



DCM-604
Cable Modem EMTA Gateway
PacketCable 1.5 and DOCSIS 2.0 Certified
4 Ports Ethernet Cable Router with 2 Ports Voice
User's Manual

Version 0.9



FCC Statement

This device complies with Class B Part 15 of the FCC Rules. The device generates, uses and can radiate radio frequency energy and, if not installed and used as instructed, may cause harmful interference to radio communication. Only Coaxial cables are to be used with this device in order to ensure compliance with FCC emissions limits. Accessories connected to this device by the user must comply with FCC Class B limits. The manufacturer is not responsible for any interference which results from use of improper cables, or which results from unauthorized changes or modifications to the device.

"A Minimum 26 AWG Line Core should be used for connection to the cable modem"

Trademarks

All trademarks are the property of their respective owners.

Table of Contents

1. INTRODUCTION	1
1.1 SYSTEM REQUIREMENTS.....	1
1.2 UNPACKING AND INSPECTION.....	1
1.3 SAFETY PRECAUTIONS.....	1
2. HARDWARE OVERVIEW	2
2.1 FRONT PANEL AND LEDs.....	2
3. ETHERNET INSTALLATION	4
4. USB DRIVER INSTALLATION	5
4.1 WINDOWS XP.....	5
4.2 WINDOWS 2003.....	7
4.3 WINDOWS VISTA.....	9
5. WEB MANAGEMENT	11
5.1 ENTER MODEM'S IP ADDRESS.....	11
5.2 STATUS.....	12
5.2.1 <i>Software Status</i>	12
5.2.2 <i>Security</i>	12
5.3 BASIC.....	13
5.3.1 <i>Setup</i>	13
5.3.2 <i>DHCP</i>	13
5.3.3 <i>Backup</i>	14
5.4 ADVANCED.....	14
5.4.1 <i>Options</i>	15
5.4.2 <i>IP Filtering</i>	16
5.4.3 <i>Port Filtering</i>	16
5.4.4 <i>Forwarding</i>	17
5.4.5 <i>Port Triggers</i>	17
5.4.6 <i>DMZ Host</i>	18
5.5 FIREWALL.....	19
5.5.1 <i>Web Filter</i>	19
5.5.2 <i>Local Log</i>	19
5.5.3 <i>Remote Log</i>	20
5.6 PARENTAL CONTROL.....	21
5.7 WIRELESS.....	1
5.7.1 <i>Radio</i>	1
5.7.2 <i>Primary Network</i>	2
5.7.3 <i>Advanced</i>	2
5.7.4 <i>Access Control</i>	3
5.7.5 <i>WMM</i>	4
5.8 MTA.....	5
5.8.1 <i>Status</i>	5
5.9 HARD RESET.....	6

1. Introduction

The DCM-604 is a Voice over IP Wireless Residential Gateway integrated with Cable Modem which allows you implement your VoIP phone call directly through Cable Modem Broadband Network service with its built-in PacketCable 1.5 and DOCSIS/EURODOCSIS 2.0 compliant specification.

And with the integration of 4 ports switch and IEEE 802.11g wireless functionality, the DCM-604 series could also be used as a Wireless Cable Modem Residential Gateway in your home or small office. The ability to route data information into your broadband network could help you easily extend your local network via wire or wireless.

1.1 System Requirements

- IBM Compatible, Macintosh or other workstation supports TCP/IP protocol.
- An Ethernet port supports 10Base-T/100Base-TX Ethernet connection or USB-equipped PC.
- Subscribed to a Cable Television company for Cable Modem services.

1.2 Unpacking and Inspection

Included in the kit is the following:

- 1 x EMTA DCM-604
- 1 x RJ-45 CAT 5 Cable
- 1 x 15V/1.0A Power Supply Adaptor
- 1 x CD-ROM containing USB Driver
- 1 x 6P4C Telephone Cord
- 1 x USB Cable

If any of above items lost or damaged, please contact your retailer or ISP for assistance.

1.3 Safety Precautions














For your protection, observe the following safety precautions when setting up and using your equipment. Failure to observe these precautions can result in serious personal injury and damage to your equipment.


- Make sure the voltages and frequency of the power outlet matches the electrical rating labels on the AC Adapter.
- Do not place any object on top of the device or force it into a confined space.
- Never push objects of any kind through openings in the casing. Dangerous voltages may be present. Conductive foreign objects could produce a short circuit that could cause fire, electrical shock, or damage to the equipment.
- Whenever there is danger of lightning, disconnect the power cable and the Hybrid-Fiber Coax cable from the cable modem to prevent damage to the unit. The use of an AC protection device will not completely protect the cable modem product from damage caused from the transmission across the Hybrid-Fiber Coax network.

2. Hardware Overview

2.1 Front Panel and LEDs

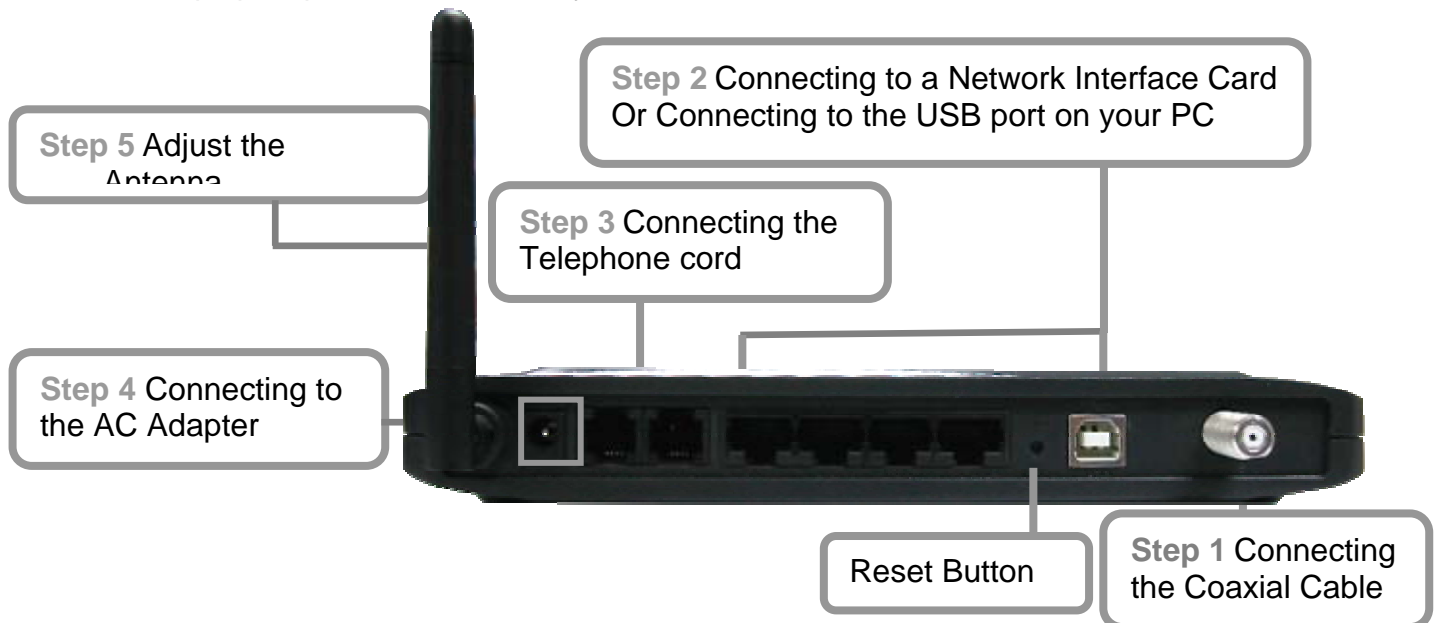
There are fourteen Light-Emitting-Diodes (LEDs) located on the front panel top provide status information to the user.

