



Broadband Router
DC-202

Full Manual

Table of Contents

REQUIREMENTS	4
INTRODUCTION	4
DC-202 Features	4
Internet Access Features.....	4
Advanced Internet Functions	5
LAN Features.....	5
Configuration & Management.....	5
Security Features.....	6
SETTING UP THE BROADBAND ROUTER	7
Physical installation	7
Top LEDs	9
Rear Panel	10
PC SETUP	11
Set up TCP/IP	11
Using DHCP.....	11
Windows 98/ME.....	11
Windows 2000/XP	11
Windows NT	13
Macintosh Clients.....	14
Linux Clients	14
Internet access	15
Windows 98/ME/2000.....	15
Windows XP	15
Accessing AOL	15
Manual configuration – Internet access	16
Your country/ISP is not listed	19
Cable Internet	19
xDSL Internet.....	24
Home Screen	30
LAN Screen	31
DHCP	32
Password Screen	33
OPERATION AND STATUS	34
Operation	34
Status Screen	34
Connection Status - PPPoE	36
Connection Status - PPTP	37
Connection Status - L2TP	38
Connection Details - Fixed/Dynamic IP Address	40
ADVANCED FEATURES	41
Overview	41
Advanced Internet Screen	42
Communication Applications	42
Special Applications.....	43
Special Applications Screen	43
Using a Special Application.....	44
Multi-DMZ.....	44

URL Filter.....	45
URL Filter Screen	45
Access Control	47
Overview	47
Access Control Screen	47
Group Members Screen.....	49
Default Schedule Screen	50
Services Screen	51
Access Control Log	52
Remote Management	53
Virtual Servers	54
IP Address seen by Internet Users.....	54
Virtual Servers Screen	54
Defining your own Virtual Servers	56
Connecting to the Virtual Servers	57
Dynamic DNS (Domain Name Server)	58
Dynamic DNS Screen	58
Upgrade Firmware	60
Config File.....	61
PC Database.....	62
PC Database Screen	62
PC Database (Admin)	63
Network Diagnostics.....	66
Options	67
Security	69
Logs.....	71
MAC Address.....	73
MAC Address Screen	73
Routing.....	74
Overview	74
Routing Screen.....	74
Configuring Other Routers on your LAN.....	76
Static Routing - Example.....	77
APPENDIX A TROUBLESHOOTING.....	78
Overview	78
General Problems	78
Internet Access.....	79
APPENDIX B SPECIFICATIONS	80
Multi-Function DC-202 Broadband Router	80
FCC Statement	80
FCC Radiation Exposure Statement.....	81
CE Marking Warning.....	81

Requirements

- Cable modem or DSL/ADSL modem.
- Standard 10/100BaseT (UTP) network cables with RJ45 connectors.
- PCs that make use of the TCP/IP network protocol.

Introduction

Congratulations on the purchase of your new DC-202 Broadband Router. The DC-202 is a multi-function device providing the following services:

- **Shared Broadband Internet Access** for all LAN users.
- **4-Port Switching Hub** for 10BaseT or 100BaseT connections.

DC-202 Features

The DC-202 incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

Internet Access Features

- **Shared Internet Access.** All users on the LAN or WLAN can access the Internet through the DC-202, 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).
- **DSL & Cable Modem Support.** The DC-202 has a 10/100BaseT Ethernet port for connecting a DSL or Cable Modem. All popular DSL and Cable Modems are supported. SingTel RAS and Big Pond (Australia) login support is also included.
- **Supports all Connection Methods.** The Internet (WAN port) connection supports PPPoE (PPP over Ethernet), PPTP (Peer-to-Peer Tunneling Protocol), L2TP (Level 2 Tunneling Protocol), SingTel RAS and Telstra Big Pond (Australia), as well as "Direct Connection" type services.
- **Fixed or Dynamic IP Address.** On the Internet (WAN port) connection, the DC-202 supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

Advanced Internet Functions

- **Communication Applications.** Support for Internet communication applications, such as interactive Games, Telephony, and Conferencing applications, which are often difficult to use when behind a Firewall, is included.
- **Special Internet Applications.** Applications which use non-standard connections or port numbers are normally blocked by the Firewall. The ability to define and allow such applications is provided, to enable such applications to be used normally.
- **Virtual Servers.** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- **DMZ.** One (1) PC on your local LAN can be configured to allow unrestricted 2-way communication with Servers or individual users on the Internet. This provides the ability to run programs which are incompatible with Firewalls.
- **URL Filter.** Use the URL Filter to block access to undesirable Web sites by LAN users.
- **Internet Access Log.** See which Internet connections have been made.
- **Access Control.** Using the Access Control feature, you can assign LAN users to different groups, and determine which Internet services are available to each group.
- **VPN Pass through Support.** PCs with VPN (Virtual Private Networking) software using PPTP, L2TP and IPSec are transparently supported - no configuration is required.

LAN Features

- **4-Port Switching Hub.** The DC-202 incorporates a 4-port 10/100BaseT switching hub, making it easy to create or extend your LAN.
- **DHCP Server Support.** Dynamic Host Configuration Protocol provides a dynamic IP address to PCs and other devices upon request. The DC-202 can act as a **DHCP Server** for devices on your local LAN and WLAN.
- **Multi Segment LAN Support.** LANs containing one or more segments are supported, via the DC-202's RIP (Routing Information Protocol) support and built-in static routing table.

Configuration & Management

- **Easy Setup.** Use your WEB browser from anywhere on the LAN for configuration.
- **Configuration File Upload/Download.** Save (download) the configuration data from the DC-202 to your PC, and restore (upload) a previously-saved configuration file to the DC-202.
- **Remote Management.** The DC-202 can be managed from any PC on your LAN. And, if the Internet connection exists, it can also (optionally) be configured via the Internet.

- **UPnP Support.** UPnP (Universal Plug and Play) allows automatic discovery and configuration of the DC-202. UPnP is supported by Windows ME, XP, or later.

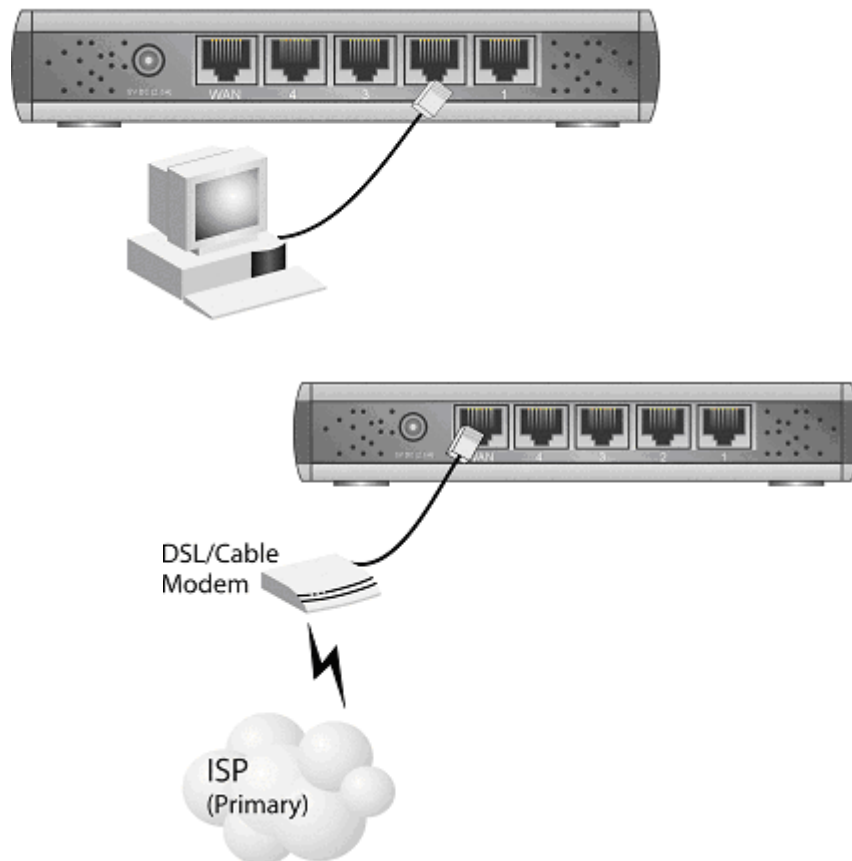
Security Features

- **Password - protected Configuration.** Optional password protection is provided to prevent unauthorized users from modifying the configuration data and settings.
- **NAT Protection.** An intrinsic side effect of NAT (Network Address Translation) technology is that by allowing all LAN users to share a single IP address, the location and even the existence of each PC is hidden. From the external viewpoint, there is no network, only a single device - the DC-202.
- **Stateful Inspection Firewall.** All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources.
- **Protection against DoS attacks.** DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The DC-202 incorporates protection against DoS attacks.

Setting up the broadband router

Physical installation

1. For the installation of the Broadband router it is assumed that you have at least one PC with a working broadband Internet connection. It is also assumed that the modem is configured in accordance with the requirements of your ISP and of the modem manufacturer. If not, first consult the manual of your ISP.
2. Before you begin, check that power is not connected to either the broadband router or the cable modem/DSL modem. Leave your cable modem/DSL modem plugged in (telephone line or cable input).



Installation - DC-202

3. Connect the LAN cables: For the DC-202, use standard LAN cables to connect the PCs to the LAN ports (hub) on the broadband router. If necessary connect the "Uplink" port to a standard port on another hub. You must use a standard LAN cable for this.

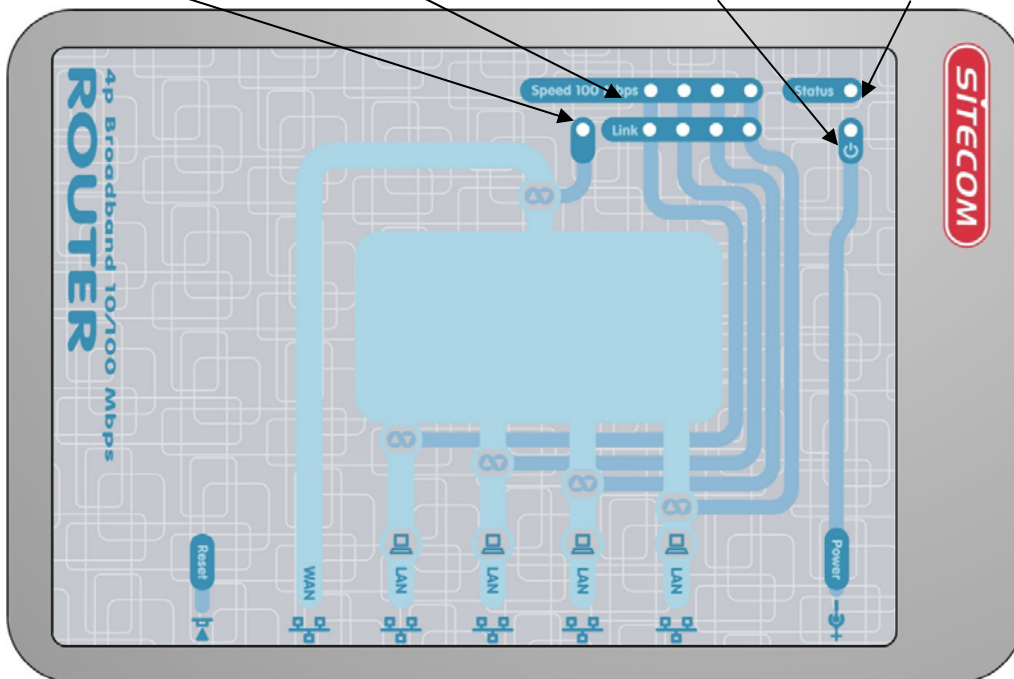
Note: If you use the "Uplink" port, then port 4 CANNOT be used.

4. Connect your cable modem/DSL modem to the WAN-port on the broadband router. Use the cable supplied with your cable modem/DSL modem. If no cable was supplied with your modem, use a standard network cable.

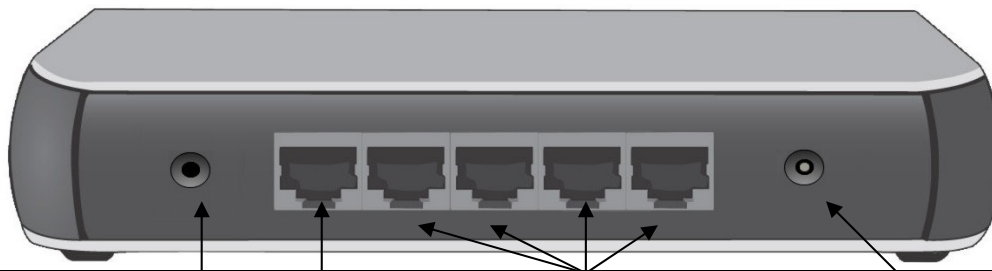
5. Switch on the cable modem/DSL modem.
6. Connect the power supply adapter to the broadband router. Use only the adapter supplied with the router.
7. Check the LEDs
 - The *Power* LED must be ON.
 - The *Status* LED must start flashing, after which it must be extinguished. If it remains on, this indicates that there is a hardware problem.
 - The *WAN* LED must be ON.
 - For each active LAN connection, the associated LAN *Link/Act* LED must be ON.

