802.11b/g supports two types of WEP security services: **Open System and Shared key**. Under open system authentication, any wireless station can connect to the Motorola Cellular Gateway NC800 provided that it knows the SSID of the Motorola Cellular Gateway NC800. If the Motorola Cellular Gateway NC800 is broadcasting this information, then any wireless client can access the Motorola Cellular Gateway NC800. Under **Shared Key** the Motorola Cellular Gateway NC800 generates a random 128-bit challenge. The station returns the challenge, encrypted with a shared key—a "secret" key configured into both the station and the Motorola Cellular Gateway NC800. The Motorola Cellular Gateway NC800 decrypts the challenge, using a CRC to verify its integrity. If the decrypted frame matches the original challenge, the station is considered authentic. The challenge/response handshake is repeated in the opposite direction for mutual authentication.

WEP data encryption is a weaker encryption method than that used by WPA-PSK. Either 64-bit or 128-bit keys can be specified. If either WEP **Data Encryption** or **Shared-Key Authentication** is required, one or more WEP encryption keys must be provided. Note that WEP data encryption can be provided even if shared-key authentication is not required and vice versa.
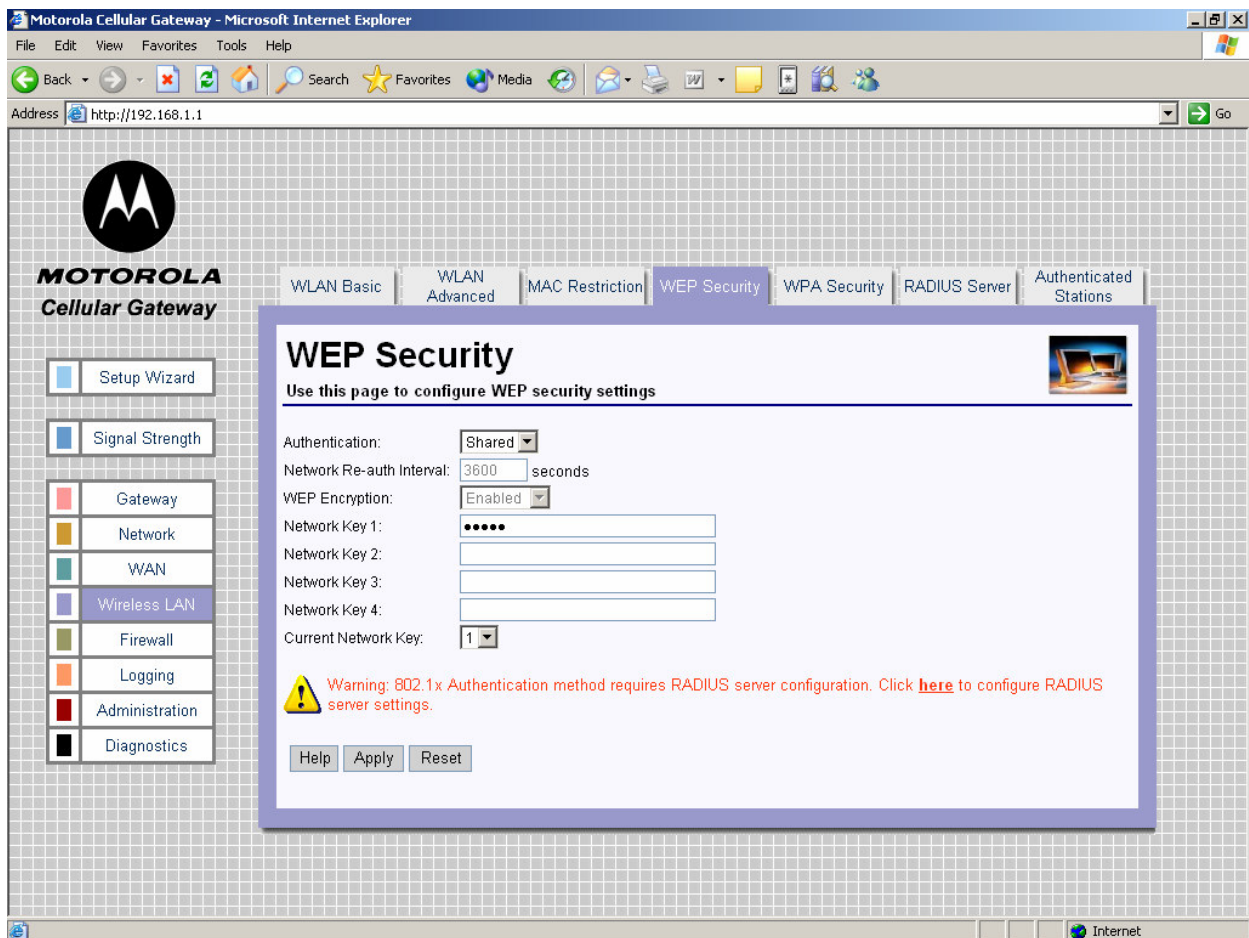
- **Authentication.** - Selects the WEP authentication method.
    - **Open** – all stations are granted access. The default value is Open.
    - **Shared Key** – stations possessing the WEP key are allowed access.
    - **802.1X** – 802.1X is used to perform authentication using a RADIUS server and WEP key distribution.

