don't care its IP address.
<b>C</b>	When " <b>Connection control</b> " is checked, check " <b>C</b> " will allow the corresponding client to connect to this device.

In this page, we provide the following Combobox and button to help you to input the MAC address.



The image shows a user interface element consisting of a label 'DHCP clients' followed by a text input field containing '- select one -' and a downward-pointing arrow. To the right of this field is a button labeled 'Copy to'. Further right is another text input field containing 'ID' and a downward-pointing arrow.

You can select a specific client in the "DHCP clients" Combobox, and then click on the "Copy to" button to copy the MAC address of the client you select to the ID selected in the "ID" Combobox.

**Previous page and Next Page** To make this setup page simple and clear, we have divided the "Control table" into several pages. You can use these buttons to navigate to different pages.

## 4.6.5 Miscellaneous Items

Home Wizard Basic Settings Security Settings Advanced Settings Toolbox DC-202

### Security

Packet Domain URL MAC MISC.

Item	Setting	Enable
▶ Remote Administrator Host / Port	0.0.0.0 / 88	<input type="checkbox"/>
▶ Administrator Time-out	600 seconds (0 to disable)	
▶ Discard PING from WAN side		<input type="checkbox"/>

Save Undo Help

INTERNET

ROUTER

Broadband xDSL/Cable Router

INTERNET NETWORK CONNECTIVITY

**SITECOM**  
EXPANDING POSSIBILITIES

### Remote Administrator Host/Port

In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect to this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses. For example, "10.1.2.0/24".

**NOTE:** When Remote Administration is enabled, the web server port will be shifted to 88. You can change web server port to other port, too.

### Administrator Time-out

The time of no activity to logout automatically. Set it to zero to disable this feature.

### Discard PING from WAN side

When this feature is enabled, any host on the WAN cannot ping this product.

## 4.7 Toolbox

### 4.7.1 System Log

The screenshot shows the 'Toolbox' page for the Sitecom DC-202. The navigation bar includes 'Home', 'Wizard', 'Basic Settings', 'Security Settings', 'Advanced Settings', and 'Toolbox'. The 'Toolbox' section has tabs for 'View log', 'Firmware', 'Misc.', 'Time', 'Backup', 'Reset', and 'Reboot'. The 'View log' tab is active, displaying 'WAN Type: Dynamic IP Address (R1.97a3)' and 'Display time: Thu Jul 01 00:03:45 2004'. Below the log information are buttons for 'Back', 'Refresh', 'Download', and 'Clear logs'. On the left side, there is a green 'INTERNET' icon and an image of the Sitecom DC-202 router. At the bottom, there is a green banner for 'Broadband xDSL/Cable Router' and a dark blue footer with 'INTERNET', 'NETWORK', 'CONNECTIVITY' icons, the 'SITECOM' logo, and the tagline 'EXPANDING POSSIBILITIES'.

You can View system log by clicking the View Log button

### 4.7.2 Firmware Upgrade

The screenshot shows the 'Toolbox' page for the Sitecom DC-202, specifically the 'Firmware' tab. The navigation bar is the same as in the previous screenshot. The 'Firmware' tab is active, showing a 'Firmware Filename' field with a 'Browse...' button. Below the field, a note states: 'Current firmware version is R1.97a3. The upgrade procedure takes about 20 seconds. Note! Do not power off the unit when it is being upgraded. When the upgrade is done successfully, the unit will be restarted automatically.' At the bottom of the section are 'Upgrade' and 'Cancel' buttons. The left side and footer are identical to the previous screenshot.

You can upgrade firmware by clicking **Firmware Upgrade** button.