LED	NAME	COLOR	MODE	STATUS
	Power	Green	On	Connected with power
			Off	Power failure or disconnect
	Cable	Green	Blinking	TFTP/DHCP in process
			On	AIO Registered
	Tx	Green	On	Upstream channel acquired
			Blinking	Acquiring upstreaming channel
	Rx	Green	On	Downstream channel acquired
			Blinking	Acquiring downstream channel
	LAN 1	Green	Blinking	Transferring Data
			On	Ethernet port 1 linked
			Off	Disconnected
	LAN 2	Green	Blinking	Transferring Data
			On	Ethernet port 2 linked
			Off	Disconnected
	LAN 3	Green	Blinking	Transferring Data
			On	Ethernet port 3 linked
			Off	Disconnected
	LAN 4	Green	Blinking	Transferring Data
			On	Ethernet port 4 linked
			Off	Disconnected
	USB	Green	Blinking	USB activity
			On	USB linked
	Voice Message	Green	Blinking	Off hook
			On	VoIP linked
	TEL1	Green	Blinking	in calling
			On	Line 1 is registered in the network
			Off	Line 1 is not registered in the network
	TEL2	Green	Blinking	in calling
			On	Line 2 is registered in the network
			Off	Line 2 is not registered in the network
	Wifi	Green	Blinking	Transferring Data
			On	WIFI Ready

	WPS	Blue	Blinking	WPS Activating
			On	WPS Connected
			Off	No WPS Connection

2.2 Rear Panel and Hardware Connection

This chapter describes the proper steps for connecting your cable modem. Please be sure to follow the steps in the sequence outlined below. Failure to do so could result in improper operation or failure of your cable modem.



Step 1: Connect a cable by feeding the F-connector on the back of the cable modem. Ensure the center conductor of the 75 ohm coaxial cable is inserted directly into the center of the F-connector. Secure the coaxial cable by carefully threading the outer shell of the coaxial cable connector onto the F-connector in a clockwise direction until tight. Be careful not to over-tighten the connector or you may damage either the connector or the cable modem.

Step 2: Connect the cable modem to an IEEE 802.3 10BaseT / 802.3u 100Base-TX Network using a RJ-45 male-terminated Ethernet cable or an USB cable to the PC. This cable modem equips with two Ethernet ports, you can connect two PCs to the cable modem at the same time if necessary.

Step 3: Connect the telephone sets to TEL1 and TEL2. Use RJ-11 telephone line to connect TEL1/TEL2 port on the cable modem and telephone socket on telephone.

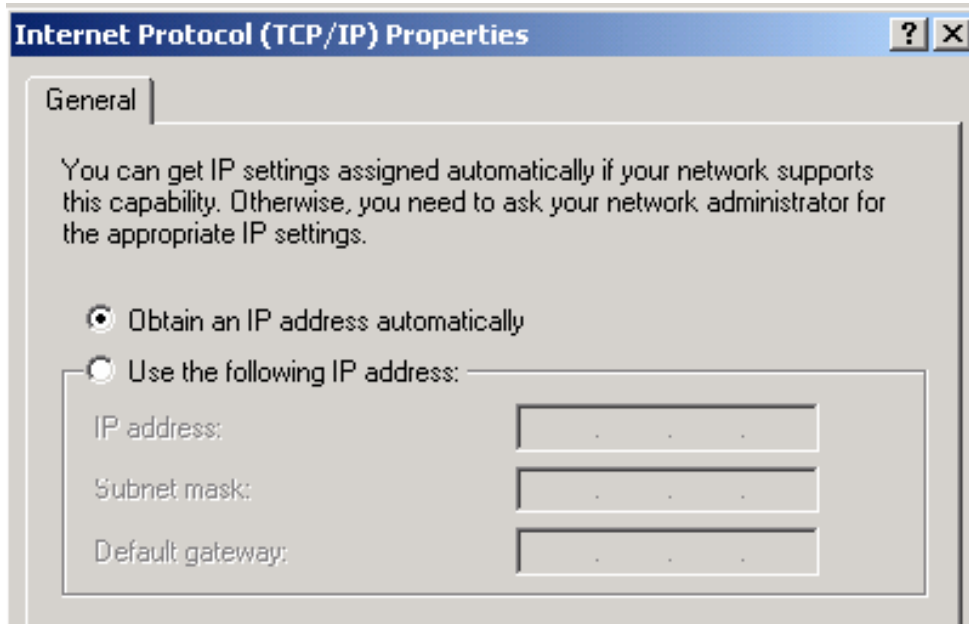
Step 4: Connect the AC Adapter to the cable modem by inserting the barrel-shaped connector into the mating power connector on the back of the cable modem. Exercise carefully to ensure the connectors are properly aligned prior to insertion and ensure the two connectors engage completely. The cable modem is shipped with an AC adapter. Remember to use only power adapter that came with the cable modem. Other power adapters might have voltages that are not correct for your particular cable modem. Using a power adapter with the wrong voltage can damage the cable modem.

Step 5: Adjust the antenna if necessary.

3. Ethernet Installation

The LAN port you are using is auto-negotiating 10/100Mbps (Switch) Ethernet Interface. You can use the Ethernet port to connect to the Internet with an Ethernet network device such as NIC/Hub/Switch through RJ45.

Before you connect to and install the cable modem, please set the IP address to "Obtain an IP address automatically" as below and do ensure the TCP/IP protocol is installed on your system and configured correctly in your PC.



Following is an example of configuring the TCP/IP Protocol on Windows 98 Operating Systems:

1. Click **Start**→**Settings**→**Control Panel**. Double click on the **Network** icon click **Properties**.
2. A list of installed network components appears. Look for an entry named TCP/IP. This entry may be followed by an arrow and a description of the NIC hardware device installed in the computer. If you don't see "TCP/IP" listed anywhere in the "The following network components are installed" box, click the **Add** button, choose **Protocol**, and click the **Add** button. Select "Microsoft" as the manufacturer and then scroll down in the list on the right to find "TCP/IP". If you see "TCP/IP" listed, proceed to step 4.
3. Click the **OK** button. You will be prompted to insert the Windows 98 installation/upgrade CD.
4. Scroll down in the box until you find a line that says "TCP/IP -> " followed by the name of your Ethernet adapter. Click on **Properties** and choose "Obtain an address automatically" which means that your PC has been configured to use DHCP (Dynamic Host Configuration Protocol).
5. Click **OK**.

Congratulations! You have successfully set up your cable modem.