    Warning: 802.1x Authentication method requires RADIUS server configuration.

- **Network Re-auth interval** – The interval in seconds at which the Motorola Cellular Gateway NC800 distributes a new WEP key. This parameter is valid only if WEP Authentication = 802.1X. The default value is 36000.
- **WEP Encryption**
  - o **Enabled** – data packets are WEP-encrypted.
  - o **Disabled** – WEP encryption is performed.
  - If WEP Authentication = 802.1X, then WEP Encryption = Enabled.
  - The default is Disabled.
- **Network Key (1 – 4)** – Enter up to four different network keys. Only one is in use as determined by the "**Current Network Key**" setting. You can choose between 128-bit or 64-bit WEP encryption. Both allow you to specify up to four keys, but only the selected "**Current Network Key**" is used. If you are using 64-bit WEP encryption, then the key must be exactly 10 hexadecimal or 5 ASCII characters in length. If you are using 128-bit WEP encryption, then the key must be exactly 26 hexadecimal or 13 ASCII characters in length. Valid hexadecimal digits are "0"-"9" and "A"-"F". This is only valid if WEP authentication is not Open, or WEP encryption is enabled. Default is blank for all keys.
  Note: When Authentication is set to 802.1X, only Network Keys 2 or 3 can be used.
- **Current Network Key** – The secret key selected for encrypting outbound traffic and/or authenticating clients. Decimal number between 1 and 4. This is only valid if WEP authentication is not Open, or WEP encryption is enabled. Default is 1.
  Note: When Authentication is set to 802.1X, only Network Keys 2 or 3 can be selected.

> **Warning:** The security settings on the WLAN adapters on the workstations or laptops need to be set up to match the security settings on the Motorola Cellular Gateway NC800. The wireless links between the workstations/laptops and the Motorola Cellular Gateway NC800 need to be restarted after the security settings have been changed.

Wireless LAN-> WPA Security

This page allows you to configure the Motorola Cellular Gateway NC800's WPA Security settings.

> **Warning:** The settings on this page become effective only if the **Wireless LAN Interface** is set to **Enable** on the **Gateway-> Basic Settings** page and Authentication is set to **Open** on the **Wireless LAN-> WEP security**.

The Motorola Cellular Gateway NC800 supports WLAN Protected Access (WPA), WPA2 (an extension of WPA, based on 802.11i) and WPA Pre-Shared Key (WPA-PSK) authentication methods. WPA, WPA2 and WPA-PSK are all more secure than WEP. The encryption methods that can be used are Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES) or both. AES is more secure, but is only supported by newer WLAN devices.

If the authentication method is WPA-PSK, a pre-shared key is entered into the Cellular Gateway NC800, and an external RADIUS server is not needed. If the authentication method is not WPA-PSK, an external RADIUS server is required to perform authentication and key distribution.

- **WPA Authentication**– Enables or Disables WPA/WPA2 authentication method.
- **WPA Pre-authentication**
  - o Enabled: Allows a WPA2 client to pre-authenticate with the Gateway toward which it is moving, while maintaining a connection to the Gateway it's moving away from.
  - o Disabled: Pre-authentication is disabled.
- **WPA Encryption**
  - o TKIP - Temporal Key Integrity Protocol
  - o AES - Advanced Encryption Standard
  - o TKIP+AES - both enabled
- **WPA-PSK Authentication**
  - o Enabled – Authentication is by possession of a pre-shared key.
  - o Disabled – Authentication requires the use of a higher-layer authentication method supported by a remote authentication server (RADIUS server).
- **WPA Pre-Shared Key –** Sets the WPA Pre-Shared Key (PSK). The key must be between 8 and 63 ASCII characters or 64 hexadecimal digits. Valid hexadecimal digits are "0"-"9" and "A"-"F". This parameter is valid if WPA PSK Authentication is Enabled.
- **Network Re-auth Interval** – The interval, in seconds, at which the gateway will request the WLAN client to re-authenticate itself.
- **Network Key Rotation Interval** – The interval, in seconds, at which a new group key (GTK) is distributed. A value of 0 means there is no periodic GTK distribution.