### 4.7.3 Miscellaneous Items

Home Wizard Basic Settings Security Settings Advanced Settings Toolbox DC-202

## Toolbox

View log Firmware **Misc.** Time Backup Reset Reboot

Item	Setting
▶ MAC Address for Wake-on-LAN	<input type="text"/> Wake up

Save Undo Help

**INTERNET**

**Broadband xDSL/Cable Router**

INTERNET NETWORK CONNECTIVITY **SITECOM** EXPANDING POSSIBILITIES

#### MAC Address for Wake-on-LAN

Wake-on-LAN is a technology that enables you to power up a networked device remotely. In order to enjoy this feature, the target device must be Wake-on-LAN enabled and you have to know the MAC address of this device, say 00-11-22-33-44-55. Clicking "Wake up" button will make the router to send the wake-up frame to the target device immediately.

## 4.7.4 System Time

Home Wizard Basic Settings Security Settings Advanced Settings Toolbox DC-202

### Toolbox

View log Firmware Misc. **Time** Backup Reset Reboot

Item	Setting
<input type="radio"/> Get Date and Time by NTP Protocol	<input type="button" value="Sync Now!"/>
Time Server	time.nist.gov
Time Zone	(GMT-08:00) Pacific Time (US & Canada)
<input type="radio"/> Set Date and Time using PC's Date and Time	
PC Date and Time:	dinsdag 27 juli 2004 11:37:19
<input checked="" type="radio"/> Set Date and Time manually	
Date	Year: 2004 Month: Jul Day: 1
Time	Hour: 0 (0-23) Minute: 0 (0-59) Second: 0 (0-59)

**Broadband xDSL/Cable Router**

INTERNET NETWORK CONNECTIVITY **SITECOM** EXPANDING POSSIBILITIES

### Get Date and Time by NTP Protocol

Selected if you want to Get Date and Time by NTP Protocol.

### Time Server

Select a NTP time server to consult UTC time

### Time Zone

Select a time zone where this device locates.

### Set Date and Time manually

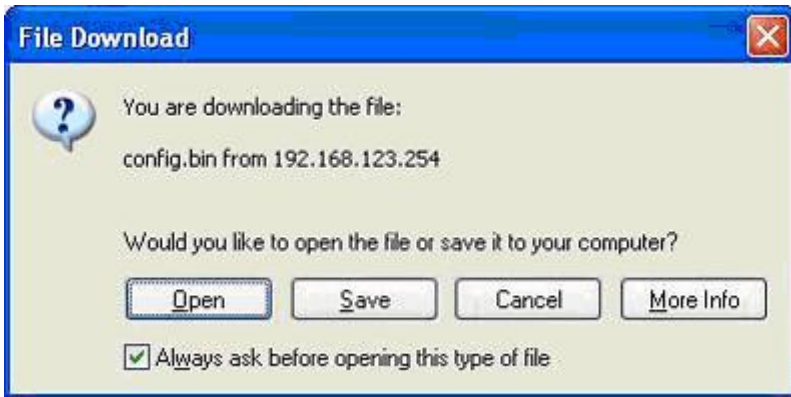
Selected if you want to Set Date and Time manually.

### Function of Buttons

**Sync Now:** Synchronize system time with network time server



### 4.7.5 Backup Setting



You can backup your settings by clicking the Backup Setting button and save it as a bin file. Once you want to restore these settings, please click Firmware Upgrade button and use the bin file you saved.

### 4.7.6 Reset to default



You can also reset this product to factory default by clicking the **Reset to default** button.

### 4.7.7 Reboot



You can also reboot this product by clicking the **Reboot** button.