Top LEDs

WAN	LAN	Power	Status (Red)
<p>On - Connection to the modem attached to the WAN (Internet) port is established.</p> <p>Flashing - Data is being transmitted or received via the WAN port.</p>	<p>For each port, there are 2 LEDs</p> <p>Link/Act</p> <p>On - Corresponding LAN (hub) port is active.</p> <p>Off - No active connection on the corresponding LAN (hub) port.</p> <p>Flashing - Data is being transmitted or received via the corresponding LAN (hub) port.</p> <p>100</p> <p>On - Corresponding LAN (hub) port is using 100BaseT.</p> <p>Off - Corresponding LAN (hub) port connection is using 10BaseT, or no active connection.</p>	<p>On - Power on.</p> <p>Off - No Power.</p>	<p>On - Error condition.</p> <p>Off - Normal operation.</p> <p>Blinking - This LED blinks during start up.</p>



Rear Panel



Reset Button	WAN port (10/100BaseT)	10/100BaseT LAN connections	Power port
<p>This button has two (2) functions:</p> <p>Reboot. When pressed and released, the DC-202 will reboot (restart).</p> <p>Clear All Data. This button can also be used to clear ALL data and restore ALL settings to the factory default values.</p> <p>To Clear All Data and restore the factory default values:</p> <p>Power Off.</p> <p>Hold the Reset Button down while you Power On.</p> <p>Keep holding the Reset Button for a few seconds, until the RED Status LED on the front panel has flashed TWICE.</p> <p>Release the Reset Button. The DC-202 is now using the factory default values.</p>	<p>Connect the DSL or Cable Modem here. If your modem came with a cable, use the supplied cable. Otherwise, use a standard LAN cable.</p>	<p>Use standard LAN cables (RJ45 connectors) to connect your PCs to these ports.</p> <p>Note:</p> <p>Any LAN port on the DC-202 will automatically function as an "Uplink" port when required. Just connect any port to a normal port on the other hub, using a standard LAN cable.</p>	<p>Connect the supplied power adapter here.</p>

PC Setup

Set up TCP/IP

If you are using a Fixed (specified) IP address, the following changes are required:

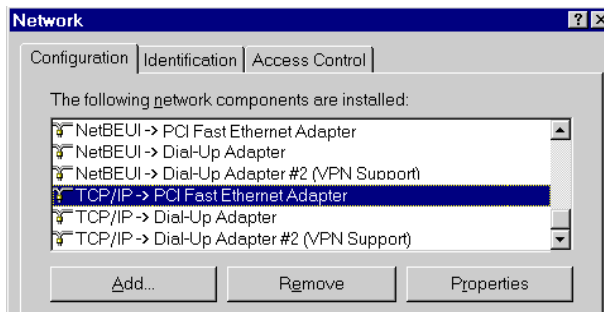
- The *Gateway* must be set to the IP address of the DC-202
- The *DNS* should be set to the address provided by your ISP.

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended.** By default, the DC-202 will act as a DHCP Server.

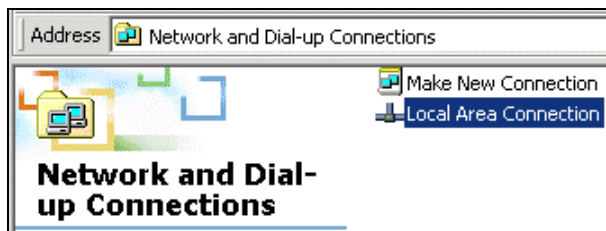
Windows 98/ME

Right click the *Network Neighbourhood* icon on the desktop and click *Properties*. The following window will be displayed:

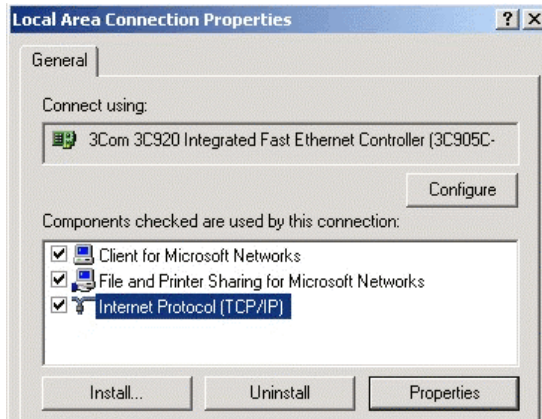


Windows 2000/XP

Right click the *My Network Places* icon on the desktop and click *Properties*. The following window will be displayed:



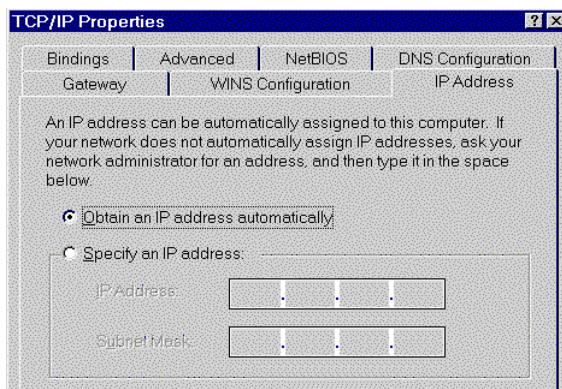
Right click the *Local Area Connection* of the correct network card, and then choose *Properties*.



If the list that appears on screen does not include a line, such as the one that has been selected above ("TCP/IP -> network card"), then follow the steps indicated below for adding this line:

- Click on the button "Add"
- Double-click on "Protocol"
- Select "Microsoft" and thereafter "TCP/IP"
- Click on "OK"
- Wait a few seconds, so that TCP/IP can be added. Thereafter, click on "OK" to leave the network properties screen. Restart your PC.

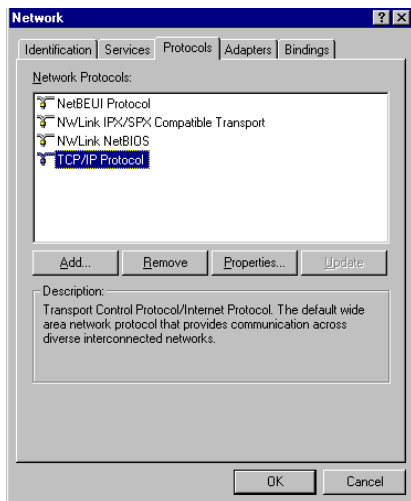
Select the line "TCP/IP -> Network card" as shown above. Click on the button *Properties* to obtain a window similar to the following:



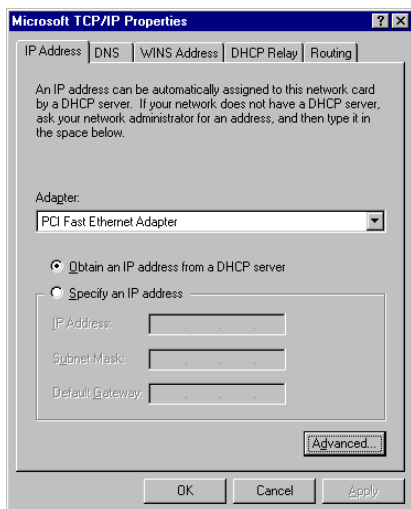
Check whether the setting "**Obtain an IP address automatically**" has been selected, as is illustrated above. The DHCP server in the broadband router will now assign an IP address to the PC.

Windows NT

Select *Control Panel - Network*, and, on the *Protocols* tab, select the TCP/IP protocol, as shown below.



Click the *Properties* button to see a screen like the one below.



Select the network card for your LAN.

Select the appropriate radio button - *Obtain an IP address from a DHCP Server*

Restart your PC, even if you have not made any changes.

Macintosh Clients

From your Macintosh, you can access the Internet via the DC-202. The procedure is as follows.

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

Note:

If using manually assigned IP addresses instead of DHCP, the required changes are:

- Set the *Router Address* field to the DC-202's IP Address.
- Ensure your DNS settings are correct.

Linux Clients

To access the Internet via the DC-202, it is only necessary to set the DC-202 as the "Gateway".

Ensure you are logged in as "root" before attempting any changes.

Fixed IP Address

By default, most Unix installations use a fixed IP Address. If you wish to continue using a fixed IP Address, make the following changes to your configuration.

- Set your "Default Gateway" to the IP Address of the DC-202.
- Ensure your DNS (Name server) settings are correct.

To act as a DHCP Client (recommended)

The procedure below may vary according to your version of Linux and X - windows shell.

1. Start your X Windows client.
2. Select *Control Panel - Network*
3. Select the "Interface" entry for your Network card. Normally, this will be called "eth0".
4. Click the *Edit* button, set the "protocol" to "DHCP", and save this data.
5. To apply your changes
 - Use the "Deactivate" and "Activate" buttons, if available.
 - OR, restart your system.

Internet access

Windows 98/ME/2000

- In the Taskbar, click on the Start button and select Settings - Control Panel - Internet options.
- Select the tab page *Connections* and click on the button *Settings*.
- Select "I want to configure my Internet connection manually" or "I want to make a connection via a LAN network" and click on "Next >".
- Select "I want to connect via a LAN network" and click on "Next >".
- Check carefully that all of the checkboxes in the screen *Internet configuration for a LAN* have **not been checked**.
- Continue with the steps in the wizard, until the task is completed.
- The configuration is now completed.

Windows XP

- In the Taskbar, click on the Start button and select - Settings – Control Panel - Internet options.
- Select the tab *Connections* and click the *Setup...* button.
- When the New Connection Wizard starts, click on *Next*.
- Select *Connect to internet* and click on *Next*.
- Select *Set up my connection manually* and click on *Next*.
- Select *Connect using a broadband connection that is always on* and click on *Next*.
- Click on *Finish* to close the Wizard.
- In the Taskbar, click on the Start button and select - Settings – Control Panel - Internet options.
- Select the *Connections* tab and click on the *LAN Settings* button.
- Check carefully that **none** of the boxes in the *Local Area Network (LAN) Settings* window are checked.
- The configuration is now completed.

Accessing AOL

To access AOL (America On Line) through the DC-202, 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 "DC-202".
- 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 "DC-202" location.

Manual configuration – Internet access

1. Make **TCP/IP** settings on your PC, as described in the foregoing section.

Do not forget to restart your PC after you have finished.

2. Using UPnP

If your Windows system supports UPnP, an icon for the DC-202 will appear in the system tray, notifying you that a new network device has been found, and offering to create a new desktop shortcut to the newly-discovered device.

- Unless you intend to change the IP Address of the DC-202, you can accept the desktop shortcut.
- Whether you accept the desktop shortcut or not, you can always find UPnP devices in *My Network Places*.

Double click the icon for the DC-202 (either on the Desktop, or in *My Network Places*) to start the configuration. Proceed with step 4.

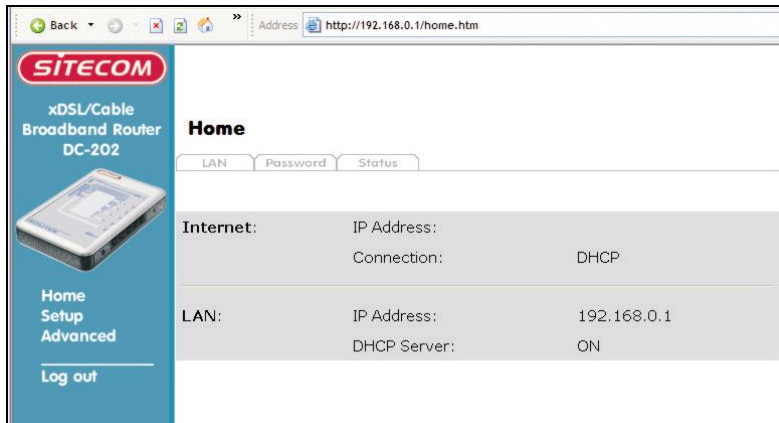
3. Start your web browser. In the *Address* field, enter the following:
192.168.0.1

If you can't connect

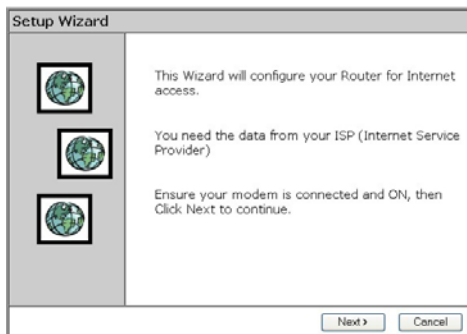
If the DC-202 does not respond, check the following:

- The DC-202 is properly installed, LAN connection is OK, and it is powered ON. You can test the connection by using the "Ping" command:
- Open the MS-DOS window or command prompt window.
- Enter the command:
ping 192.168.0.1
If no response is received, either the connection is not working, or your PC's IP address is not compatible with the DC-202's IP Address. (See next item.)
- If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.0.2 to 192.168.0.254 to be compatible with the DC-202's default IP Address of 192.168.0.1. Also, the *Network Mask* must be set to 255.255.255.0. See *Chapter 4 - PC Configuration* for details on checking your PC's TCP/IP settings.
- Ensure that your PC and the DC-202 are on the same network segment. (If you don't have a router, this must be the case.)

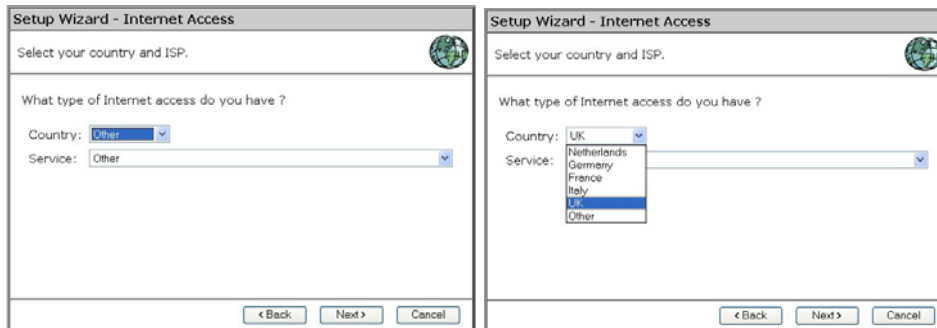
4. The start up window will now be displayed. Click on **Setup**.