⚠ **Warning:** The security settings on the WLAN adapters on the workstations or laptops need to be set up to match the security settings on the Motorola Cellular Gateway NC800. The wireless links between the workstations/laptops and the Motorola Cellular Gateway NC800 need to be restarted after the security settings have been changed. WPA-PSK can only be used on the Motorola Cellular Gateway NC800 if the clients support it.
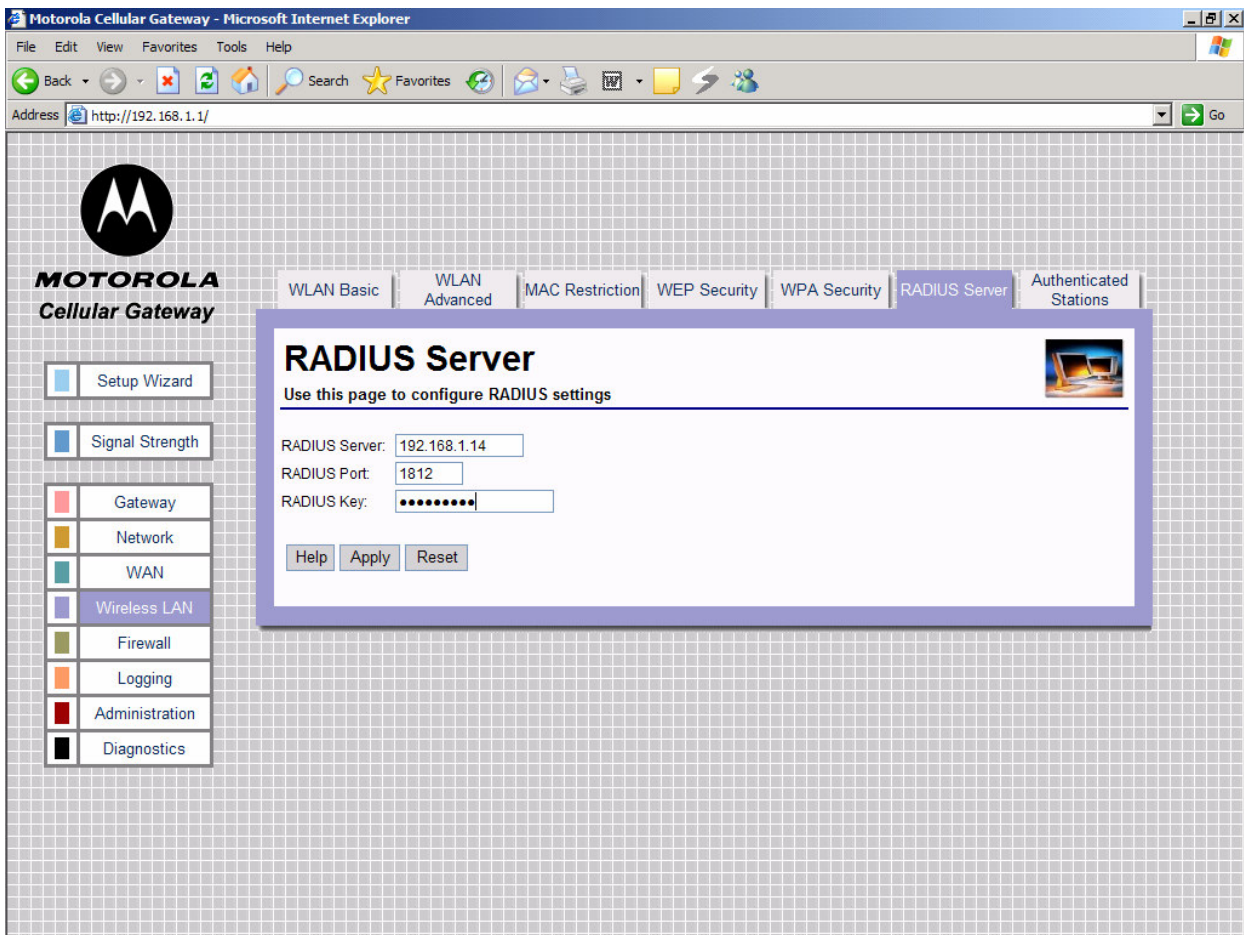
Wireless LAN-> RADIUS Server

This page allows you to configure the Motorola Cellular Gateway NC800's RADIUS Server Security settings.