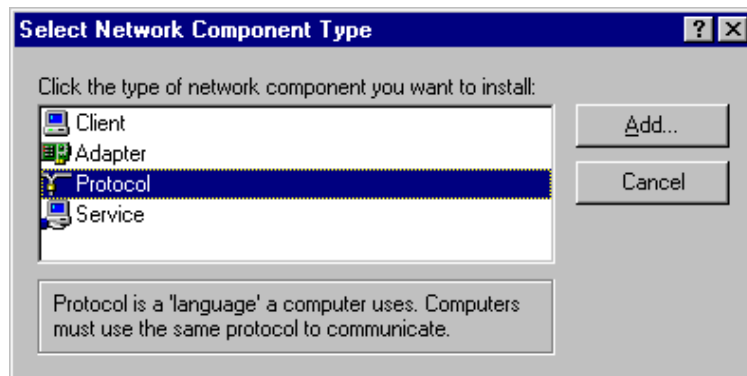
## Appendix A TCP/IP Configuration for Windows

95/98

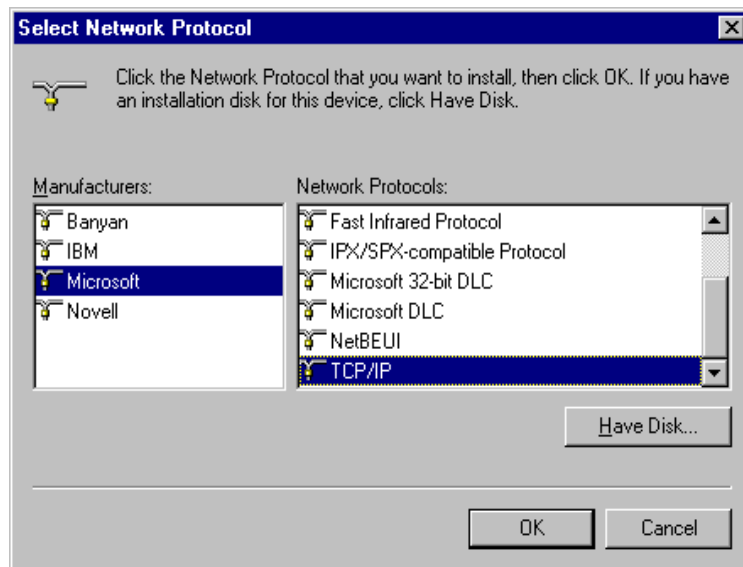
This section introduces you how to install TCP/IP protocol into your personal computer. And suppose you have been successfully installed one network card on your personal computer. If not, please refer to your network card manual. Moreover, the Section B.2 tells you how to set TCP/IP values for working with this NAT Router correctly.

### A.1 Install TCP/IP Protocol into Your PC

1. Click **Start** button and choose **Settings**, then click **Control Panel**.
2. Double click **Network** icon and select **Configuration** tab in the Network window.
3. Click **Add** button to add network component into your PC.
4. Double click **Protocol** to add TCP/IP protocol.



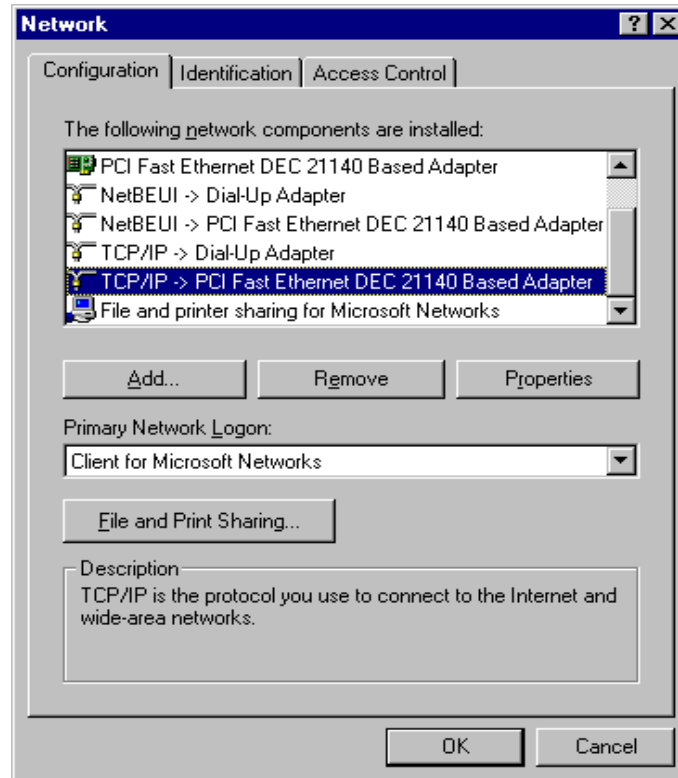
5. Select **Microsoft** item in the manufactures list. And choose **TCP/IP** in the Network Protocols. Click **OK** button to return to Network window.