5. The **Set up wizard** will now be displayed; check that the modem is connected and click on **Next**.



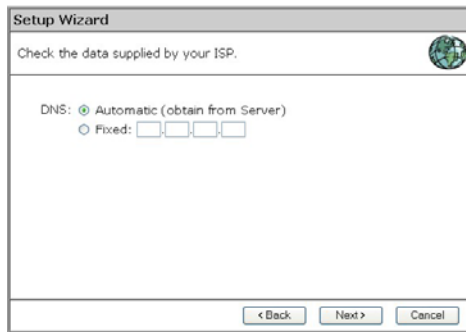
6. Select your country from the **Country** list. If your Country isn't listed, please see the next Chapter "**Your Country/ISP is not listed**"



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



8. 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 screenshot shows a window titled "Setup Wizard" with the subtitle "Check the data supplied by your ISP." Below this, there are two radio button options for DNS configuration: "Automatic (obtain from Server)" which is selected, and "Fixed:" followed by four empty input boxes. At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

9. Click **finish** to complete the configuration. Click on **Close**. If **Test Internet Connection** is checked, the router will test the connection after you have clicked on finish. Wait until this test has been completed before you click on close.



The screenshot shows a window titled "Setup Wizard" with the subtitle "Data input completed." Below this, there is a checked checkbox for "Test Internet Connection" and the instruction "Click 'Finish' to save all data to the Internet Gateway." There is a text area labeled "Test results" which is currently empty. At the bottom of the window, there are three buttons: "< Back", "Finish", and "Close".

The configuration is now completed.

Your country/ISP is not listed

Select the type of your Internet connection, (for instance cable or ADSL) and then click on **Next**.

Cable Internet

- Fill in the **Hostname** and the **Domain name**, if you received this from your Internet service provider.

For some providers it will be necessary to fill in the **MAC address** of the network card the Modem was attached to originally.

If you received an *username and password* from your ISP, then choose **PPPoE**

If you received an *Server address* from your provider besides an *username and password*, then choose **L2TP** (Currently L2TP is only used by a Dutch provider)

If you didn't receive a username and password, then choose **None**.

- PPPoE

Fill in your **Username** and your **password**.

Choose the Connect Behavior.

"Automatic connect/Disconnect" causes the router to connect as soon as an application is started which require an internet connection (i.e. MSN, ICQ, Windows update, etc.)

"Manual Connect/Disconnect" causes the router to connect only when the user clicks 'connect' in the 'Connection details' window.

"Keep Alive" causes the router to maintain the connection at all time.

The **"Auto-disconnect Time-out periode"** is the amount of time after which the router disconnects from internet.

Then click **Next**.

The image shows two side-by-side screenshots of the 'Setup Wizard - PPPoE' window. Both windows have the title 'Setup Wizard - PPPoE' and the subtitle 'Check the data supplied by your ISP.' Below the subtitle, there is a text prompt: 'Enter the PPPoE "Username" and "Password" provided by your ISP.' There are two input fields: 'User Name:' with the text 'username' and 'Password:' with a masked password '*****'. Below these fields is a 'Connect behavior:' dropdown menu. In the left screenshot, the dropdown is set to 'Automatic Connect/Disconnect'. In the right screenshot, the dropdown is open, showing three options: 'Automatic Connect/Disconnect', 'Manual Connect/Disconnect', and 'Keep alive (maintain connection)'. Below the dropdown is an 'Auto-disconnect Timeout period:' field with the value '15 min'. At the bottom of each window are three buttons: '< Back', 'Next >', and 'Cancel'.

If your provider has assigned you a fixed IP address, you input this in the field **Specified IP Address** and also fill in your **DNS IP address**. If you have a dynamic IP address, select the option **IP address is assigned automatically**. Then click **Next**.

The image shows a screenshot of the 'Setup Wizard - IP Address' window. The title is 'Setup Wizard - IP Address' and the subtitle is 'Check the data supplied by your ISP.' Below the subtitle, there is a text prompt: 'What type of IP Address was assigned by your ISP?'. There are two radio button options: 'IP Address is assigned automatically (Dynamic IP Address)' and 'Specified IP Address (Static IP Address)'. The 'Specified IP Address' option is selected. Below this option is an input field for the IP address with the placeholder 'xxxx . xxx . xxx . xxx'. Below the IP address field is a 'DNS:' section with two radio button options: 'Automatic (obtain from server)' and 'Fixed: [][][][]'. The 'Automatic' option is selected. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

Click **finish** to complete the configuration. Click on **Close**. If **Test Internet Connection** is checked, the router will test the connection after you have clicked on finish. Wait until this test has been completed before you click on close.

The image shows a screenshot of the 'Setup Wizard' window. The title is 'Setup Wizard' and the subtitle is 'Data input completed.' Below the subtitle, there is a text prompt: 'Click "Finish" to save all data to the Internet Gateway.' There is a checkbox labeled 'Test Internet Connection' which is checked. Below the checkbox is a 'Test results' section with a text area. At the bottom of the window are three buttons: '< Back', 'Finish', and 'Close'.

The configuration is now completed.

- L2TP

Fill in the L2TP server IP address or Domain Name

Fill in your **Username** and your **password**.

Choose the Connect Behavior.

"Automatic connect/Disconnect" causes the router to connect as soon as an application is started which require an internet connection (i.e. MSN, ICQ, Windows update, etc.)

"Manual Connect/Disconnect" causes the router to connect only when the user clicks 'connect' in the 'Connection details' window.

"Keep Alive" causes the router to maintain the connection at all time.

The **"Auto-disconnect Time-out periode"** is the amount of time after which the router disconnects from internet.

Then click **Next**.

If your provider has assigned you a fixed IP address, you input this in the field **Specified IP Address** and also fill in your **DNS IP address**. If you have a dynamic IP address, select the option **IP address is assigned automatically**. Then click **Next**.

Click **finish** to complete the configuration. Click on **Close**. If **Test Internet Connection** is checked, the router will test the connection after you have clicked on finish. Wait until this test has been completed before you click on close.

The configuration is now completed

- NONE

If your provider has assigned you a fixed IP address, you input this in the field **Specified IP Address** and also fill in your **DNS IP address**. If you have a dynamic IP address, select the option **IP address is assigned automatically**. The click **Next**.



The screenshot shows a dialog box titled "Setup Wizard - IP Address". The main text says "Check the data supplied by your ISP." Below this, it asks "What type of IP Address was assigned by your ISP?". There are two radio button options: "IP Address is assigned automatically (Dynamic IP Address)" and "Specified IP Address (Static IP Address)". The second option is selected. Under "Specified IP Address", there are four input fields for IP address segments, each containing "xxxx". Below that, there are two radio button options for DNS: "Automatic (obtain from server)" (selected) and "Fixed:" followed by four empty input fields. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Click **finish** to complete the configuration. Click on **Close**. If **Test Internet Connection** is checked, the router will test the connection after you have clicked on finish. Wait until this test has been completed before you click on close.



The screenshot shows a dialog box titled "Setup Wizard". The main text says "Data input completed." Below this, there is a checked checkbox for "Test Internet Connection". Underneath, it says "Click 'Finish' to save all data to the Internet Gateway." There is a text area labeled "Test results" which is currently empty. At the bottom, there are three buttons: "< Back", "Finish", and "Close".

The configuration is now completed

xDSL Internet

If you received an *username and password* from your ISP, then choose **PPPoE**

If you received an *Server address* from your provider besides an *username and password*, then choose **PPTP** or **L2TP**. Please check with your ISP which protocol you need. (Currently L2TP is only used by a Dutch provider)

If you didn't receive a username and password, then choose **None**.



Setup Wizard - DSL Modem

Check the data supplied by your ISP.

What type of Login is used for Internet Access ?

- PPPoE
- PPTP (requires PPTP Server IP Address)
- L2TP (requires L2TP Server Address)
- None (no username or password)

< Back Next > Cancel

- PPPoE

Fill in your **Username** and your **password**.

Choose the Connect Behavior.

"Automatic connect/Disconnect" causes the router to connect as soon as an application is started which require an internet connection (i.e. MSN, ICQ, Windows update, etc.)

"Manual Connect/Disconnect" causes the router to connect only when the user clicks 'connect' in the 'Connection details' window.

"Keep Alive" causes the router to maintain the connection at all time.

The **"Auto-disconnect Time-out periode"** is the amount of time after which the router disconnects from internet.

Then click **Next**.

The image shows two side-by-side screenshots of the 'Setup Wizard - PPPoE' window. Both windows have the title 'Setup Wizard - PPPoE' and the subtitle 'Check the data supplied by your ISP.' The main text says 'Enter the PPPoE "Username" and "Password" provided by your ISP.' There are input fields for 'User Name:' (containing 'username') and 'Password:' (containing '*****'). Below these are a 'Connect behavior:' dropdown menu and an 'Auto-disconnect Timeout period:' field set to '15 min'. In the left screenshot, the dropdown menu is set to 'Automatic Connect/Disconnect'. In the right screenshot, the dropdown menu is open, showing options: 'Automatic Connect/Disconnect', 'Manual Connect/Disconnect', and 'Keep alive (maintain connection)'. The 'Keep alive (maintain connection)' option is highlighted. At the bottom of each window are buttons for '< Back', 'Next >', and 'Cancel'.

If your provider has assigned you a fixed IP address, you input this in the field **Specified IP Address** and also fill in your **DNS IP address**. If you have a dynamic IP address, select the option **IP address is assigned automatically**. Then click **Next**.

The image shows a screenshot of the 'Setup Wizard - IP Address' window. The title is 'Setup Wizard - IP Address' and the subtitle is 'Check the data supplied by your ISP.' The main text asks 'What type of IP Address was assigned by your ISP?'. There are two radio buttons: 'IP Address is assigned automatically (Dynamic IP Address)' and 'Specified IP Address (Static IP Address)'. The 'Specified IP Address (Static IP Address)' radio button is selected. Below this is a text input field for the IP address, containing 'xxxx.xxxx.xxxx.xxxx'. There are also two radio buttons for DNS: 'Automatic (obtain from server)' and 'Fixed: [][][][]'. The 'Automatic (obtain from server)' radio button is selected. At the bottom of the window are buttons for '< Back', 'Next >', and 'Cancel'.

Click **finish** to complete the configuration. Click on **Close**. If **Test Internet Connection** is checked, the router will test the connection after you have clicked on finish. Wait until this test has been completed before you click on close.

The image shows a screenshot of the 'Setup Wizard' window. The title is 'Setup Wizard' and the subtitle is 'Data input completed.' There is a checkbox labeled 'Test Internet Connection' which is checked. Below this is the text 'Click "Finish" to save all data to the Internet Gateway.' and a section titled 'Test results' with an empty text area. At the bottom of the window are buttons for '< Back', 'Finish', and 'Close'.

The configuration is now completed.

- PPTP

Fill in the PPTP server IP address or Domain Name

Fill in your **Username** and your **password**.

Choose the Connect Behavior.

"Automatic connect/Disconnect" causes the router to connect as soon as an application is started which require an internet connection (i.e. MSN, ICQ, Windows update, etc.)

"Manual Connect/Disconnect" causes the router to connect only when the user clicks 'connect' in the 'Connection details' window.

"Keep Alive" causes the router to maintain the connection at all time.

The **"Auto-disconnect Time-out periode"** is the amount of time after which the router disconnects from internet.

Then click **Next**.

If your provider has assigned you a fixed IP address, you input this in the field **Specified IP Address** and also fill in your **DNS IP address**. If you have a dynamic IP address, select the option **IP address is assigned automatically**. The click **Next**.

Click **finish** to complete the configuration. Click on **Close**. If **Test Internet Connection** is checked, the router will test the connection after you have clicked on finish. Wait until this test has been completed before you click on close.

The configuration is now completed

- L2TP

Fill in the L2TP server IP address or Domain Name

Fill in your **Username** and your **password**.

Choose the Connect Behavior.

"Automatic connect/Disconnect" causes the router to connect as soon as an application is started which require an internet connection (i.e. MSN, ICQ, Windows update, etc.)

"Manual Connect/Disconnect" causes the router to connect only when the user clicks 'connect' in the 'Connection details' window.

"Keep Alive" causes the router to maintain the connection at all time.

The **"Auto-disconnect Time-out periode"** is the amount of time after which the router disconnects from internet.

Then click **Next**.

If your provider has assigned you a fixed IP address, you input this in the field **Specified IP Address** and also fill in your **DNS IP address**. If you have a dynamic IP address, select the option **IP address is assigned automatically**. The click **Next**.

Click **finish** to complete the configuration. Click on **Close**. If **Test Internet Connection** is checked, the router will test the connection after you have clicked on finish. Wait until this test has been completed before you click on close.

The configuration is now completed

- NONE

If your provider has assigned you a fixed IP address, you input this in the field **Specified IP Address** and also fill in your **DNS IP address**. If you have a dynamic IP address, select the option **IP address is assigned automatically**. The click **Next**.



The screenshot shows a window titled "Setup Wizard - IP Address". The main text says "Check the data supplied by your ISP." Below this, it asks "What type of IP Address was assigned by your ISP?". There are two radio button options: "IP Address is assigned automatically (Dynamic IP Address)" and "Specified IP Address (Static IP Address)". The second option is selected. Under "Specified IP Address", there are four input fields for IP address segments, each containing "xxxx". Below that, there are two radio button options for DNS: "Automatic (obtain from server)" (selected) and "Fixed:" followed by four empty input fields. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Click **finish** to complete the configuration. Click on **Close**. If **Test Internet Connection** is checked, the router will test the connection after you have clicked on finish. Wait until this test has been completed before you click on close.