⚠️ **Warning:** The settings on this page become effective only if the **Wireless LAN Interface** is set to **Enable** on the **Gateway-> Basic Settings** page.

If WPA is enabled but PSK Authentication is disabled, or if the WEP authentication method is 802.1X, then an external RADIUS server is required to perform authentication. Settings here have to match those on the external RADIUS Server.

- **RADIUS Server** – Sets IP address of the RADIUS server, which acts as the Authentication Server. Decimal numbers are specified in dotted notation.
- **RADIUS Port** – Sets the UDP port number of the RADIUS server. Decimal number between 0 and 65535.
- **RADIUS Key –** The shared secret key for the RADIUS connection. Maximum 255 characters.

Wireless LAN-> Authenticated Stations

This page allows you to configure the Motorola Cellular Gateway NC800's Authenticated Stations Security settings.

Warning: The information on this page is only updated when the **Wireless LAN Interface** is set to **Enable** on the **Gateway-> Basic Settings** page.

The Motorola Cellular Gateway NC800 displays a list of authenticated WLAN stations. This is a display of the current WLAN status. No settings can be made on this page.
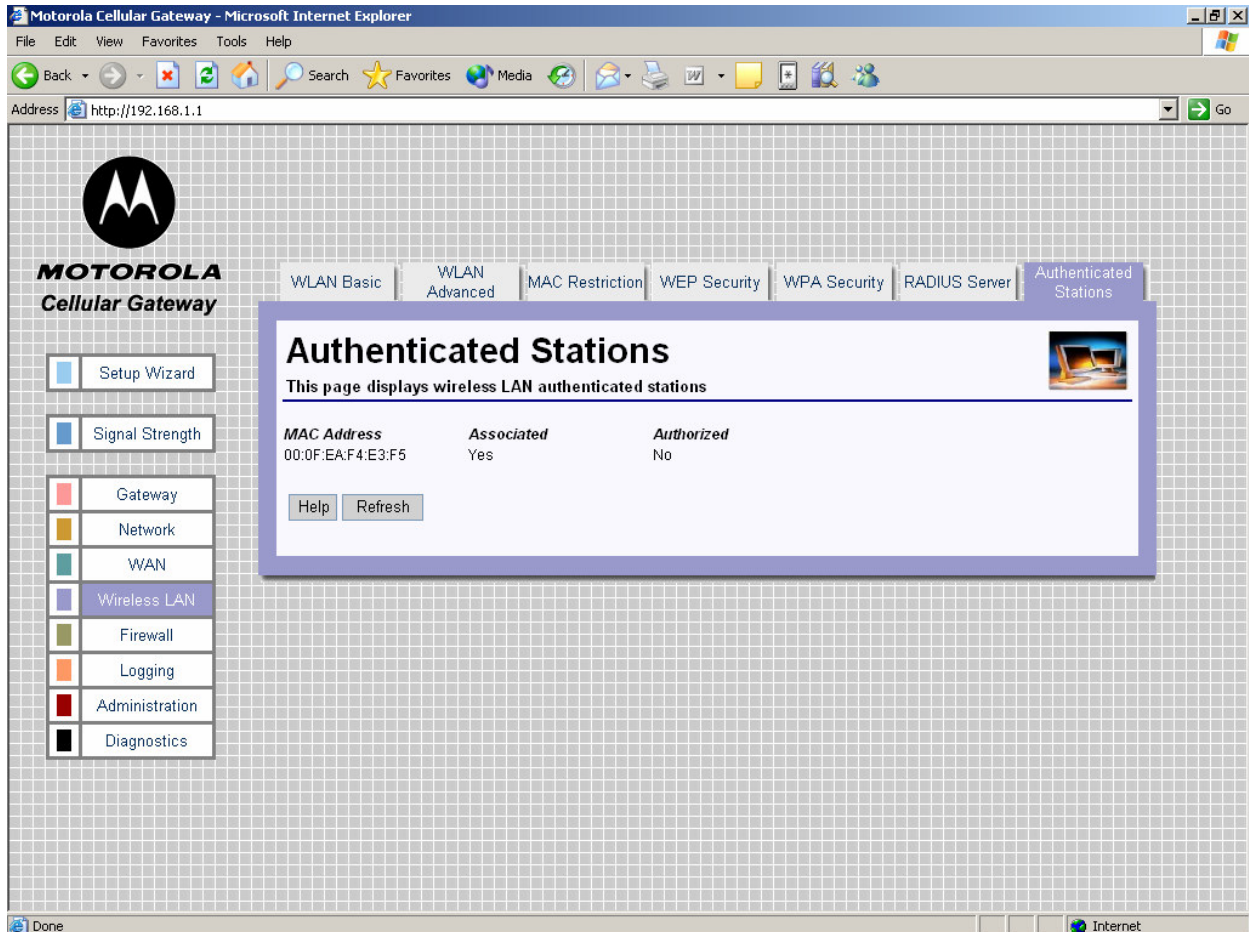
- **MAC Address** – The MAC address of the WLAN station.
- **Associated** – **Yes** or **No** is used to indicate whether WLAN station has been associated with the Motorola Cellular Gateway NC800. A WLAN station becomes associated with the Gateway when the user selects the Gateway's SSID.
- **Authorized** – **Yes** or **No** is used to indicate whether WLAN station has been authorized to use LAN resources. A WLAN station becomes authorized when it successfully completed WPA or 802.1x authentication. If WPA and 802.1x are disabled on the Gateway this field will always be No, even when the client has successfully connected to the Gateway.