6. The TCP/IP protocol shall be listed in the Network window. Click **OK** to complete the install procedure and restart your PC to enable the TCP/IP protocol.

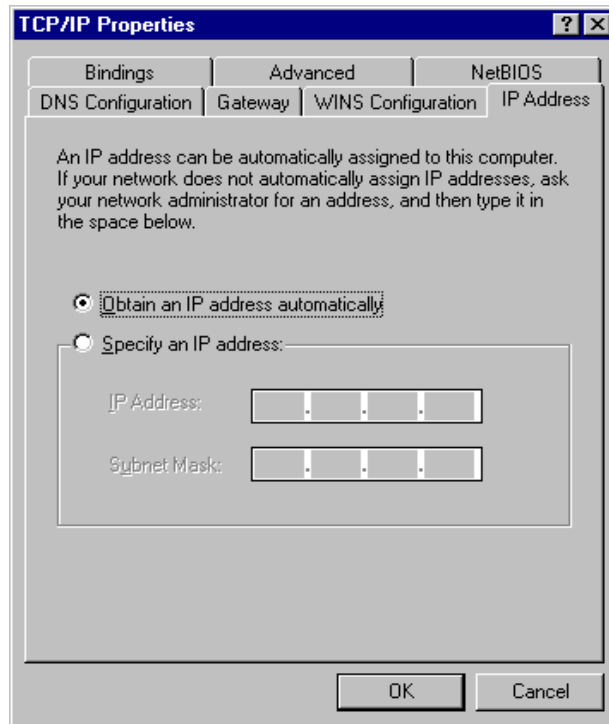
## A.2 Set TCP/IP Protocol for Working with NAT Router

1. Click **Start** button and choose **Settings**, then click **Control Panel**.
2. Double click **Network** icon. Select the TCP/IP line that has been associated to your network card in the **Configuration** tab of the Network window.