4. USB Driver Installation

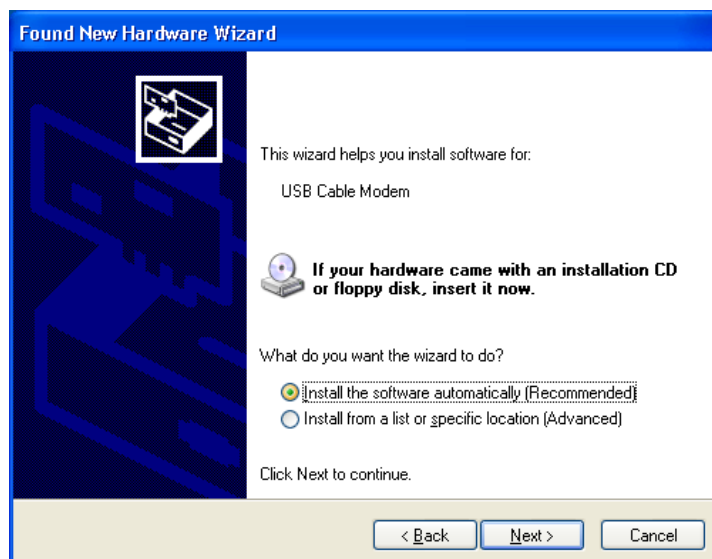
Using the USB port to connect to the Internet allows you to install the cable modem more quickly and easily than connecting to the Internet using the Ethernet port, since you do not need to install a network interface card (NIC).

4.1 Windows XP

1. Connect USB cable from PC to cable modem.
2. Connect RF cable and power on Cable Modem. Wait until it register, it will take about 40 seconds to 4 minutes depends on network traffic. Cable Modem may reboot if you previously connect it through Ethernet port.
3. Windows will prompt new hardware found, insert the Driver CD into your CD-ROM drive.
4. You may see this window if you had update your Windows XP to Service Pack 2. Select "Yes, this time only" and then click **Next**.



5. Select "Install the software automatically (Recommended)" and then click **Next**.



- Windows will locate the driver automatically. Please click **Continue Anyway** to continue the installation process.



- Windows shall find the location of USB driver and complete the installation. Click **Finish**.

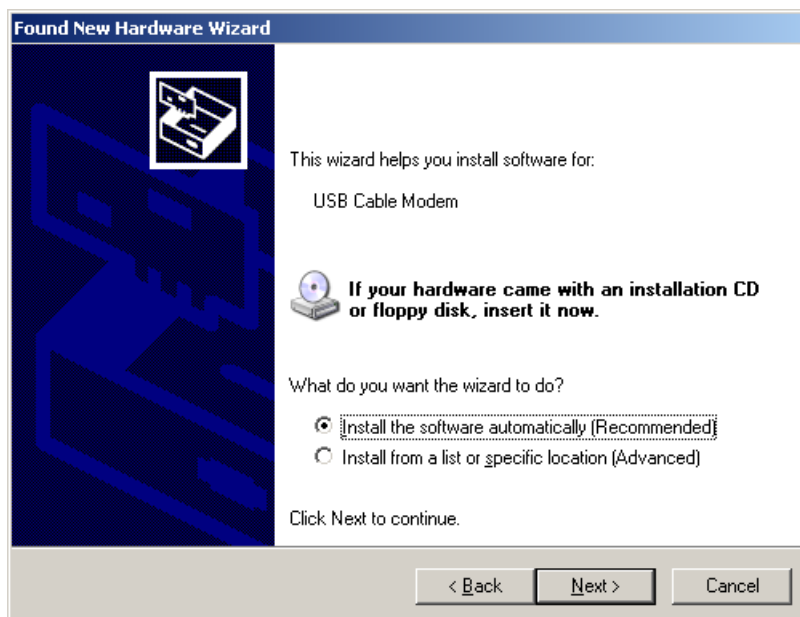


4.2 Windows 2003

1. Connect USB cable from PC to cable modem.
2. Connect RF cable and power on Cable Modem. Wait until it register, it will take about 40 seconds to 4 minutes depends on network traffic. Cable Modem may reboot if you previously connect it through Ethernet port.
3. Windows will prompt new hardware found, insert the Driver CD into your CD-ROM drive.
4. Select "Yes, this time only" and then click **Next**.



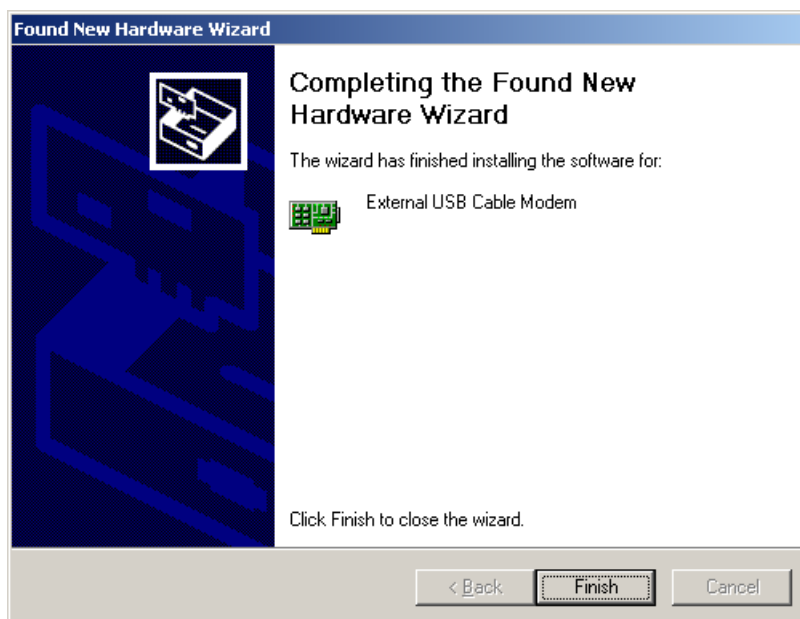
5. Select "Install the software automatically (Recommended)" and then click **Next**.



- Windows will locate the driver automatically. Please click **Continue Anyway** to continue the installation process.



- Windows shall find the location of USB driver and complete the installation. Click **Finish**.



4.3 Windows Vista

1. Connect USB cable from PC to cable modem.
2. Connect RF cable and power on Cable Modem. Wait until it register, it will take about 40 seconds to 4 minutes depends on network traffic. Cable Modem may reboot if you previously connect it through Ethernet port.
3. Windows will prompt new hardware found, insert the Driver CD into your CD-ROM drive.
4. Click "Locate and install driver software (recommended)" item



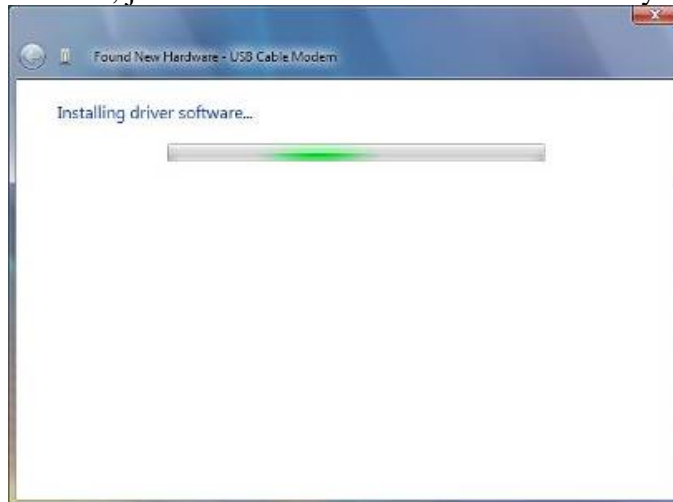
5. Insert the Driver disk that came with your cable modem into your CD-ROM drive. Windows Vista will automatically searched and found this driver.