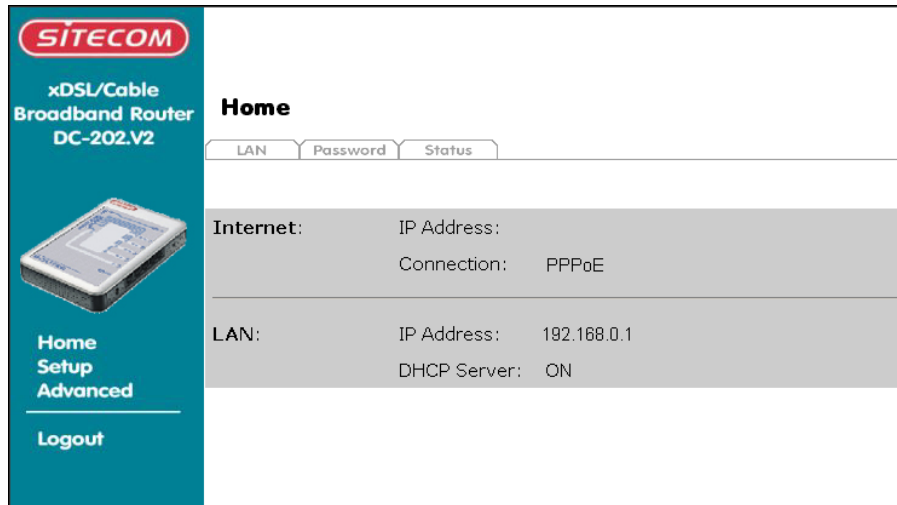


The screenshot shows a window titled "Setup Wizard". The main text says "Data input completed." Below this, there is a checked checkbox for "Test Internet Connection". Underneath, it says "Click 'Finish' to save all data to the Internet Gateway." There is a text area labeled "Test results" which is currently empty. At the bottom, there are three buttons: "< Back", "Finish", and "Close".

The configuration is now completed

Home Screen

After finishing the Setup Wizard, you will see the *Home* screen. When you connect in future, you will see this screen when you connect. An example screen is shown below.



Navigation & Data Input

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



On each screen, clicking the "Help" button will display help for that screen.

From any help screen, you can access the list of all help files (help index).

LAN Screen

Click *LAN* tab In the HOME menu to reach the **LAN** screen An example screen is shown below.

The screenshot shows the LAN configuration interface for the SITECOM DC-202.V2 router. It features a sidebar with 'Home Setup Advanced' and 'Logout' options. The main area is titled 'Home' and has three tabs: 'LAN', 'Password', and 'Status'. Under the 'LAN' tab, there are fields for 'TCP/IP' configuration: 'IP Address' (192.168.0.1), 'Subnet Mask' (255.255.255.0), a checkbox for 'DHCP Server' (unchecked), 'Start IP Address' (with a value of 2), and 'Finish IP Address' (with a value of 51). At the bottom right of the configuration area are 'Save', 'Cancel', and 'Help' buttons.

Data - LAN Screen

TCP/IP	
IP Address	IP address for the DC-202, as seen from the local LAN. Use the default value unless the address is already in use or your LAN is using a different IP address range. In the latter case, enter an unused IP Address from within the range used by your LAN.
Subnet Mask	The default value 255.255.255.0 is standard for small (class "C") networks. For other networks, use the Subnet Mask for the LAN segment to which the DC-202 is attached (the same value as the PCs on that LAN segment).
DHCP Server	<ul style="list-style-type: none"> • If Enabled, the DC-202 will allocate IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default (and recommended) value is Enabled. • If you are already using a DHCP Server, this setting must be Disabled, and the existing DHCP server must be re-configured to treat the DC-202 as the default Gateway. See the following section for further details. • The Start IP Address and Finish IP Address fields set the values used by the DHCP server when allocating IP Addresses to DHCP clients. This range also determines the number of DHCP clients supported. <p>See the following section for further details on using DHCP.</p>
Buttons	
Save	Save the data on screen.
Cancel	The "Cancel" button will discard any data you have entered and reload the file from the DC-202.

DHCP

What DHCP Does

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

- The client request is made when the client device starts up (boots).
- The DHCP Server provides the *Gateway* and *DNS* addresses to the client, as well as allocating an IP Address.
- The DC-202 can act as a **DHCP server**.
- Windows 95/98/ME and other non-Server versions of Windows will act as a DHCP **client**. This is the default Windows setting for the TCP/IP network protocol. However, Windows uses the term *Obtain an IP Address automatically* instead of "DHCP Client".
- You must NOT have two (2) or more DHCP Servers on the same LAN segment. (If your LAN does not have other Routers, this means there must only be one (1) DHCP Server on your LAN.)

Using the DC-202's DHCP Server

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

- Enable or Disable the DC-202's *DHCP Server* function.
- Set the range of IP Addresses allocated to PCs by the DHCP Server function.



Note!

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

Using another DHCP Server

You can only use one (1) DHCP Server per LAN segment. If you wish to use another DHCP Server, rather than the DC-202's, the following procedure is required.

1. Disable the DHCP Server feature in the DC-202. This setting is on the LAN screen.
2. Configure the DHCP Server to provide the DC-202's IP Address as the *Default Gateway*.

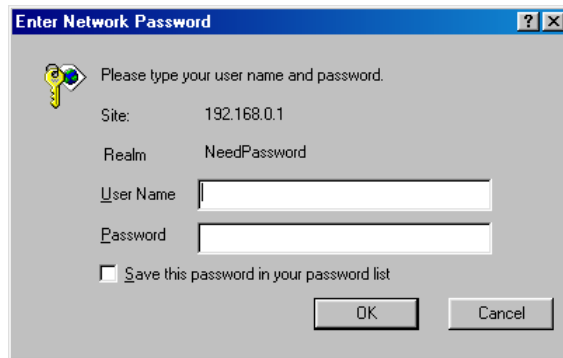
Password Screen

The password screen allows you to assign a password to the DC-202.



The screenshot shows the configuration interface for the DC-202 router. On the left is a sidebar with the SITECOM logo, product name 'xDSL/Cable Broadband Router DC-202.V2', a product image, and navigation links: 'Home Setup', 'Advanced', and 'Logout'. The main area is titled 'Home' and has tabs for 'LAN', 'Password', and 'Status'. The 'Password' tab is active, showing a description: 'The password protects the configuration data. Once set (recommended), you will be prompted for the password when you connect.' Below this are two input fields: 'New password:' and 'Verify password:', both masked with dots. At the bottom right are 'Save', 'Cancel', and 'Help' buttons.

Once you have assigned a password to the DC-202 (on the *Password* screen above) you will be prompted for the password when you connect, as shown below. (If no password has been set, this dialog will not appear.)



The screenshot shows a Windows-style dialog box titled 'Enter Network Password'. It contains a key icon and the text 'Please type your user name and password.' Below this are fields for 'Site:' (192.168.0.1) and 'Realm:' (NeedPassword). There are two input fields: 'User Name' and 'Password'. At the bottom, there is a checkbox labeled 'Save this password in your password list' which is unchecked, and 'OK' and 'Cancel' buttons.

- Leave the "User Name" blank.
- Enter the password for the DC-202, as set on the *Password* screen above.

Operation and Status

Operation

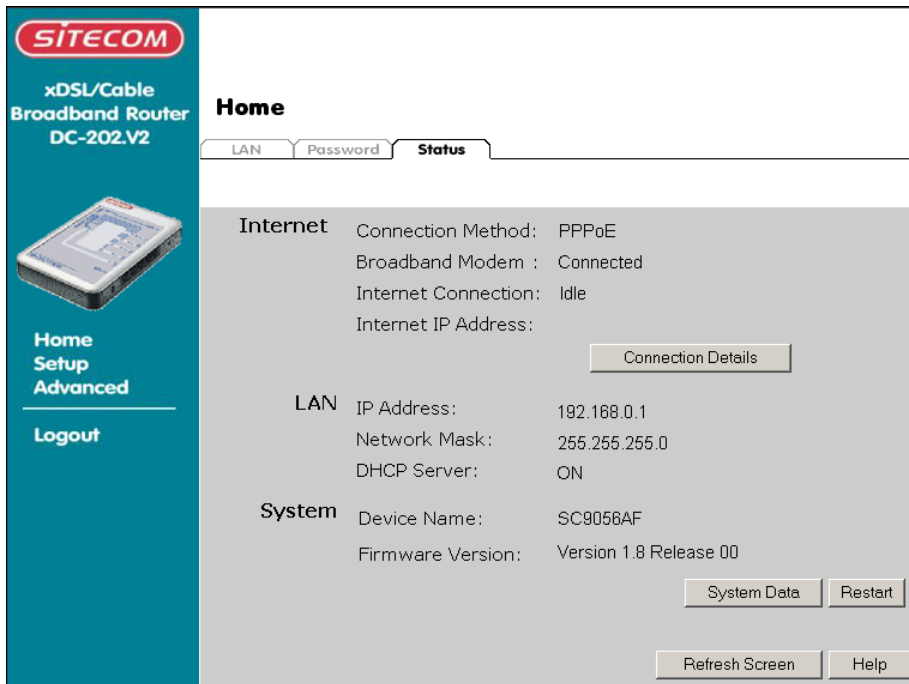
Once both the DC-202 and the PCs are configured, operation is automatic.

However, there are some situations where additional Internet configuration may be required:

- If using Internet-based **Communication Applications**, it may be necessary to specify which PC receives an incoming connection. Refer to chapter *Advanced Features* for further details.
- Applications which use non-standard connections or port numbers may be blocked by the DC-202's built-in firewall. You can define such applications as **Special Applications** to allow them to function normally. Refer to chapter *Advanced Features* for further details.
- Some non-standard applications may require use of the **DMZ** feature. Refer to chapter *Advanced Features* for further details.

Status Screen

Use the **Status** tab on the Home menu to view this screen.



The screenshot shows the web interface for the Sitecom DC-202 V2 router. The left sidebar contains the Sitecom logo, the product name 'xDSL/Cable Broadband Router DC-202.V2', an image of the router, and navigation links: 'Home Setup', 'Advanced', and 'Logout'. The main content area is titled 'Home' and has three tabs: 'LAN', 'Password', and 'Status' (which is selected). The 'Status' tab displays the following information:

Internet	Connection Method:	PPPoE
	Broadband Modem :	Connected
	Internet Connection:	Idle
	Internet IP Address:	
		Connection Details
LAN	IP Address:	192.168.0.1
	Network Mask:	255.255.255.0
	DHCP Server:	ON
System	Device Name:	SC9056AF
	Firmware Version:	Version 1.8 Release 00
		System Data Restart
		Refresh Screen Help

Data - Status Screen

Internet	
Connection Method	This indicates the current connection method, as set in the Setup Wizard.
Broadband Modem	This shows the connection status of the modem.
Internet Connection	<p>Current connection status:</p> <ul style="list-style-type: none"> • Active • Idle • Unknown • Failed <p>If there is an error, you can click the "Connection Details" button to find out more information.</p>
Internet IP Address	This IP Address is allocated by the ISP (Internet Service Provider).
"Connection Details" Button	Click this button to open a sub-window and view a detailed description of the current connection. Depending on the type of connection, a "log" may also be available.
LAN	
IP Address	The IP Address of the DC-202.
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.
DHCP Server	<p>This shows the status of the DHCP Server function - either "Enabled" or "Disabled".</p> <p>For additional information about the PCs on your LAN, and the IP addresses allocated to them, use the <i>PC Database</i> option on the <i>Advanced</i> menu.</p>
System	
Device Name	This displays the current name of the DC-202.
Firmware Version	The current version of the firmware installed in the DC-202.
"System Data" Button	Clicking this button will open a Window which lists all system details and settings.
Buttons	
Connection Details	View the details of the current Internet connection. The sub-screen displayed will depend on the connection method used. See the following sections for details of each sub-screen.
System Data	Display all system information in a sub-window.
Restart	Clicking this button will restart (reboot) the DC-202. All existing connections though the DC-202 will be terminated, but will usually re-connect automatically.
Refresh Screen	Update the data displayed on screen.

Connection Status - PPPoE

If using PPPoE (PPP over Ethernet), a screen like the following example will be displayed when the "Connection Details" button is clicked.

Connection Status - PPPoE

Connection

Physical Address: 00-c0-02-01-85-7d
 IP Address:
 Network Mask:
 PPPoE Link Status: OFF

Connection Log

```
005:Reset physical connection
004:stop PPP
003:try to hang up
002:sub_wait:timeout
001:wait 100 msec "WAN start... "
000:stop PPP
```

Connect and Disconnect buttons should only be needed if the setting "Connect automatically, as required" is Disabled.

Data - PPPoE Screen

Connection	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.
PPPoE Link Status	This indicates whether or not the connection is currently established. <ul style="list-style-type: none"> If the connection does not exist, the "Connect" button can be used to establish a connection. If the connection currently exists, the "Disconnect" button can be used to break the connection.
Connection Log	
Connection Log	<ul style="list-style-type: none"> 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.
Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

Connection Status - PPTP

If using PPTP (Peer-to-Peer Tunneling Protocol), a screen like the following example will be displayed when the "Connection Details" button is clicked.

Connection Status - PPTP

Connection

Physical Address: 00-c0-02-01-85-7d
 IP Address: 192.168.9.43
 Connection Status ON

Connection Log

```
014:port[2]:ppp up successfully
013:IPCP up, set MTU:1500
012:start PPP
011:physical line is connected
010:Reset physical connection
009:stop PPP
```

Connect and Disconnect buttons should only be needed if using "Manual Connection".