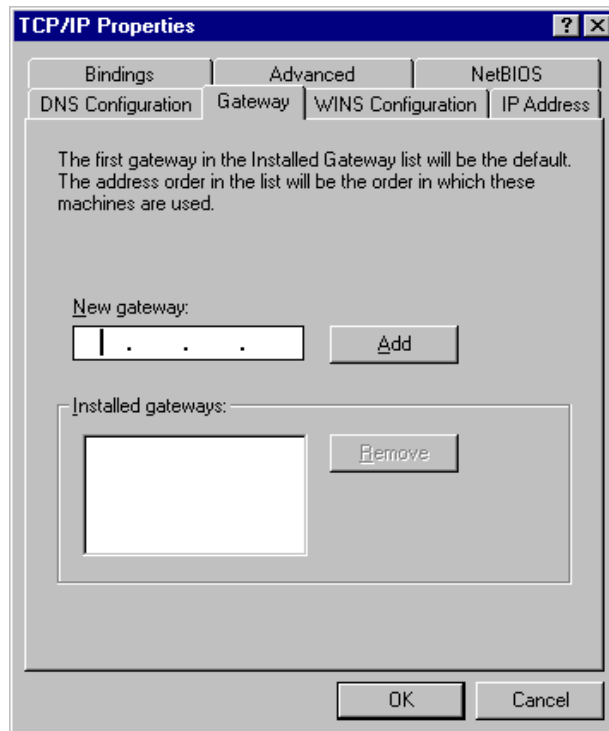


3. Click **Properties** button to set the TCP/IP protocol for this NAT Router.
4. Now, you have two setting methods:

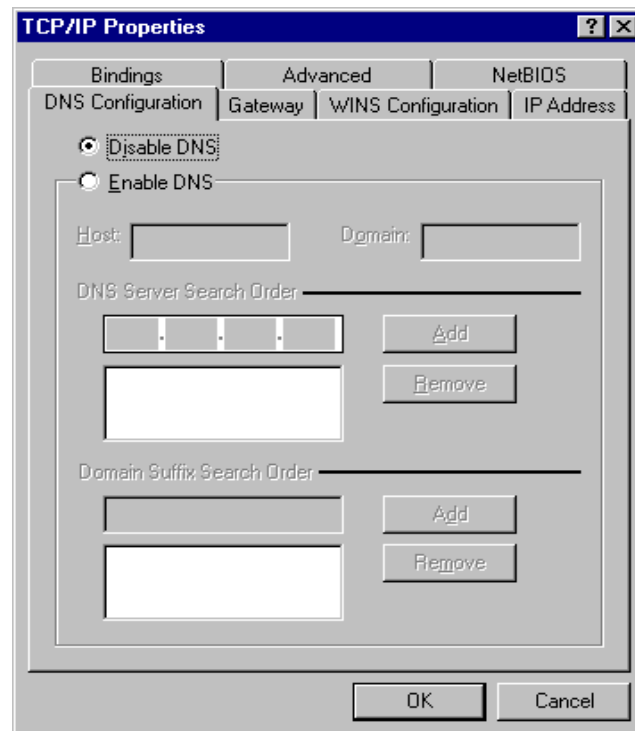
- a. Select **Obtain an IP address automatically** in the IP Address tab.



- b. Don't input any value in the Gateway tab.

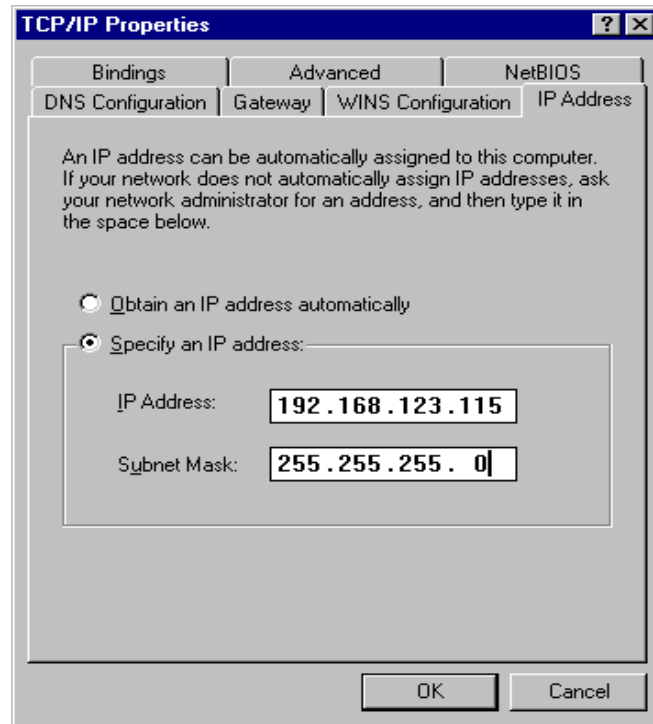


- c. Choose **Disable DNS** in the DNS Configuration tab.