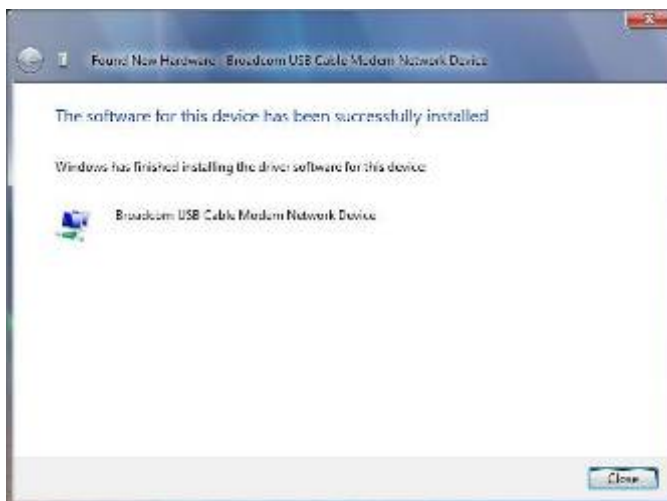
6. During the driver installation, your system may pop-up a dialogue as below window, just click "Install this driver software anyway".



7. During the driver installation, your system may pop-up a dialogue as below window, just click "Install this driver software anyway".



8. Click "Close" button to finish the driver installation.



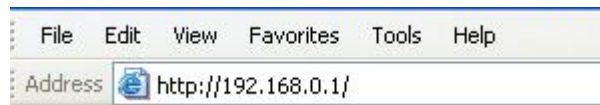
5. Web Management

For easy-changing the default setting or quick-checking diagnostics for troubleshooting, a Web-based GUI is built-in for your access.

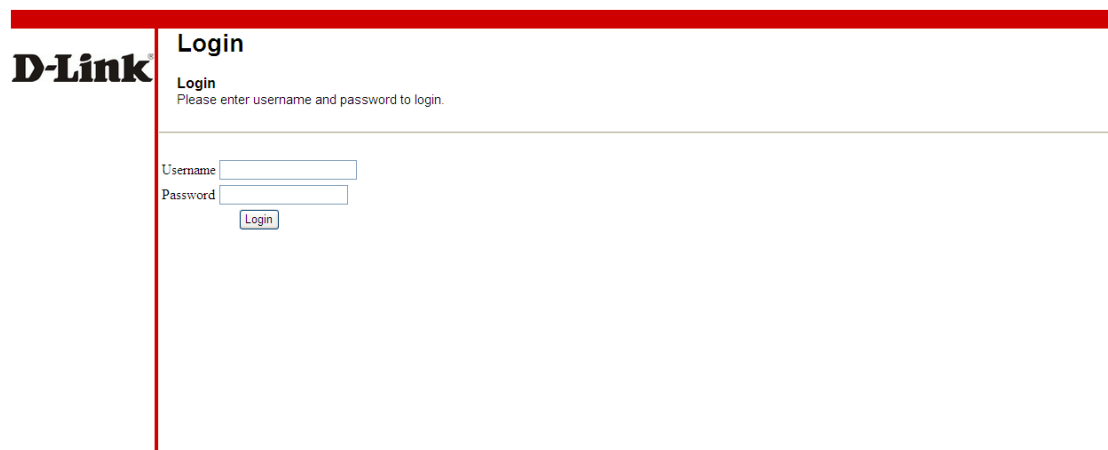
5.1 Enter Modem's IP address

Use the following procedures to login to your DCM-604.

1. Open your web browser.
You may get an error message. This is normal. Continue on to the next step.
2. Type the default IP address of the DCM-604 (e.g. **192.168.0.1**) and press Enter.

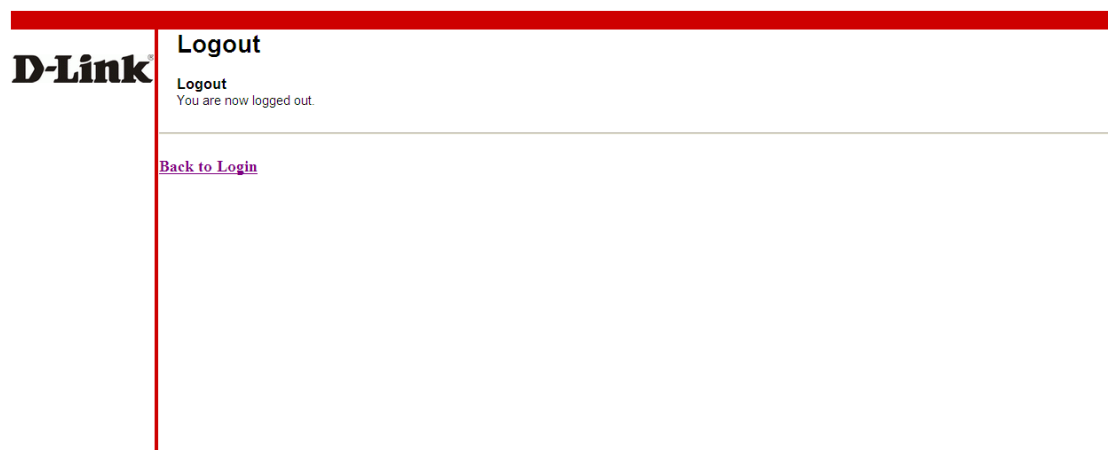


3. The Log In page appears. Type the user name (**admin**) and your password (**password**) in the respective fields.

A screenshot of the D-Link web management interface. The page has a red header bar. On the left side, there is a vertical red bar with the "D-Link" logo. The main content area is titled "Login". Below the title, there is a sub-heading "Login" and a message: "Please enter username and password to login." There are two input fields: "Username" and "Password". Below the "Password" field is a "Login" button. The page is framed by red horizontal bars at the top and bottom.

©2008 D-LINK. All rights reserved.

4. Click the Logout button to leave the application.

A screenshot of the D-Link web management interface. The page has a red header bar. On the left side, there is a vertical red bar with the "D-Link" logo. The main content area is titled "Logout". Below the title, there is a sub-heading "Logout" and a message: "You are now logged out." Below the message is a link labeled "Back to Login". The page is framed by red horizontal bars at the top and bottom.

©2008 D-LINK. All rights reserved.

There are seven categories in this web management including Status, Basic, Advanced and Firewall. The following sections describe their details.

5.2 Status

The Status page shows hardware and software information about the DCM-604 that may be useful to your cable service provider.

5.2.1 Software Status

The Software page shows how long the DCM-604 has operated since last being powered up, and some key information the DCM-604 received during the initialization process with your cable service provider.