Data - PPTP Screen

Connection	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
PPTP Status	<p>This indicates whether or not the connection is currently established.</p> <ul style="list-style-type: none"> If the connection does not exist, the "Connect" button can be used to establish a connection. If the connection currently exists, the "Disconnect" button can be used to break the connection.
Connection Log	
Connection Log	<ul style="list-style-type: none"> The Connection Log shows status messages relating to the existing connection. The "Clear Log" button will restart the Log, while the Refresh button will update the messages shown on screen.
Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

Connection Status - L2TP

If using L2TP, a screen like the following example will be displayed when the "Connection Details" button is clicked.

Figure 1: L2TP Status Screen

Data - L2TP Screen

Connection	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Connection Status	<p>This indicates whether or not the connection is currently established.</p> <ul style="list-style-type: none"> If the connection does not exist, the "Connect" button can be used to establish a connection. If the connection currently exists, the "Disconnect" button can be used to break the connection.
Connection Log	
Connection Log	<ul style="list-style-type: none"> The Connection Log shows status messages relating to the existing connection. The "Clear Log" button will restart the Log, while the Refresh button will update the messages shown on screen.
Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

Connection Log Messages

Message	Description
Connect on Demand	Connection attempt has been triggered by the "Connect automatically, as required" 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 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, a 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.

Connection Details - Fixed/Dynamic IP Address

If your access method is "Direct" (no login), a screen like the following example will be displayed when the "Connection Details" button is clicked.

Connection Details

Internet

Physical Address: 00-c0-02-01-85-7d
 IP Address: 192.168.9.42
 Network Mask: 255.255.255.0
 Default Gateway: 192.168.9.254
 DNS IP Address: 168.95.192.1
 168.95.1.1
 DHCP Client: ON
 Lease obtained: 0 days,0 hrs,10 minutes
 Remaining lease time: 0 days,0 hrs,9 minutes

Data - Fixed/Dynamic IP address Screen

Internet	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.
Default Gateway	The IP Address of the remote Gateway or Router associated with the IP Address above.
DNS IP Address	The IP Address of the Domain Name Server which is currently used.
DHCP Client	<p>This will show "Enabled" or "Disabled", depending on whether or not this device is functioning as a DHCP client.</p> <p>If "Enabled" the "Remaining lease time" field indicates when the IP Address allocated by the DHCP Server will expire. The lease is automatically renewed on expiry; use the "Renew" button if you wish to manually renew the lease immediately.</p>
Buttons	
Re-lease/Renew Button will display EITHER "Release" OR "Renew"	<p>This button is only useful if the IP address shown above is allocated automatically on connection. (Dynamic IP address). If you have a Fixed (Static) IP address, this button has no effect.</p> <ul style="list-style-type: none"> If the ISP's DHCP Server has NOT allocated an IP Address for the DC-202, this button will say "Renew". Clicking the "Renew" button will attempt to re-establish the connection and obtain an IP Address from the ISP's DHCP Server. If an IP Address has been allocated to the DC-202 (by the ISP's DHCP Server), this button will say "Release". Clicking the "Release" button will break the connection and release the IP Address.
Refresh	Update the data shown on screen.

Advanced Features

Overview

The following advanced features are provided.

- Advanced Internet
- Communication Applications
- Special Applications
- Multi-DMZ
- URL Filter
- Access Control
- Remote Management
- Virtual Servers
- Dynamic DNS
- Upgrade Firmware
- Config File
- PC Database
- Network Diagnostics
- Options
- Security
- Logs
- MAC Address
- Routing

These features are all available from the ***Advanced*** menu. This Chapter provides details of each feature.

Advanced Internet Screen

This screen allows configuration of all advanced features relating to Internet access.

- Communication Applications
- Special Applications
- Multi-DMZ
- URL filter

An example screen is shown below.

Advanced Internet
Access control
Remote management
Virtual servers
Dynamic DNS
Upgrade Firmware
Config File

PC Database
Network diag
Options
Security
Logs
MAC Address
Routing

Communication Applications

Select an Application: Age of Empires
H323(CUseeME & MS NetMeeting & TGI Phone)
ICU II (ICU 2)
Internet Phone

Send incoming calls to: Select a PC
 Save when finished, not after each change.

Special Applications

If an application does not work, you can define it as a Special Application.

Special Applications

Multi-DMZ

If you have only 1 WAN IP address, only DMZ 1 can be used.

	Enable WAN IP address	PC
1.	<input type="checkbox"/>	Select a PC
2.	<input type="checkbox"/> 0 . 0 . 0 . 0	Select a PC
3.	<input type="checkbox"/> 0 . 0 . 0 . 0	Select a PC
4.	<input type="checkbox"/> 0 . 0 . 0 . 0	Select a PC
5.	<input type="checkbox"/> 0 . 0 . 0 . 0	Select a PC
6.	<input type="checkbox"/> 0 . 0 . 0 . 0	Select a PC
7.	<input type="checkbox"/> 0 . 0 . 0 . 0	Select a PC

[My PC is not listed](#)

URL Filter

Enable [URL Filter](#)

Configure URL Filter

Save

Cancel

Help

Communication Applications

Most applications are supported transparently by the DC-202. But sometimes it is not clear which PC should receive an incoming connection. This problem could arise with the **Communication Applications** listed on this screen.

If this problem arises, you can use this screen to set which PC should receive an incoming connection, as described below.

Data - Communication Applications

Select an Application

This lists applications which may generate incoming connections, where the destination PC (on your local LAN) is unknown.

Send incoming calls to

This lists the PCs on your LAN.

- If necessary, you can add PCs manually, using the "PC Database" option on the advanced menu.
- For each application listed above, you can choose a destination PC.
- There is no need to "Save" after each change; you can set the destination PC for each application, then click "Save".

Special Applications

If you use Internet applications which use non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the DC-202's firewall. In this case, you can define the application as a "Special Application".

Special Applications Screen

This screen can be reached by clicking the *Special Applications* button on the *Internet* screen.

You can then define your Special Applications. You will need detailed information about the application; this is normally available from the supplier of the application.

Also, note that the terms "Incoming" and "Outgoing" on this screen refer to traffic from the client (PC) viewpoint

Special Applications							
Special Applications can only be used by 1 user at any time.							
	Name	Incoming Ports			Outgoing Ports		
		Type	Start	Finish	Type	Start	Finish
1. <input type="checkbox"/>	dialpad	udp	51200	51201	udp	51200	51201
2. <input type="checkbox"/>	paltalk	udp	2090	2091	udp	2090	2091
3. <input type="checkbox"/>	quicktime	udp	6970	6999	tcp	554	554
4. <input type="checkbox"/>		udp			udp		
5. <input type="checkbox"/>		udp			udp		
6. <input type="checkbox"/>		udp			udp		
7. <input type="checkbox"/>		udp			udp		
8. <input type="checkbox"/>		udp			udp		
9. <input type="checkbox"/>		udp			udp		
10. <input type="checkbox"/>		udp			udp		
11. <input type="checkbox"/>		udp			udp		
12. <input type="checkbox"/>		udp			udp		

Data - Special Applications Screen

Check-box	Use this to Enable or Disable this Special Application as required.
Name	Enter a descriptive name to identify this Special Application.
Incoming Ports	<ul style="list-style-type: none"> • Type - Select the protocol (TCP or UDP) used when you receive data from the special application or service. (Note: Some applications use different protocols for outgoing and incoming data). • Start - Enter the beginning of the range of port numbers used by the application server, for data you receive. If the application uses a single port number, enter it in both the "Start" and "Finish" fields. • Finish - Enter the end of the range of port numbers used by the application server, for data you receive.
Outgoing Ports	<ul style="list-style-type: none"> • Type - Select the protocol (TCP or UDP) used when you send data to the remote system or service. • Start - Enter 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. • Finish - Enter the end 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.

Using a Special Application

- Configure the *Special Applications* screen as required.
- On your PC, use the application normally. Remember that only one (1) PC can use each Special application at any time. Also, when 1 PC is finished using a particular Special Application, there may need to be a "Time-out" before another PC can use the same Special Application. The "Time-out" period may be up to 3 minutes.



Note!

If an application still cannot function correctly, try using the "DMZ" feature.

Multi-DMZ

This feature, if enabled, allows one (1) or more computers on your LAN to be exposed to all users on the Internet.

- If you only have 1 WAN IP addresses, only DMZ 1 can be used. This uses the primary IP address (which may be dynamic), so you do not have to enter it.
- If you have multiple WAN IP addresses, you can specify a DMZ PC for each IP address. You must enter the other WAN IP addresses which are allocated to you.

The DMZ feature allows unrestricted 2-way communication between the "DMZ PC" and other Internet users or Servers.

- This allows almost any application to be used on the "DMZ PC".
- The "DMZ PC" will receive all "Unknown" connections and data sent to the corresponding IP address from the Internet.

- If the DMZ feature is enabled, you must select the PC to be used as the "DMZ PC".



The "DMZ PC" is effectively outside the Firewall, making it more vulnerable to attacks. For this reason, you should only enable the DMZ feature when required.

URL Filter

The URL Filter allows you to block access to undesirable Web site

- To use this feature, you must define "filter strings". If the "filter string" appears in a requested URL, the request is blocked.
- Enabling the *URL Filter* also affects the *Internet Access Log*. If Enabled, the "Destination" field in the log will display the URL. Otherwise, it will display the IP Address.
- The *URL Filter* can be Enabled or Disabled on the *Advanced Internet* screen.

URL Filter Screen

Click the "Configure URL Filter" button on the *Internet* screen to access the *URL Filter* screen. An example screen is shown below.

URL Filter

Filter Strings

When enabled, a request is blocked if any of these entries occur in the requested URL.

Current Entries

Add Filter String:

Filter Strings should be as specific as possible.

Data - URL Filter Screen

Filter Strings	
Current Entries	This lists any existing entries. If you have not entered any values, this list will be empty.
Add Filter String	To add an entry to the list, enter it here, and click the "Add" button. An entry may be a Domain name (e.g. www.trash.com) or simply a string. (e.g. ads/) Any URL which contains ANY entry ANYWHERE in the URL will be blocked.
Buttons	
De-lete/Delete All	Use these buttons to delete the selected entry or all entries, as required. Multiple entries can be selected by holding down the CTRL key while selecting.(On the Macintosh, hold the SHIFT key while selecting.)
Add	Use this to add the current Filter String to the site list.

Access Control

This feature is accessed by the *Access Control* link on the Advanced menu.

Overview

The Access Control feature allows administrators to restrict the level of Internet Access available to PCs on your LAN. With the default settings, everyone has unrestricted Internet access.

To use this feature:

1. Set the desired restrictions on the "Default" group. All PCs are in the "Default" group unless explicitly moved to another group.
2. Set the desired restrictions on the other groups ("Group 1", "Group 2", "Group 3" and "Group 4") as needed.
3. Assign PC to the groups as required.



Restrictions are imposed by blocking "Services", or types of connections. All common Services are pre-defined. If required, you can also define your own Services.

Access Control Screen

To view this screen, select the *Access Control* link on the Advanced menu.

Advanced

Advanced Internet	Access control	Remote management	Virtual servers	Dynamic DNS	Upgrade Firmware	Config File
PC Database	Network diag	Options	Security	Logs	MAC Address	Routing

Group Group 1 Members

Internet Access Restrictions: Block all Internet access

Block by Schedule: None Define Schedule

Services

ALL(TCP/UDP:1..65534)

AIM(TCP:5190)

BGP(TCP:179)

BOOTP_CLIENT(UDP:68)

BOOTP_SERVER(UDP:67..68)

CU-SEEME(TCP/UDP:7648)

DNS(TCP/UDP:53)

FINGER(TCP:79)

Edit Service List

Select Services to Block.
Hold CTRL key (on MAC, SHIFT) to select multiple items

View Log
 Clear Log
 Refresh

Save
 Cancel
 Help

Data - Access Control Screen

Group	
Group	Select the desired Group. The screen will update to display the settings for the selected Group. Groups are named "Default", "Group 1", "Group 2", "Group 3" and "Group 4", and cannot be re-named.
"Members" Button	<p>Click this button to add or remove members from the current Group.</p> <ul style="list-style-type: none"> If the current group is "Default", then members can not be added or deleted. This group contains PCs not allocated to any other group. To remove PCs from the Default Group, assign them to another Group. To assign PCs to the Default Group, delete them from the Group they are currently in. <p>See the following section for details of the <i>Group Members</i> screen.</p>
Internet Access	
Restrictions	<p>Select the desired options for the current group:</p> <ul style="list-style-type: none"> None - Nothing is blocked. Use this to create the least restrictive group. Block all Internet access - All traffic via the WAN port is blocked. Use this to create the most restrictive group. Block selected Services - You can select which Services are to block. Use this to gain fine control over the Internet access for a group.

Block by Schedule	If Internet access is being blocked, you can choose to apply the blocking only during scheduled times. (If access is not blocked, no Scheduling is possible, and this setting has no effect.)
Define Schedule Button	Clicking this will open a sub-window where you can define or modify the Schedule.
Services	This lists all defined Services. Select the Services you wish to block. To select multiple services, hold the CTRL key while selecting. (On the Macintosh, hold the SHIFT key rather than CTRL.)
Edit Service List Button	If you wish to define additional Services, or manage the Service list, click this button to open the "Services" screen.
Buttons	
Members	Click this button to add or remove members from the current Group. If the current group is "Default", then members can not be added or deleted. This group contains PCs not allocated to any other group. See the following section for details of the <i>Group Members</i> screen.
Define Schedule	Click this to open a sub-window where you can define or modify the Schedule.
Edit Service List	If you wish to define additional Services, or manage the Service list, click this button to open the "Services" screen.
Save	Save the data on screen.
Cancel	Reverse any changes made since the last "Save".
View Log	Click this to open a sub-window where you can view the "Access Control" log. This log shows attempted Internet accesses which have been blocked by the Access Control feature.
Clear Log	Click this to clear and restart the "Access Control" log, making new entries easier to read.
Refresh	Update the data on screen.