Special Buttons:
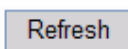
Refresh | Refreshes the list to the most recent status.

Firewall

The firewall on the Motorola Cellular Gateway NC800 is a security software system that enforces an access control policy between the Internet and the Motorola Cellular Gateway NC800 LAN. A firewall determines which information passes in and out of the network.

There are five pages in the Firewall category:

Firewall-> Permanent Port Forwarding If external users from the Internet need to have access to certain services on the LAN connected to the Motorola Cellular Gateway NC800, then the relevant ports and the addresses of the devices providing those services are specified on this page.

Firewall-> Application Port Forwarding Some services provided to external users from the Internet need to use different ports for inbound and outbound traffic. The relevant ports and the addresses of the devices where these applications are running are specified on this page.

Firewall-> MAC Address Filtering If certain devices on the LAN must be prevented from accessing the Motorola Cellular Gateway NC800, then their MAC addresses can be specified on this page.

Firewall-> Port Filtering If access to the Internet must be restricted, then the relevant information is entered on this page.

Firewall-> DMZ Host If a DMZ host is provided, its IP address is specified on this page.

Firewall-> Permanent Port Forwarding

This function allows external users from the Internet to have WAN access to public services on the LAN network. These public services are specialized Internet applications such as Web servers, FTP servers and e-mail servers. These types of requests from the external users are forwarded by the Motorola Cellular Gateway NC800 to the appropriate computer on the LAN network.