(Pls change the screen capture. Pls use f/w 4k)

Status

Software
This page displays information on the current system software.

Information	
Standard Specification Compliant	DOCSIS 2.0
Hardware Version	1.2
Bootloader Version	2.1.71
Software Version	107.704w.4422.629.003b
Cable Modem MAC Address	00:30:54:d5:a5:18
Cable Modem Serial Number	W1N81A00038
CM certificate	Installed

Status

System Up Time 0 days 00h 52m 58s
Network Access Denied

©2008 D-LINK. All rights reserved.

5.2.2 Security

This page allows the configuration of administration access privileges and the ability to restore the settings to factory defaults to the system and allows switching to router or bridge mode. If DCM-604 mode set as bridge, the "basic", "advance" and "firewall" tabs of webpage will be disabled. The DCM-604 home page will change to 192.168.100.1. And to access home page, need to set up connected device (PC) IP address as 192.168.100.xx. After changing the settings, click Apply, then the modem will reboot to take effect setting. And wait for DCM-604 boot up completes.

Security
This page allows configuration of administration access privileges and the ability to restore factory defaults to the system and switch router and bridge mode. If DCM-604 set as bridge, the "basic", "advance" and "firewall" tab of webpage will be disable. The DCM-604 home page will change to 192.168.100.1. To access home page, your computer have to set up IP address as 192.168.100.x. After changing the function, the modem will reboot to take effect setting. Please wait for DCM-604 boot up completed.

Soft Reboot Modem

Password Change User ID

New Password

Re-Enter New Password

Current User ID Password

Mode Bridge Router

Restore Factory Defaults Yes No

©2008 D-LINK. All rights reserved.

5.3 Basic

The Basic page contains the basic features of DCM-604 including Setup, DHCP and Backup

5.3.1 Setup

This setup page allows configuring the basic features of the broadband gateway related to your ISP's connection.

Status **Basic** Advanced Firewall Parental Control Wireless MTA Logout

D-Link

Basic

Setup
This page allows configuration of the basic features of the broadband gateway related to your ISP's connection.

Network Configuration

LAN
IP Address: 192 . 168 . 0 . 1
MAC Address: 00:10:18:de:ad:05

WAN
IP Address:
MAC Address: 00:30:54:d5:a5:1a
Duration: D: -- H: -- M: -- S: --
Expires:
Release WAN Lease Renew WAN Lease

WAN Connection Type: DHCP

Host Name: (Required by some ISPs)
Domain Name: (Required by some ISPs)
MTU Size: 0 (256-1500 octets, 0 = use default)
Spoofed MAC Address: 00 . 00 . 00 . 00 . 00 . 00
Apply

©2008 D-Link. All rights reserved.

5.3.2 DHCP

The DHCP page allows you to activate/deactivate the DHCP server function of the DCM-604, and, if the DHCP server is activated, to see DHCP leases it has provided.

Status **Basic** Advanced Firewall Parental Control Wireless MTA Logout

D-Link

Basic

DHCP
This page allows configuration and status of the optional internal DHCP server for the LAN.

DHCP Server: Yes (selected) No
Starting Local Address: 192.168.0.10
Number of CPEs: 245
Lease Time: 3600
Apply

DHCP Clients

MAC Address	IP Address	Subnet Mask	Duration	Expires	Select
0024e8927152	192.168.0.011	255.255.255.000	D:00 H:01 M:00 S:00	-----	<input type="radio"/>

Current System Time: -----
Force Available

WINS Addresses
Add Primary Add Secondary Add Tertiary
Primary: 0.0.0.0
Secondary: 0.0.0.0
Tertiary: 0.0.0.0
Remove WINS Address Clear All

©2008 D-Link. All rights reserved.

With this function activated, your cable service provider's DHCP server provides one IP address for the DCM-604, and the DCM-604's DHCP server provides IP addresses, starting at the address you set in **Starting Local Address** field, to your PCs. A DHCP server leases an IP address with an expiration time.

To set the maximum number of PCs to which the DCM-604 will issue IP addresses, enter it in the **Number of CPEs** box and then click **Apply**. (CPE is another term sometimes used for PC.)

The table on the bottom of this page shows the information of DHCP clients including the IP and MAC addresses of each PC. Since MAC addresses are unique and permanently fixed into hardware, you can identify any PC listed by its MAC address. The DCM-604 provides leases for 3600 seconds (default), and has an automatic renewal mechanism that will keep extending a lease as long as the associated PC remains active.

You can cancel an IP address lease by selecting it in the DHCP Client Lease Info list and then clicking the **Force Available** button. If you do this, you may have to perform a DHCP Renew on that PC, so it can obtain a new lease.

5.3.3 Backup

This page allows you to save your current settings locally on your PC, or restore previously saved settings.

©2008 D-LINK. All rights reserved.

5.4 Advanced

The Advanced page allows you to enable/disable some advanced features of the DCM-604.

5.4.1 Options

The Options page allows you to enable/disable some advanced features supported by DCM-604.

The screenshot shows the D-Link Advanced Options configuration page. The navigation menu on the left includes: Options, IP Filtering, Port Filtering, Forwarding, Port Triggers, and DMZ Host. The main content area is titled "Advanced" and "Options". Below the title, there are several checkboxes for enabling or disabling features:

- WAN Blocking: Enable
- IPsec PassThrough: Enable
- PPTP PassThrough: Enable
- Remote Config Management: Enable
- Multicast Enable: Enable
- UPnP Enable: Enable

Below these options is a section for "PassThrough Mac Addresses (example: 01:23:45:67:89:AB)". It includes an "Add Mac Address" button and a text input field. Below the input field, it says "Addresses entered: 0/32". At the bottom of this section are "Remove Mac Address" and "Clear All" buttons.

©2008 D-LINK. All rights reserved.

Check the option you want to use and click **Apply** button to enable the function(s).

- **WAN Blocking:** To prevent others on the WAN side from being able to ping your DCM-604. With WAN Blocking on, your DCM-604 will not respond to pings it receives, effectively "hiding" your gateway.
- **IPSec Pass-through:** To enable IPSec type packets to pass through between WAN and LAN.
- **PPTP Pass-through:** To enable PPTP type packets to pass through between WAN and LAN.
- **Remote Config Management:** To make the Web Management pages of your DCM-604 accessible from the WAN side. Page access is limited to only those who know the DCM-604 access password you set in the **Status--Security** page.
When accessing the DCM-604 from a remote location, you must use HTTP port 8080 and your IP address. This is the "WAN IP address" that appears at the **Basic--Setup** page. For example, if this IP address were 211.20.15.28, you would navigate to [http:// 211.20.15.28:8080](http://211.20.15.28:8080) to reach the DCM-604's Web Management page from a remote location.
- **Multicast Enable:** To enable multicast traffic to pass through between WAN and LAN. You may need to enable this to see some types of broadcast streaming and content on the Internet, such as webcasting of a popular live event.
- **UPnP Enable:** UPnP (Universal Plug and Play) offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and everywhere in between.