Group Members Screen

This screen is displayed when the *Members* button on the *Access Control* screen is clicked.

The screenshot shows a window titled "Group Members" with a subtitle "Group: Group 1". It features two list boxes: "Members (PCs)" on the left and "Other PCs" on the right. The "Other PCs" list contains one entry: "jessica.192.168.0.5 (LAN)". Between the list boxes are three buttons: "Del >>", "<< Add", and "Close".

Use this screen to add or remove members (PCs) from the current group.

- The "Del >>" button will remove the selected PC (in the *Members* list) from the current group.
- The "<< Add" button will add the selected PC (in the *Other PCs* list) to the current group.



**PCs not assigned to any group will be in the "Default" group.
PCs deleted from any other Group will be added to the "Default" group.**

Default Schedule Screen

This screen is displayed when the *Define Schedule* button on the *Access Control* screen is clicked.

- This schedule can be (optionally) applied to any Access Control Group.
- Blocking will be performed during the scheduled time (between the "Start" and "Finish" times.)
- Two (2) separate sessions or periods can be defined.
- Times must be entered using a 24 hr clock.
- If the time for a particular day is blank, no action will be performed.

Default Schedule				
Use 24 hour clock. On all day: 00:00 to 24:00 Off all day: All fields blank				
Day	Session 1		Session 2	
	Start	Finish	Start	Finish
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"/>
Sunday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Data - Default Schedule Screen

Day	Each day of the week can scheduled independently.
Session 1 Session 2	Two (2) separate sessions or periods can be defined. Session 2 can be left blank if not required.

Start	Enter the start using a 24 hr clock.
Finish	Enter the finish time using a 24 hr clock.

Services Screen

This screen is displayed when the *Edit Service List* button on the *Access Control* screen is clicked.

The screenshot shows a window titled "Services". Inside, there is a section "Available Services" with a list box containing: ALL(TCP/UDP:1..65534), AIM(TCP:5190), BGP(TCP:179), BOOTP_CLIENT(UDP:68), BOOTP_SERVER(UDP:67,68), and CU-SEEME(TCP/UDP:7648). Below the list is a "Delete" button. Below that is a section "Add New Service" with a dialog box containing: Name: (text input), Type: (dropdown menu with "TCP" selected), Start Port: (text input) (TCP or UDP), Finish Port: (text input) (TCP or UDP), and ICMP Type: (dropdown menu with "n/a" selected) (0..255). Below the dialog are "Add" and "Cancel" buttons. At the bottom right of the window are "Help" and "Close" buttons.

Data - Services Screen

Available Services	
Available Services	This lists all the available services.
"Delete" button	Use this to delete any Service you have added. Pre-defined Services can not be deleted.
Add New Service	
Name	Enter a descriptive name to identify this service.
Type	Select the protocol (TCP, UDP, ICMP) used to the remote system or service.
Start Port	For TCP and UDP Services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the "Start" and "Finish" fields.
Finish Port	For TCP and UDP Services, enter the end of the range of port numbers used by the service. If the service uses a single port number, enter it in both the "Start" and "Finish" fields.
ICMP Type	For ICMP Services, enter the type number of the required service.

Buttons	
Delete	Delete the selected service from the list.
Add	Add a new entry to the Service list, using the data shown in the "Add New Service" area on screen.
Cancel	Clear the " Add New Service " area, ready for entering data for a new Service.

Access Control Log

To check the operation of the Access Control feature, an *Access Control Log* is provided. Click the *View Log* button on the *Access Control* screen to view this log.

This log shows attempted Internet accesses which have been **blocked** by the *Access Control* function.

Data shown in this log is as follows:

Date/Time	Date and Time of the attempted access.
Name	If known, the name of the PC whose access was blocked. This name is taken from the <i>Network Clients</i> database
Source IP address	The IP Address of the PC or device whose access request was blocked
MAC address	The hardware or physical address of the PC or device whose access request was blocked
Destination	The destination URL or IP address

Remote Management

If enabled, this feature allows you to manage the DC-202 via the Internet.

Advanced						
Advanced Internet	Access control	Remote management	Virtual servers	Dynamic DNS	Upgrade Firmware	Config File
PC Database	Network diag	Options	Security	Logs	MAC Address	Routing
<p>Remote Administration If enabled, this device can be administered via the Internet, using your Web Browser. See help for details of the "Port Number".</p> <p><input type="checkbox"/> Enable Remote Management</p> <p>Port Number: <input type="text" value="8080"/></p> <p>Current IP Address to connect to this device:</p> <p style="text-align: right;"> <input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/> </p>						

Figure 2: Remote Management Screen

Data - Remote Management Screen

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

To connect from a remote PC via the Internet

1. Ensure your Internet connection is established, and start your Web Browser.
2. In the "Address" bar, enter "HTTP://" followed by the Internet IP Address of the DC-202. If the port number is not 80, the port number is also required. (After the IP Address, enter ":" followed by the port number.)

e.g.

HTTP://123.123.123.123:8080

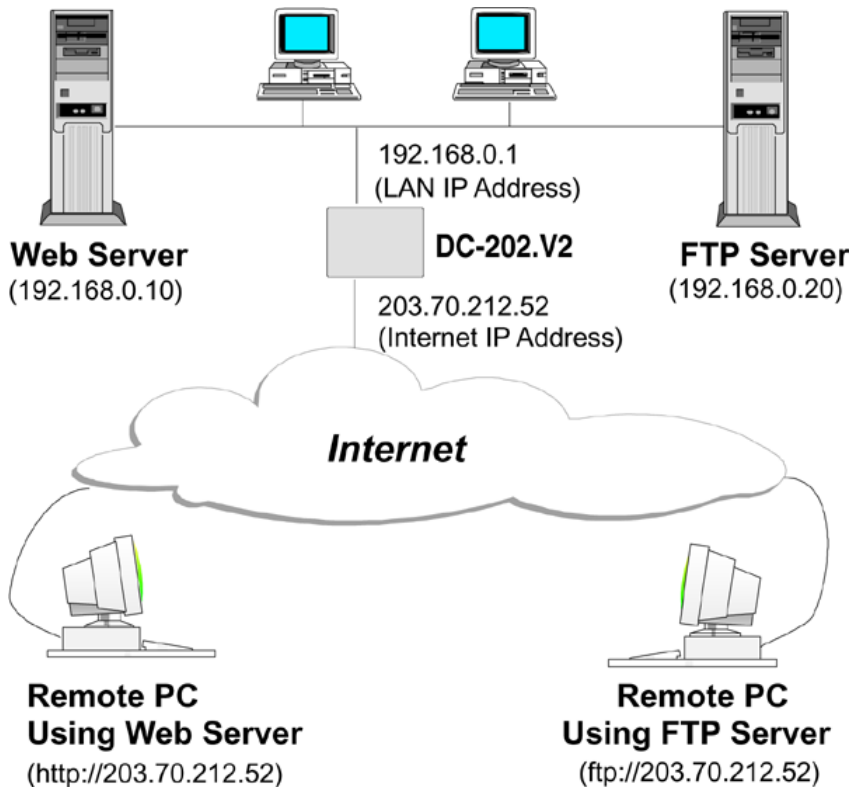
This example assumes the WAN IP Address is 123.123.123.123, and the port number is 8080.

Virtual Servers

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

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

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



IP Address seen by Internet Users

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

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

This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers.

However, you can use the *DDNS (Dynamic DNS)* feature to allow users to connect to your Virtual Servers using a URL, instead of an IP Address.

Virtual Servers Screen

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

Advanced

Advanced Internet
Access control
Remote management
Virtual servers
Dynamic DNS
Upgrade Firmware
Config File

PC Database
Network diag
Options
Security
Logs
MAC Address
Routing

Servers

Defaults
Disable All

Web
FTP(Control)
FTP(Data)
E-Mail(POP3)
E-Mail(SMTP)

Delete

Properties

Clear Form

Enable Web
PC (Server): Select a PC [My PC is not listed](#)
Protocol: TCP
Internal (LAN) Ports: 80 ~ 80
External (WAN) Ports: 80 ~ 80

Update Selected Server
Add as new Server

Help

This screen lists a number of pre-defined Servers, and allows you to define your own Servers. Details of the selected Server are shown in the "Properties" area.

Data - Virtual Servers Screen

Servers	
Servers	This lists a number of pre-defined Servers, plus any Servers you have defined. Details of the selected Server are shown in the "Properties" area.
Properties	
Enable	Use this to Enable or Disable support for this Server, as required. <ul style="list-style-type: none"> If Enabled, any incoming connections will be forwarded to the selected PC. If Disabled, any incoming connection attempts will be blocked.
PC (Server)	Select the PC for this Server. The PC must be running the appropriate Server software.
Protocol	Select the protocol (TCP or UDP) used by the Server.
Internal (LAN) Ports	Enter the port number which the Server software is configured to use.
External (WAN) Ports	The port number used by Internet users when connecting to the Server. This is normally the same as the Internal Port Number. If it is different, this device will perform a "mapping" or "translation" function, allowing the server to use one port address, while clients use a different port address.

Buttons	
Defaults	This will delete any Servers you have defined, and set the pre-defined Servers to use their default port numbers.
Disable All	This will cause the "Enable" setting of all Virtual Servers to be set OFF.
Update Selected Server	Update the current Virtual Server entry, using the data shown in the "Properties" area on screen.
Add as new Server	Add a new entry to the Virtual Server list, using the data shown in the "Properties" area on screen. The entry selected in the list is ignored, and has no effect.
Delete	Delete the current Virtual Server entry. Note that the pre-defined Servers can not be deleted. Only Servers you have defined yourself can be deleted.
Clear Form	Clear all data from the "Properties" area, ready for input of a new Virtual Server entry.



For each entry, the PC must be running the appropriate Server software.

Defining your own Virtual Servers

If the type of Server you wish to use is not listed on the *Virtual Servers* screen, you can define and manage your own Servers:

Create a new Server:

1. Click "Clear Form"
2. Enter the required data, as described above.
3. Click "Add".
4. The new Server will now appear in the list.

Modify (Edit) a Server:

1. Select the desired Server from the list
2. Make any desired changes (for example, change the Enable/Disable setting).
3. Click "Update" to save changes to the selected Server.

Delete a Server:

1. Select the entry from the list.
2. Click "Delete".

Note: You can only delete Servers you have defined. Pre-defined Server cannot be deleted.



From the Internet, ALL Virtual Servers have the IP Address allocated by your ISP.

Connecting to the Virtual Servers

Once configured, anyone on the Internet can connect to your Virtual Servers. They must use the Internet IP Address (the IP Address allocated to you by your ISP).

e.g.

`http://203.70.212.52`

`ftp://203.70.212.52`

It is more convenient if you are using a Fixed IP Address from your ISP, rather than Dynamic. However, you can use the *Dynamic DNS* feature, described in the following section, to allow users to connect to your Virtual Servers using a URL, rather than an IP Address.

Dynamic DNS (Domain Name Server)

This free service is very useful when combined with the *Virtual Server* feature. It allows Internet users to connect to your Virtual Servers using a URL, rather than an IP Address.

This also solves the problem of having a dynamic IP address. With a dynamic IP address, your IP address may change whenever you connect, which makes it difficult to connect to you.

The Service works as follows:

1. You must register for the service at <http://www.dyndns.org> (Registration is free). Your password will be E-mailed to you.
2. After registration, use the "Create New Host" option (at www.dyndns.org) to request your desired Domain name.
3. Enter your data from www.dyndns.org in the DC-202's DDNS screen.
4. The DC-202 will then automatically ensure that your current IP Address is recorded at <http://www.dyndns.org>
5. From the Internet, users will be able to connect to your Virtual Servers (or DMZ PC) using your Domain name, as shown on this screen.

Dynamic DNS Screen

Select *Advanced* on the main menu, then *Dynamic DNS*, to see a screen like the following:

Advanced						
Advanced Internet	Access control	Remote management	Virtual servers	Dynamic DNS	Upgrade Firmware	Config File
PC Database	Network diag	Options	Security	Logs	MAC Address	Routing
<p>DDNS Service DDNS (Dynamic DNS) allows Internet users to connect to your Virtual Servers (or DMZ PC) using a domain name instead of an IP Address.</p> <p>You must Register for the DDNS service at one of the listed Service suppliers.</p> <p>DDNS Data DDNS Service: <input type="text" value="dyndns"/> <input type="button" value="Web Site"/></p> <p>User Name: <input type="text"/></p> <p>Password/Key: <input type="text"/></p> <p>Domain Name: <input type="text"/> .<input type="text" value="dyndns"/> .<input type="text" value="org"/></p> <p>Domain name allocated to you by the Service</p> <p>DDNS Status:</p> <p style="text-align: right;"><input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/></p>						

Data - Dynamic DNS Screen

DDNS Service	
DDNS Service	<ul style="list-style-type: none"> You must register for the service at one of the listed Service Providers. You can reach the Service provider's Web Site by selecting them in the list and clicking the "Web Site" button. Apply for a Domain Name, and ensure it is allocated to you. Details of your DDNS account (Name, password, Domain name) must then be entered and saved on this screen. This device will then automatically ensure that your current IP Address is recorded by the DDNS Service Provider. (You do NOT need to use the "Client" program provided by some DDNS Service providers.) From the Internet, users will now be able to connect to your Virtual Servers (or DMZ PC) using your Domain name.
DDNS Data	
DDNS Service	Select the desired DDNS Service provider.
User Name	Enter your Username for the DDNS Service.
Pass-word/Key	Enter your current password for the DDNS Service.
Domain Name	Enter the domain name allocated to you by the DDNS Service. If you have more than one name, enter the name you wish to use.
DDNS Status	<ul style="list-style-type: none"> This message is returned by the DDNS Server Normally, this message should be "Update successful" If the message is "No host", this indicates the host name entered was not allocated to you. You need to connect to DDNS Service provider and correct this problem.