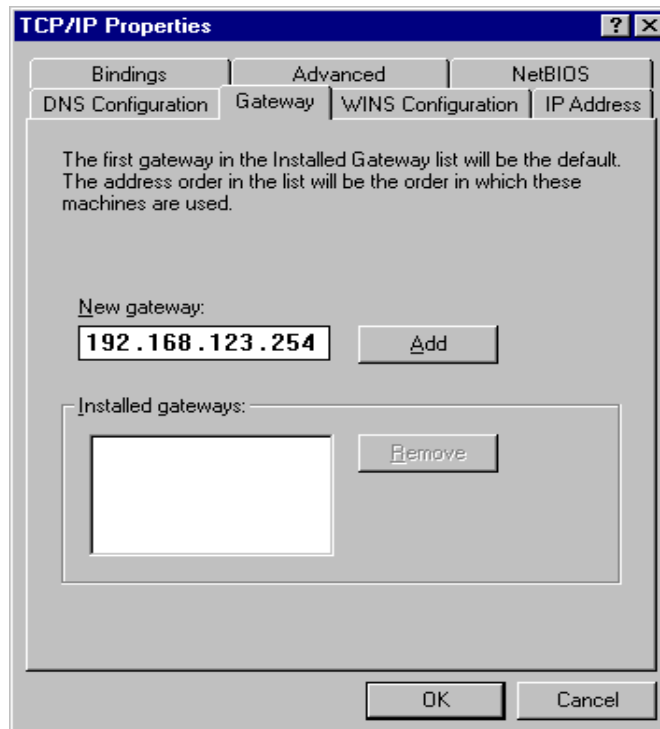


B. Configure IP manually

- a. Select **Specify an IP address** in the IP Address tab. The default IP address of this product is 192.168.123.254. So please use 192.168.123.xxx (xxx is between 1 and 253) for IP Address field and 255.255.255.0 for Subnet Mask field.

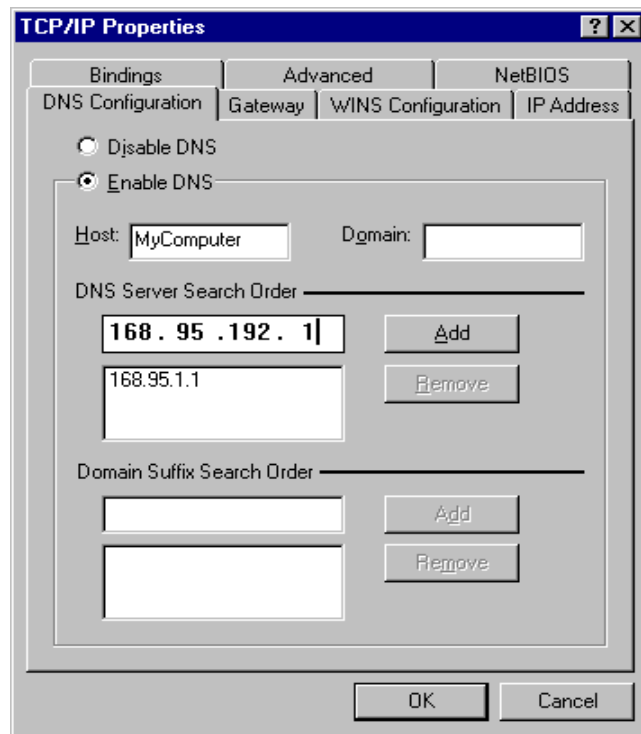


- b. In the Gateway tab, add the IP address of this product (default IP is 192.168.123.254) in the New gateway field and click **Add** button.



- c. In the DNS Configuration tab, add the DNS values which are provided by the

ISP into DNS Server Search Order field and click **Add** button.





## ***Appendix B FAQ and Troubleshooting***

### Reset to factory Default

There are 2 methods to reset to default.

#### **Restore with RESET button**

First, turn off the router and press the RESET button in. And then, power on the router and push the RESET button down until the M1 and or M2 LED (or Status LED) start flashing, then remove the finger. If LED flashes about 8 times, the RESTORE process is completed. However, if LED flashes 2 times, repeat.

#### **Restore directly when the router power on**

First, push the RESET button about 5 seconds (M1 will start flashing about 5 times), then release the button.