5.4.2 IP Filtering

The IP Filtering page enables you to enter the IP address ranges of PCs on your LAN that you don't permit to have outbound access ability to the WAN. These PCs can still communicate with each other on your LAN, but packets they originate to WAN addresses are blocked by the DCM-604.

D-Link Advanced

IP Filtering
This page allows configuration of IP address filters in order to block internet traffic to specific network devices on the LAN.

Start Address	End Address	Enabled
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>

Apply

©2008 D-LINK. All rights reserved.

To enable IP Filtering feature of DCM-604, check the **Enable** box and click **Apply** button.

5.4.3 Port Filtering

The Port Filtering page allows you to enter ranges of destination ports (applications) that you don't want your LAN PCs to send packets to. Any packets your LAN PCs send to these destination ports will be blocked. For example, you could block access to worldwide web browsing (HTTP port 80) but still allow email service (SMTP port 25 and POP3 port 110).

D-Link Advanced

Port Filtering
This page allows configuration of port filters in order to block specific internet services to all devices on the LAN.

Start Port	End Port	Protocol	Enabled
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>

Apply

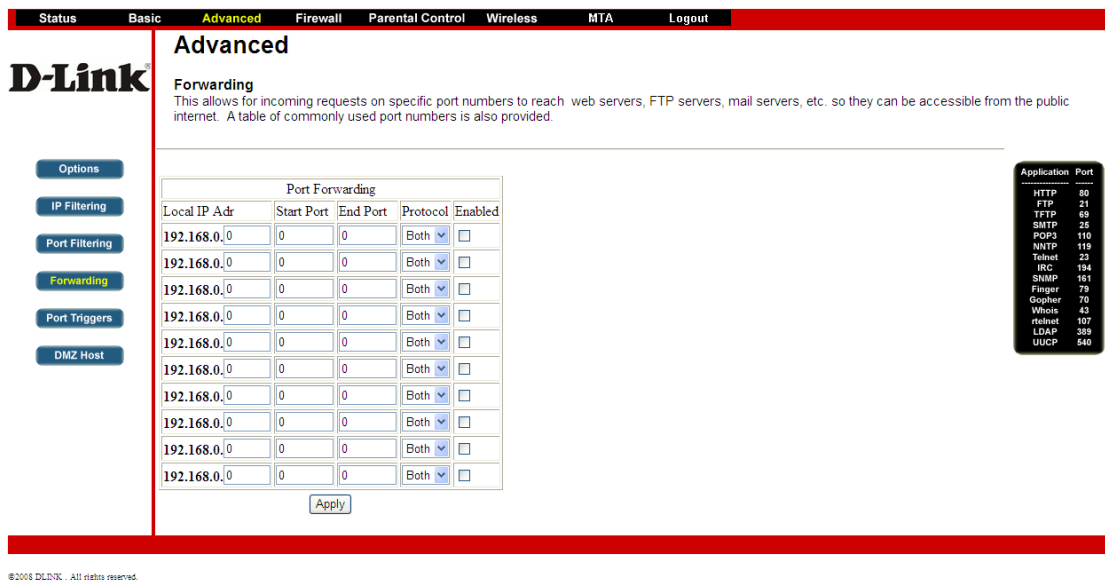
©2008 D-LINK. All rights reserved.

To enable port filtering, enter the **Start port** and **End port** for each range. Then select its protocol from the drop-down list and check the **Enable** box, and click **Apply** button. To block only one port, set both Start and End ports the same.

5.4.4 Forwarding

For communications between LAN and WAN, the DCM-604 normally only allows you to originate an IP connection with a PC on the WAN; it will ignore attempts of the WAN PC to originate a connection onto your PC. This protects you from malicious attacks from outsiders. However, sometimes you may wish for anyone outside to be able to originate a connection to a particular PC on your LAN if the destination port (application) matches one you specify.

The Forwarding page allows you to specify up to 10 rules.



Advanced

Forwarding
This allows for incoming requests on specific port numbers to reach web servers, FTP servers, mail servers, etc. so they can be accessible from the public internet. A table of commonly used port numbers is also provided.

Options
IP Filtering
Port Filtering
Forwarding
Port Triggers
DMZ Host

Port Forwarding				
Local IP Addr	Start Port	End Port	Protocol	Enabled
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>

Apply

Application	Port
HTTP	80
FTP	21
TFTP	69
SMTP	25
POP3	110
NNTP	119
Telnet	23
IRC	194
SNMP	161
Finger	79
Gopher	70
Whois	43
rsh/rlogin	107
LDAP	389
UUCP	540

©2008 D-Link. All rights reserved.

Using the Port Forwarding page, you can provide local services (web servers, FTP servers, mail servers, etc) for people on the Internet or play Internet games. A table of commonly used port numbers is also provided.

5.4.5 Port Triggers

The Port Triggers page allows you to configure dynamic triggers to specific devices on the LAN. This allows for special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messaging program features may require these special settings.

Advanced

Port Triggers
This page allows configuration of dynamic triggers to specific devices on the LAN. This allows for special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messaging program features may require these special settings.

Trigger Range		Target Range		Protocol	Enable
Start Port	End Port	Start Port	End Port		
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>

Apply

©2008 D-LINK. All rights reserved.

Port Triggering is an elegant mechanism that does the forwarding for you, each time you play the game.

You can specify up to 10 port ranges on which to trigger.

5.4.6 DMZ Host

The DMZ page allows you to configure a specific network device to be exposed or visible directly to the WAN (public Internet). Setting a host on your local network as demilitarized zone (DMZ) forwards any network traffic that is not redirected to another host via the port forwarding feature to the IP address of the host (PC). This designates one PC on your LAN that should be left accessible to all PCs from the WAN side for all ports. For example, if you locate a HTTP server on this machine, anyone will be able to access that HTTP server by using your DCM-604's IP address as the destination. This may be used when problem applications do not work with port triggers. The setting of "0" indicates NO DMZ PC.

Advanced

DMZ Host (Exposed Host)
This page allows configuration of a specific network device to be exposed or visible directly to the WAN (public internet). This may be used when problem applications do not work with port triggers. Entering a "0" means there are no exposed hosts.

DMZ Address 192.168.0.0

Apply

©2008 D-LINK. All rights reserved.

5.5 Firewall

The DCM-604 provides built-in firewall functions, enabling you to protect the system against denial of service (DoS) attacks and other unwelcome or malicious accesses to your LAN.

5.5.1 Web Filter

This page allows certain Web-oriented cookies, java scripts, and pop-up windows to be blocked by the firewall. A list of "trusted computers" can also be defined that are not subject to any filters configured. Specific Firewall features can also be enabled. It is highly recommended that the Firewall is left enabled at all times for protection against Denial of Service attacks. Go to the Parental Control page to block internet access to specific sites.