Upgrade Firmware

The firmware (software) in the DC-202 can be upgraded using your Web Browser.

You must first download the upgrade file, then select *Upgrade* on the *Advanced* menu. You will see a screen like the following.

Advanced						
Advanced Internet	Access control	Remote management	Virtual servers	Dynamic DNS	Upgrade Firmware	Config File
PC Database	Network diag	Options	Security	Logs	MAC Address	Routing
<p>The upgrade firmware file needs to be downloaded and stored on your PC.</p> <p>DC-202.V2 Password: <input type="text"/></p> <p>Upgrade File: <input type="text"/> <input type="button" value="Browse..."/></p> <p><input type="button" value="Start Upgrade"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/></p>						

To perform the Firmware Upgrade:

6. Click the "Browse" button and navigate to the location of the upgrade file.
7. Select the upgrade file. Its name will appear in the *Upgrade File* field.
8. Click the "Start Upgrade" button to commence the firmware upgrade.



The DC-202 is unavailable during the upgrade process, and must restart when the upgrade is completed. Any connections to or through the DC-202 will be lost.

Config File

This feature allows you to download the current settings from the DC-202, and save them to a file on your PC.

You can restore a previously-downloaded configuration file to the DC-202, by uploading it to the DC-202.

This screen also allows you to set the DC-202 back to its factory default configuration. Any existing settings will be deleted.

An example *Config File* screen is shown below.

Data - Config File Screen

Backup Config	Use this to download a copy of the current configuration, and store the file on your PC. Click <i>Download</i> to start the download.
Restore Config	<p>This allows you to restore a previously-saved configuration file back to the DC-202.</p> <p>Click <i>Browse</i> to select the configuration file, then click <i>Restore</i> to upload the configuration file.</p> <p>WARNING !</p> <p>Uploading a configuration file will destroy (overwrite) ALL of the existing settings.</p>
Default Config	<p>Clicking the <i>Restore Defaults</i> button will reset the DC-202 to its factory default settings.</p> <p>WARNING !</p> <p>This will delete ALL of the existing settings.</p>

PC Database

The PC Database is used whenever you need to select a PC (e.g. for the "DMZ" PC). It eliminates the need to enter IP addresses. Also, you do not need to use fixed IP addresses on your LAN.

PC Database Screen

An example *PC Database* screen is shown below.

The screenshot shows the 'Advanced Administration' interface with the 'PC Database' tab selected. The interface includes a navigation menu with options like 'Advanced Internet', 'Access control', 'Remote management', 'Virtual servers', 'Dynamic DNS', 'Upgrade Firmware', 'Config File', 'Network diag', 'Options', 'Security', 'Logs', 'MAC Address', and 'Routing'. The main content area contains instructions: 'DHCP Clients are automatically added and updated. If not listed, try restarting the PC. PCs using a Fixed IP address can be added and deleted below.' Below this is a 'Known PCs' list with one entry: 'jessica 192.168.0.2 (LAN) (DHCP)'. To the right of the list is an 'Add' button and a form for entering a 'Name' and 'IP Address'. At the bottom of the list area is a 'Delete' button. At the bottom of the main content area are 'Refresh' and 'Generate Report' buttons. At the very bottom are 'Advanced Administration' and 'Help' buttons.

- PCs which are "DHCP Clients" are automatically added to the database, and updated as required.
- By default, non-Server versions of Windows act as "DHCP Clients"; this setting is called "Obtain an IP Address automatically".
- The DC-202 uses the "Hardware Address" to identify each PC, not the name or IP address. The "Hardware Address" can only change if you change the PC's network card or adapter.
- This system means you do NOT need to use Fixed (static) IP addresses on your LAN. However, you can add PCs using Fixed (static) IP Addresses to the PC database if required.

Data - PC Database Screen

Known PCs	This lists all current entries. Data displayed is <i>name (IP Address) type</i> . The "type" indicates whether the PC is connected to the LAN.
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC's "hostname".
IP Address	Enter the IP Address of the PC. The PC will be sent a "ping" to determine its hardware address. If the PC is not available (not connected, or not powered On) you will not be able to add it.
Buttons	
Add	This will add the new PC to the list. The PC will be sent a "ping" to determine its hardware address. If the PC is not available (not connected, or not powered On) you will not be able to add it.
Delete	Delete the selected PC from the list. This should be done in 2 situations: <ul style="list-style-type: none"> • The PC has been removed from your LAN. • The entry is incorrect.
Refresh	Update the data on screen.
Generate Report	Display a read-only list showing full details of all entries in the PC database.
Advanced Administration	View the Advanced version of the PC database screen - <i>PC Database (Admin)</i> . See below for details.

PC Database (Admin)

This screen is displayed if the "Advanced Administration" button on the ***PC Database*** is clicked. It provides more control than the standard ***PC Database*** screen.

Advanced

Advanced Internet	Access control	Remote management	Virtual servers	Dynamic DNS	Upgrade Firmware	Config File
PC Database	Network diag	Options	Security	Logs	MAC Address	Routing

Any PC may be added, edited or deleted. If adding a PC which is not connected and On, you must provide the MAC (hardware) address

Known PCs

jessica 192.168.0.2 (LAN) 0010b5bb8009(DHCP)

PC Properties

Name:

IP Address: Automatic (DHCP Client)
 DHCP Client - reserved IP address: ...
 Fixed IP address (set on PC): ...

MAC Address: Automatic discovery (PC must be available on LAN)
 MAC address is

Data - PC Database (Admin) Screen

Known PCs	This lists all current entries. Data displayed is <i>name (IP Address) type</i> . The "type" indicates whether the PC is connected to the LAN.
PC Properties	
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC's "hostname".
IP Address	<p>Select the appropriate option:</p> <ul style="list-style-type: none"> Automatic - The PC is set to be a DHCP client (Windows: "Obtain an IP address automatically"). The DC-202 will allocate an IP address to this PC when requested to do so. The IP address could change, but normally won't. DCHP Client - Reserved IP Address - Select this if the PC is set to be a DCHP client, and you wish to guarantee that the DC-202 will always allocate the same IP Address to this PC. Enter the required IP address. Only the last field is required; the other fields must match the DC-202's IP address. Fixed IP Address - Select this if the PC is using a Fixed (Static) IP address. Enter the IP address allocated to the PC. (The PC must be configured to use this IP address.)

MAC Address	Select the appropriate option <ul style="list-style-type: none">• Automatic discovery - Select this to have the DC-202 contact the PC and find its MAC address. This is only possible if the PC is connected to the LAN and powered On.• MAC is - Enter the MAC address on the PC. The MAC address is also called the "Hardware Address", "Physical Address", or "Network Adapter Address". The DC-202 uses this to provide a unique identifier for each PC. Because of this, the MAC address can NOT be left blank.
Buttons	
Add as New Entry	Add a new PC to the list, using the data in the "Properties" box. If "Automatic discovery" (for MAC address) is selected, the PC will be sent a "ping" to determine its hardware address. This will fail unless the PC is connected to the LAN, and powered on.
Update Selected PC	Update (modify) the selected PC, using the data in the "Properties" box.
Clear Form	Clear the "Properties" box, ready for entering data for a new PC.
Refresh	Update the data on screen.
Generate Report	Display a read-only list showing full details of all entries in the PC database.
Standard Screen	Click this to view the standard <i>PC Database</i> screen.

Network Diagnostics

This screen allows you to perform a "Ping" or a DNS lookup. These activities can be useful in solving network problems. An example **Network Diagnostics** screen is shown below.

Advanced

Advanced Internet	Access control	Remote management	Virtual servers	Dynamic DNS	Upgrade Firmware	Config File
PC Database	Network diag	Options	Security	Logs	MAC Address	Routing

Ping Ping this IP Address: . . .

Ping Results

DNS Lookup Domain name/URL:

DNS Lookup Results

Data - Network Diagnostics Screen

Ping	
Ping this IP Address	Enter the IP address you wish to ping. The IP address can be on your LAN, or on the Internet. Note that if the address is on the Internet, and no connection currently exists, you could get a "Timeout" error. In that case, wait a few seconds and try again.
Ping Button	After entering the IP address, click this button to start the "Ping" procedure. The results will be displayed in the <i>Ping Results</i> pane.
DNS Lookup	
Domain name/URL	Enter the Domain name or URL for which you want a DNS (Domain Name Server) lookup. Note that if the address is on the Internet, and no connection currently exists, you could get a "Timeout" error. In that case, wait a few seconds and try again.
Lookup Button	After entering the Domain name/URL, click this button to start the "DNS Lookup" procedure.

Options

This screen allows advanced users to enter or change a number of settings. For normal operation, there is no need to use this screen or change any settings.

An example *Options* screen is shown below.

Advanced						
Advanced Internet	Access control	Remote management	Virtual servers	Dynamic DNS	Upgrade Firmware	Config File
PC Database	Network diag	Options	Security	Logs	MAC Address	Routing

Backup DNS	Backup DNS (1) IP Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
	Backup DNS (2) IP Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
	These DNS (Domain Name Servers) are used only if the primary DNS is unavailable.	
TFTP	<input type="checkbox"/> Enable Firmware Upgrade using TFTP	
UPnP	<input type="checkbox"/> Enable UPnP Services	
	<input checked="" type="checkbox"/> Allow configuration changes through UPnP	
	<input type="checkbox"/> Allow Internet access to be disabled	
MTU	MTU (Maximum Transmission Unit): <input type="text" value="1500"/> (1..1500) bytes	
	This setting only affects PPPoE and PPTP connections.	

Data - Options Screen

Backup DNS	
IP Address	Enter the IP Address of the DNS (Domain Name Servers) here. These DNS will be used only if the primary DNS is unavailable.
TFTP	
Enable Firmware Upgrade using TFTP	<ul style="list-style-type: none"> If enabled, TFTP (Trivial FTP) can be used to upgrade the firmware in this device. This is normally not required; a Windows utility is available for this purpose. You must obtain the firmware upgrade file first; instructions for using TFTP will be available with the upgrade.
UpnP	
Enable UPnP Services	<ul style="list-style-type: none"> UPnP (Universal Plug and Play) allows automatic discovery and configuration of equipment attached to your LAN. UPnP is by supported by Windows ME, XP, or later. If Enabled, this device will be visible via UPnP. If Disabled, this device will not be visible via UPnP.
Allow Configuration...	<ul style="list-style-type: none"> If checked, then UPnP users can change the configuration. If Disabled, UPnP users can only view the configuration. But currently, this restriction only applies to users running Windows XP, who access the <i>Properties</i> via UPnP. (e.g. Right - click the DC-202 in <i>My Network Places</i>, and select <i>Properties</i>)
Allow Internet access to be disabled	<ul style="list-style-type: none"> If checked, then UPnP users can disable Internet access via this device. If Disabled, UPnP users can NOT disable Internet access via this device. But currently, this restriction only applies to users running Windows XP, who access the <i>Properties</i> via UPnP. (e.g. Right - click the DC-202 in <i>My Network Places</i>, and select <i>Properties</i>)
MTU	
MTU size	<p>MTU (Maximum Transmission Unit) value should only be changed if advised to do so by Technical Support.</p> <ul style="list-style-type: none"> Enter a value between 1 and 1500. This device will still auto-negotiate with the remote server, to set the MTU size. The smaller of the 2 values (auto-negotiated, or entered here) will be used. For direct connections (not PPPoE or PPTP), the MTU used is always 1500.

Security

This screen allows you to set Firewall and other security-related options.

Advanced						
Advanced Internet	Access control	Remote management	Virtual servers	Dynamic DNS	Upgrade Firmware	Config File
PC Database	Network diag	Options	Security	Logs	MAC Address	Routing
<p>Firewall <input checked="" type="checkbox"/> Enable DoS (Denial of Service) Firewall Threshold: <input checked="" type="radio"/> High (WAN bandwidth > 2 Mbps) <input type="radio"/> Medium (WAN bandwidth 1 - 2 Mbps) <input type="radio"/> Low (WAN bandwidth < 1 Mbps)</p> <p>If Enabled (recommended), invalid packets and connections are dropped. The "Threshold" affects invalid connections only.</p> <p>Options <input type="checkbox"/> Respond to ICMP (ping) on WAN interface <input checked="" type="checkbox"/> Allow IPsec <input checked="" type="checkbox"/> Allow PPTP <input checked="" type="checkbox"/> Allow L2TP</p>						
				Save	Cancel	Help

Data - Security Screen

Firewall	
Enable DoS Firewall	<p>If enabled, DoS (Denial of Service) attacks will be detected and blocked. The default is enabled. It is strongly recommended that this setting be left enabled.</p> <p>Note:</p> <ul style="list-style-type: none"> A DoS attack does not attempt to steal data or damage your PCs, but overloads your Internet connection so you can not use it - the service is unavailable. This device uses "Stateful Inspection" technology. This system can detect situations where individual TCP/IP packets are valid, but collectively they become a DoS attack.
Threshold	<p>This setting affects the number of "half-open" connections allowed.</p> <ul style="list-style-type: none"> A "half-open" connection arises when a remote client contacts the Server with a connection request, but then does not reply to the Server's response. While the optimum number of "half-open" connections allowed (the "Threshold") depends on many factors, the most important factor is the available bandwidth of your Internet connection. Select the setting to match the bandwidth of your Internet connection.