The screenshot shows the D-Link Firewall configuration interface. At the top, there is a navigation bar with tabs: Status, Basic, Advanced, **Firewall**, Parental Control, Wireless, MTA, and Logout. The main header is "Firewall". Below it, the "Web Content Filter" section is active, with a description: "This page allows certain Web-oriented cookies, java scripts, and pop-up windows to be blocked by the firewall. A list of 'trusted computers' can also be defined that are not subject to any filters configured. Specific Firewall features can also be enabled. It is highly recommended that the Firewall is left enabled at all times for protection against Denial of Service attacks. Go to the Parental Control page to block internet access to specific sites." On the left sidebar, there are buttons for "Web Filter", "Local Log", and "Remote Log". The main content area is titled "Web Features" and lists several options with checkboxes: Filter Proxy (unchecked), Filter Cookies (unchecked), Filter Java Applets (unchecked), Filter ActiveX (unchecked), Filter Popup Windows (unchecked), Block Fragmented IP Packets (unchecked), Port Scan Detection (unchecked), IP Flood Detection (checked), and Firewall Protection (checked). An "Apply" button is located at the bottom of the list.

©2008 D-LINK. All rights reserved.

5.5.2 Local Log

The Local Log page allows you to configure the firewall event log reported via email alert, and these attack records are also visible in the table on the bottom of this page.

The screenshot shows the D-Link Firewall configuration interface for the "Local Log" section. The navigation bar is the same as in the previous screenshot, with "Firewall" selected. The main header is "Firewall". Below it, the "Local Log" section is active, with a description: "This page allows configuration of Firewall event log reporting via email alerts and a local view of the attacks on the system." On the left sidebar, there are buttons for "Web Filter", "Local Log", and "Remote Log". The main content area contains configuration fields: "Contact Email Address" (text input), "SMTP Server Name" (text input), and "E-mail Alerts" (checkbox, currently unchecked). An "Apply" button is located below these fields. Below the configuration area, there is a table header with columns: "Description", "Count", "Last Occurrence", "Target", and "Source". Below the table header, there are two buttons: "E-mail Log" and "Clear Log".

©2008 D-LINK. All rights reserved.

Specify the e-mail address and its SMTP of the administrator who needs to receive the notice of any attempted firewall violations. Type the addresses in standard Internet e-mail address format, for example, yourname@onecompany.com. Then check the **Enable** box to enable the alert feature and click Apply button.

Click **E-mail Log** to immediately send the email log. Click **Clear Log** to clear the table of entries for a fresh start.

5.5.3 Remote Log

The screenshot shows the D-Link web interface for the Firewall section. The top navigation bar includes Status, Basic, Advanced, Firewall (highlighted), Parental Control, Wireless, MTA, and Logout. The main content area is titled 'Firewall' and contains a 'Remote Log' section. Below the D-Link logo, there are three buttons: 'Web Filter', 'Local Log', and 'Remote Log' (highlighted). The 'Remote Log' section includes a description: 'This page allows optional configuration of events to be sent to a local SysLog server.' It features a 'Send selected events' section with three checkboxes: 'Permitted Connections', 'Blocked Connections', and 'Product Configuration Events'. Below these is a text input field for the SysLog server IP address, currently showing '192.168.0.0', and an 'Apply' button.

©2008 D-LINK. All rights reserved.

5.6 Parental Control

5.6.1 User Setup

This page allows configuration of users. "White List Only" feature limits the user to visit only those sites specified in the Allowed Domain List in Parental Control, Basic page of his/her content rule. Actually, this page helps you to identify whether or not the Websites are blocked to access.

Status	Basic	Advanced	Firewall	Parental Control	Wireless	MTA	Logout
--------	-------	----------	----------	------------------	----------	-----	--------

D-Link **Parental Control**

User Setup
This page allows configuration of users. 'White List Only' feature limits the user to visit only the sites, specified in the Allowed Domain List of his/her content rule.

User Configuration

User Settings

1. Default Enable

Password

Re-Enter Password

Trusted User Enable

Content Rule White List Access Only 1. Default

Time Access Rule

Session Duration 0 min

Inactivity time 0 min

Trusted Computers
Optionally, the user profile displayed above can be assigned to a computer to bypass the Parental Control login on that computer.

00 : 00 : 00 : 00 : 00 : 00

No Trusted Computers

©2008 D-LINK. All rights reserved.

5.6.2 Basic Setup

This page allows basic selections of rules which block certain Internet content and certain Web sites. When you change your Parental Control settings, you must click on the appropriate "Apply", "Add" or "Remove" button for your new setting to take effect. If you refresh your browser's display, you will see the currently active settings.

Status Basic **Advanced** Firewall **Parental Control** Wireless MTA Logout

D-Link

User Setup
Basic
ToD Filter
Local Log

Parental Control

Basic Setup

This page allows basic selection of rules which block certain Internet content and certain Web sites. When you change your Parental Control settings, you must click on the appropriate "Apply", "Add" or "Remove" button for your new settings to take effect. If you refresh your browser's display, you will see the currently active settings.

Parental Control Activation
This box must be checked to turn on Parental Control
 Enable Parental Control

Content Policy Configuration

Content Policy List
 1. Default

Keyword List	Blocked Domain List	Allowed Domain List
anonymizer	anonymizer.com	
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Add Keyword"/>	<input type="button" value="Add Domain"/>	<input type="button" value="Add Allowed Domain"/>
<input type="button" value="Remove Keyword"/>	<input type="button" value="Remove Domain"/>	<input type="button" value="Remove Allowed Domain"/>

Override Password
If you encounter a blocked website, you can override the block by entering the following password

Password:
 Re-Enter Password:
 Access Duration:

©2008 D-Link. All rights reserved.

5.6.3 Time of Day Filter

This page allows configuration of time access policies to block all internet traffic to and from specific network devices based on time of day setting. And it helps to ensure that the target or connected computer cannot access the internet at all.

You can select Everyday or a day of the week by Enabling the check box and can change the Time to All Day or specific the start and end time by entering the time.

Status Basic **Advanced** Firewall **Parental Control** Wireless MTA Logout

D-Link

User Setup
Basic
ToD Filter
Local Log

Parental Control

Time of Day Access Policy

This page allows configuration of time access policies to block all internet traffic to and from specific network devices based on time of day settings.

Time Access Policy Configuration
Create a new policy by giving it a descriptive name, such as "Weekend" or "Working Hours"

Time Access Policy List
 Enabled

Days to Block
 Everyday Sunday Monday Tuesday
 Wednesday Thursday Friday Saturday

Time to Block
 All day
 Start: (hour) (min)
 End: (hour) (min)

©2008 D-Link. All rights reserved.

5.6.4 Local Log

This page displays Parental Control Local log reporting.

D-Link Parental Control

Event Log
This page displays Parental Control event log reporting.

User Setup
Basic
ToD Filter
Local Log

Last Occurrence	Action	Target	User	Source
-----------------	--------	--------	------	--------

Clear Log

©2008 D-LINK . All rights reserved.

5.7 Wireless

5.7.1 Radio

D-Link Wireless

802.11 Radio
This page allows configuration of the Wireless Radio including current country and channel number.

Enabled Wireless Interfaces: CBV104EHW-A518 (00:03:CF:A4:70:13)

Wireless Enabled

Country: SINGAPORE

Output Power 100%

Channel 6 Current : 6

Apply Restore Wireless Defaults

©2008 D-LINK . All rights reserved.

5.7.2 Primary Network

[Status](#)
[Basic](#)
[Advanced](#)
[Firewall](#)
[Parental Control](#)
[Wireless](#)
[MTA](#)
[Logout](#)

D-Link

Wireless

802.11 Primary Network
This page allows configuration of the Primary Wireless Network and its security settings.

CBV704EW-A518 (00:03:C9:A4:70:13)

Primary Network: Enabled Disabled
 Automatic Security Configuration: Enabled Disabled

Network Name (SSID):

Closed Network: Enabled Disabled

WPA: Enabled Disabled
 WPA-PSK: Enabled Disabled
 WPA2: Enabled Disabled
 WPA2-PSK: Enabled Disabled

WPA/WPA2 Encryption: Enabled Disabled

WPA Pre-Shared Key: Show Key

RADIUS Server:
 RADIUS Port:
 RADIUS Key:

Group Key Rotation Interval:
 WPA/WPA2 Re-auth Interval:

WEP Encryption: WEP (128-bit) WEP (64-bit)

Shared Key Authentication: Optional Disabled

802.1x Authentication: Enabled Disabled

Network Key 1:
 Network Key 2:
 Network Key 3:
 Network Key 4:

Current Network Key:

PassPhrase:

©2008 D-LINK. All rights reserved.

5.7.3 Advanced

This page allows configuration of data rates and WiFi thresholds.

[Status](#)
[Basic](#)
[Advanced](#)
[Firewall](#)
[Parental Control](#)
[Wireless](#)
[MTA](#)
[Logout](#)

D-Link

Wireless

802.11 Advanced
This page allows configuration of data rates and WiFi thresholds.

54g™ Mode:

Basic Rate Set:

54g™ Protection:

XPress™ Technology: Enabled Disabled

Afterburner™ Technology: Enabled Disabled

Rate:

Beacon Interval:

DTIM Interval:

Fragmentation Threshold:

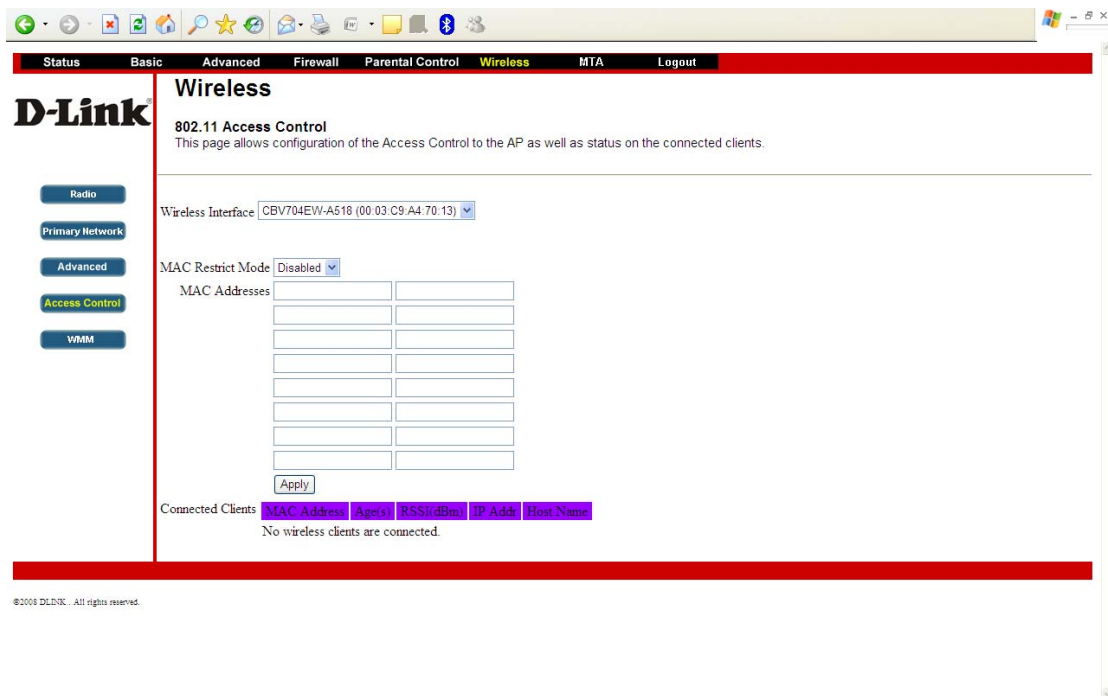
RTS Threshold:

Multicast Rate:

©2008 D-LINK. All rights reserved.

5.7.4 Access Control

This page allows configuration of the Access Control to the AP as well as on the connected clients.



5.7.5 WMM

This page allows configuration of the Wi-Fi Multimedia QoS.

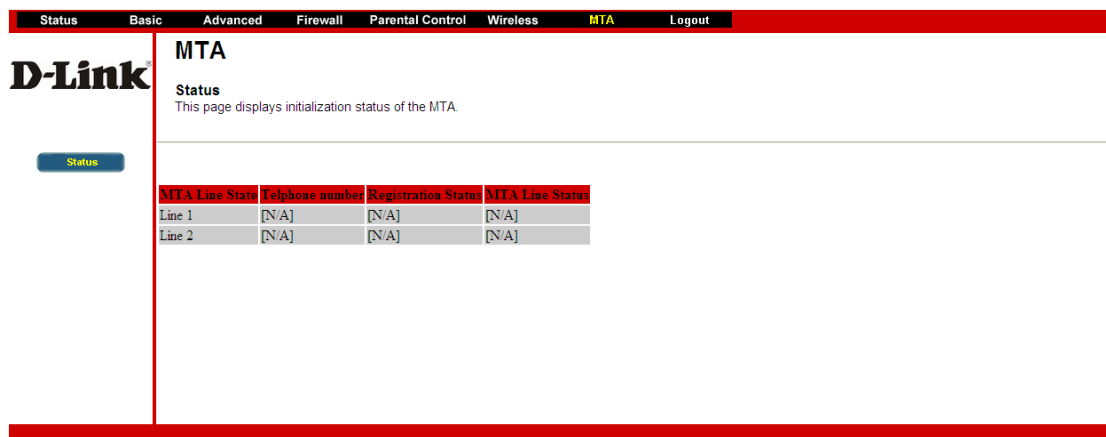
The screenshot shows the D-Link web interface. At the top, there is a navigation bar with tabs: Status, Basic, Advanced, Firewall, Parental Control, **Wireless**, MTA, and Logout. On the left side, there is a sidebar with the D-Link logo and a list of menu items: Radio, Primary Network, Advanced, Access Control, and **WMM**. The main content area is titled "Wireless" and contains the following text: "802.11 Wi-Fi Multimedia" and "This page allows configuration of the Wi-Fi Multimedia QoS." Below this, there are three configuration options, each with a dropdown menu: "WMM Support" set to "On", "No-Acknowledgement" set to "Off", and "Power Save Support" set to "On". An "Apply" button is located below these options.

5.8 MTA

Section MTA has 5 sub-items, which indicate the status of MTA. These information can help you to understand the parameters of MTA operation.

5.8.1 Status

This page displays initialization status of the MTA.



MTA Line State	Telephone number	Registration Status	MTA Line Status
Line 1	[N/A]	[N/A]	[N/A]
Line 2	[N/A]	[N/A]	[N/A]

5.9 Hard Reset

To factory reset the DCM604, press and hold the reset button for at least 10sec