Options	
Respond to ICMP	<p>The ICMP protocol is used by the "ping" and "traceroute" programs, and by network monitoring and diagnostic programs.</p> <ul style="list-style-type: none">• If checked, the DC-202 will respond to ICMP packets received from the Internet.• If not checked, ICMP packets from the Internet will be ignored. Disabling this option provides a slight increase in security.
Allow IPsec	<p>The IPsec protocol is used to establish a secure connection, and is widely used by VPN (Virtual Private Networking) programs.</p> <ul style="list-style-type: none">• If checked, IPsec connections are allowed.• If not checked, IPsec connections are blocked.
Allow PPTP	<p>PPTP (Point to Point Tunneling Protocol) is widely used by VPN (Virtual Private Networking) programs.</p> <ul style="list-style-type: none">• If checked, PPTP connections are allowed.• If not checked, PPTP connections are blocked.
Allow L2TP	<p>L2TP is a protocol developed by Cisco for VPNs (Virtual Private Networks).</p> <ul style="list-style-type: none">• If checked, L2TP connections are allowed.• If not checked, L2TP connections are blocked.

Logs

The Logs record various types of activity on the DC-202. This data is useful for troubleshooting, but enabling all logs will generate a large amount of data and adversely affect performance.

Since only a limited amount of log data can be stored in the DC-202, log data can also be E-mailed to your PC.

Advanced

Advanced Internet	Access control	Remote management	Virtual servers	Dynamic DNS	Upgrade Firmware	Config File
PC Database	Network diag	Options	Security	Logs	MAC Address	Routing

Enable Logs

Outgoing (Internet) connections View Log

Access Control View Log

DoS (Denial or Service) attacks View Log

Timezone:

E-Mail Reports

Send E-mail alert immediately when attacked

E-mail Logs: Connection Log
 Access Control Log

Send: When log is full
 Every Sunday at AM

E-Mail Address

E-mail address:

Subject:

SMTP Server: Address:
 IP address:

Port No. (Default: 25)

Data - Logs Screen

Enable Logs	
Outgoing Connections	If selected, Outgoing Internet connections are logged. Normally, the (Internet) "Destination" will be shown as an IP address. But if the "URL Filter" is enabled, the "Destination" will be shown as a URL.
Access Control	If enabled, the log will include attempted outgoing connections which have been blocked by the "Access Control" feature.
DoS Attacks	If enabled, this log will show details of DoS (Denial of Service) attacks which have been blocked by the built-in Firewall.
Timezone	Select the correct Timezone for your location. This is required for the date/time shown on the logs to be correct.

E-Mail Reports	
Send E-mail alert	If enabled, an E-mail will be sent immediately if a DoS (Denial of Service) attack is detected. If enabled, the E-mail address information must be provided.
E-mail Logs	You can choose to have the logs E-mailed to you, by enabling either or both checkboxes. If enabled, the Log will be sent to the specified E-mail address. The interval between E-mails is determined by the "Send" setting.
Send	<p>Select the desired option for sending the log by E-mail.</p> <ul style="list-style-type: none"> • When log is full - The time is not fixed. The log will be sent when the log is full, which will depend on the volume of traffic. • Every day, Every Monday ... - The log is sent on the interval specified. • If "Every day" is selected, the log is sent at the time specified. • If the day is specified, the log is sent once per week, on the specified day. • Select the time of day you wish the E-mail to be sent. • If the log is full before the time specified to send it, it will be sent regardless.
E-Mail Address	
E-mail Address	Enter the E-mail address the Log is to be sent to. The E-mail will also show this address as the Sender's address.
Subject	Enter the text string to be shown in the "Subject" field for the E-mail.
SMTP Server	Enter the address or IP address of the SMTP (Simple Mail Transport Protocol) Server you use for outgoing E-mail.
Port No.	Enter the port number used to connect to the SMTP Server. The default value is 25.

MAC Address

The MAC (hardware) address is a low-level network identifier. It may be called "MAC Address", "Hardware Address", or "Physical Address". On a PC, this address is associated with the Network card or adapter. The address on the *MAC Address* screen is the address on the Internet (WAN port) interface, and has no effect on the LAN interface.

- If your ISP asks for the *Network Adapter Address*, *Physical Address*, *Hardware Address*, or *MAC Address* for the PC the DSL/Cable modem is connected to, provide this value.
- If your ISP has already recorded a MAC Address, you can change the address used by the DC-202 to match the address recorded by your ISP.

MAC Address Screen

Select *MAC Address* from the *Advanced* menu to reach a screen like the example below.

Advanced						
Advanced Internet	Access control	Remote management	Virtual servers	Dynamic DNS	Upgrade Firmware	Config File
PC Database	Network diag	Options	Security	Logs	MAC Address	Routing
<p>MAC Address This set the MAC address (also called hardware or physical address) used on the WAN port (Internet interface). It is only necessary to change this if your ISP expects you to use a particular MAC address.</p> <p>MAC Address: <input type="text" value="00c00201857a"/> <input type="button" value="Default"/> <input type="button" value="Copy from PC"/></p> <p><input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/></p>						

Data - MAC Address Screen

MACAddress	The current MAC (hardware) address is displayed. If your ISP has recorded a Hardware Address, you can "spoof" that address by entering it in the address field. The hardware address consists of 12 characters, where each character is a digit (0..9) or a character between A and F.
Buttons	
Default	Inserts the default MAC address into the MAC address field. You must click "Save" to actually change the address used.
Copy from PC	Inserts the MAC address from your PC into the MAC address field. You must click "Save" to actually change the address used.
Save	Save your changes to the DC-202.
Cancel	Reverse any changes made since the last "Save".



If the MAC address is changed, the DC-202 must restart.

Routing

Overview

- If you don't have other Routers or Gateways on your LAN, you can ignore the "Routing" page completely.
- If the DC-202 is only acting as a Gateway for the local LAN segment, ignore the "Routing" page even if your LAN has other Routers.
- If your LAN has a standard Router (e.g. Cisco) on your LAN, and the DC-202 is to act as a Gateway for all LAN segments, enable RIP (Routing Information Protocol) and ignore the Static Routing table.
- If your LAN has other Gateways and Routers, and you wish to control which LAN segments use each Gateway, do NOT enable RIP (Routing Information Protocol). Configure the Static Routing table instead. (You also need to configure the other Routers.)
- If using Windows 2000 Data center Server as a software Router, enable RIP on the DC-202, and ensure the following Windows 2000 settings are correct:
 - Open *Routing and Remote Access*
 - In the console tree, select *Routing and Remote Access*, [server name], *IP Routing*, *RIP*
 - In the "Details" pane, right-click the interface you want to configure for RIP version 2, and then click "Properties".
 - On the "General" tab, set *Outgoing packet protocol* to "RIP version 2 broadcast", and *Incoming packet protocol* to "RIP version 1 and 2".

Routing Screen

The routing table is accessed by the *Routing* link on the *Administration* menu.

Using this Screen

Generally, you will use either RIP (Routing Information Protocol) OR the Static Routing Table, as explained above, although it is possible to use both methods simultaneously.

Static Routing Table

- If RIP is not used, 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 other Routers must also be configured. See *Configuring Other Routers on your LAN* later in this chapter for further details and an example.

Advanced						
Advanced Internet	Access control	Remote management	Virtual servers	Dynamic DNS	Upgrade Firmware	Config File
PC Database	Network diag	Options	Security	Logs	MAC Address	Routing
<p>RIP <input type="checkbox"/> Enable RIP (Routing Information Protocol) V1 Save</p>						
Static Routing		Static Routing Table Entries				
		<div style="border: 1px solid black; height: 40px; width: 100%;"></div>				
		Properties				
		Destination Network: <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> Network Mask: <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> Gateway IP Address: <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> Metric: <input type="text"/> <div style="text-align: right; margin-top: 5px;">Clear Form</div>				
		Add Update Delete				
					Generate Report Help	

Data - Routing Screen

RIP	
Enable RIP	<p>Check this to enable the RIP (Routing Information Protocol) feature of the DC-202.</p> <p>The DC-202 supports RIP 1 only.</p>
Static Routing	
Static Routing Table Entries	<p>This list shows all entries in the Routing Table.</p> <ul style="list-style-type: none"> The "Properties" area shows details of the selected item in the list. Change any the properties as required, then click the "Update" button to save the changes to the selected entry.
Properties	<ul style="list-style-type: none"> Destination Network - The network address of the remote LAN segment. For standard class "C" LANs, the network address is the first 3 fields of the Destination IP Address. The 4th (last) field can be left at 0. Network Mask - The Network Mask for the remote LAN segment. For class "C" networks, the default mask is 255.255.255.0 Gateway IP Address - The IP Address of the Gateway or Router which the DC-202 must use to communicate with the destination above. (NOT the router attached to the remote segment.) Metric - The number of "hops" (routers) to pass through to reach the remote LAN segment. The shortest path will be used. The default value is 1.

Buttons	
Save	Save the RIP setting. This has no effect on the Static Routing Table.
Add	Add a new entry to the Static Routing table, using the data shown in the "Properties" area on screen. The entry selected in the list is ignored, and has no effect.
Update	Update the current Static Routing Table entry, using the data shown in the "Properties" area on screen.
Delete	Delete the current Static Routing Table entry.
Clear Form	Clear all data from the "Properties" area, ready for input of a new entry for the Static Routing table.
Generate Report	Generate a read-only list of all entries in the Static Routing table.

Configuring Other Routers on your LAN

It is essential that all IP packets for devices not on the local LAN be passed to the DC-202, 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 DC-202 as the *Default Route* or *Default Gateway*.

Local Router

The local router is the Router installed on the same LAN segment as the DC-202. This router requires that the *Default Route* is the DC-202 itself. Typically, routers have a special entry for the *Default Route*. It should be configured as follows.

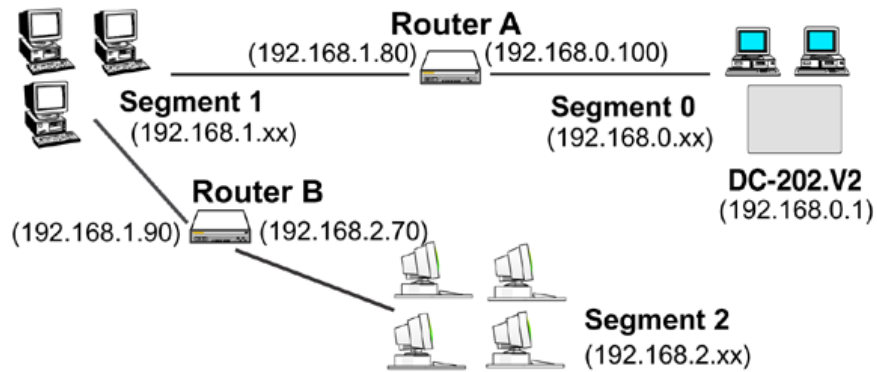
Destination IP Address	Normally 0.0.0.0, but check your router documentation.
Network Mask	Normally 0.0.0.0, but check your router documentation.
Gateway IP Address	The IP Address of the DC-202.
Metric	1

Other Routers on the Local LAN

Other routers on the local LAN must use the DC-202's *Local Router* as the *Default Route*. The entries will be the same as the DC-202's local router, with the exception of the *Gateway IP Address*.

- For a router with a direct connection to the DC-202's local Router, the *Gateway IP Address* is the address of the DC-202's local router.
- For routers which must forward packets to another router before reaching the DC-202's local router, the *Gateway IP Address* is the address of the intermediate router.

Static Routing - Example



For the DC-202's Routing Table

For the LAN shown above, with 2 routers and 3 LAN segments, the DC-202 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 (DC-202's local Router)
Metric	2
Entry 2 (Segment 2)	
Destination IP Address	192.168.2.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100
Metric	3

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 (DC-202'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 (DC-202's local router)

Appendix A

Troubleshooting

Overview

This chapter covers some common problems that may be encountered while using the DC-202 and some possible solutions to them. If you follow the suggested steps and the DC-202 still does not function properly, contact your dealer for further advice.

General Problems

Problem 1: Can't connect to the DC-202 to configure it.

Solution 1: Check the following:

- The DC-202 is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the DC-202 are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.0.2 to 192.168.0.254 and thus compatible with the DC-202's default IP Address of 192.168.0.1.
Also, the Network Mask should be set to 255.255.255.0 to match the DC-202.
In Windows, you can check these settings by using *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

Internet Access

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

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

- Check if other PCs work. If they do, ensure that your PCs IP settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address.
- If the PCs are configured correctly, but still not working, check the DC-202. 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 DC-202 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 DC-202.**

Solution 2: The DC-202 processes the data passing through it, so it is not transparent.

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

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

- It is a security risk, since the firewall is disabled.
- Only one (1) PC can use this feature.

Appendix B

Specifications

Multi-Function DC-202 Broadband Router

Model	DC-202
Dimensions	140mm(W) * 99mm(D) * 27mm(H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol:	TCP/IP
Network Interface:	5 Ethernet: 4 * 10/100BaseT (RJ45) LAN connection 1 * 10/100BaseT (RJ45) for WAN
LEDs	11
Power Adapter	9 V DC External

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the

user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) This device must accept any interference received, including interference that may cause undesired operation.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

CE Marking Warning

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