No port forwarding takes place unless at least one entry exists in the port forwarding table. Any incoming packet that does not match the port numbers on the incoming WAN interface is dropped.
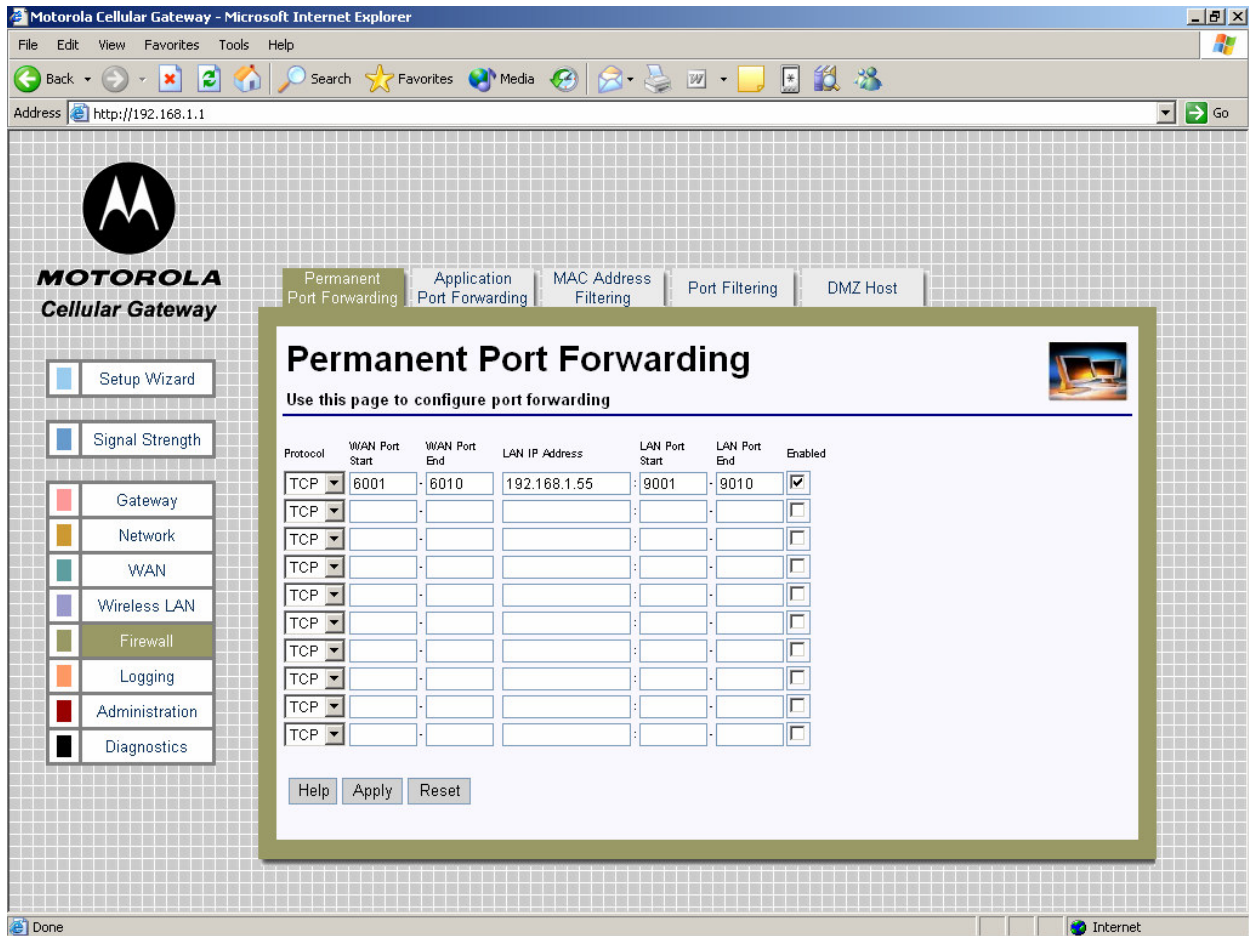
You can specify up to 10 port forwarding entries:

- **Protocol** – Select TCP or UDP for the protocol to be forwarded.
- **WAN Port Start** – The start of the range of port numbers at the incoming WAN interface. To configure a single port number, leave the starting or ending port number empty. Decimal numbers between 0 and 65535.
- **WAN Port End** – The end of the range of port numbers at the incoming WAN interface. To configure a single port number, leave the starting or ending port number empty. Decimal numbers between 0 and 65535.
- **LAN IP Address** – The IP address of the server on the LAN to forward the packet to. Decimal number specified in dotted notation.
- **LAN Port Start** – The start of the range of port numbers at the outgoing LAN interface. Decimal numbers between 0 and 65535.
- **LAN Port End** – The end of the range of port numbers at the outgoing LAN interface. To configure a single port number leave the starting or ending port number empty. Decimal numbers between 0 and 65535.
- **Enabled** – Tick this box to activate the entry.

Port forwarding is an advanced function. No changes should be made to the settings without a thorough understanding of the relevant networking concepts.

Any PC exposed to the Internet using the Permanent Port Forwarding feature should have its DHCP client functionality disabled and should have a new static IP address assigned to it. This is because its IP address may change when using the DHCP function.

Firewall-> Application Triggered Port Forwarding

Some programs, such as Internet games and videoconferencing, require multiple ports for data transmission. Data transmitted using File Transfer Protocol (FTP), for example, is sent from your computer via one port and related data (e.g. an acknowledgement of receipt of data) returns via another port. These multiple port transmissions may cause problems with network address translation (NAT) because the NAT service anticipates that packets related to data sent via one port will return to the same port.

If you are having trouble running a particular program on your network, you may need to establish application-triggered port forwarding for that program. Essentially, application-triggered port forwarding tells the Motorola Cellular Gateway NC800 how to direct traffic across networks.

To configure port forwarding for a specific program, you must specify the protocol that the application uses, the outbound port from which data associated with that particular protocol should be sent, and the inbound port or ports to which related data will return. When the Motorola Cellular Gateway NC800 receives a data packet from the wide area network that uses the specified protocol, it sends the packet to the client on your network that is currently using the program.

The inbound ports that you specify will open only when data is sent from the corresponding outbound port. These ports will close again after a certain amount of time has elapsed with no data sent to the inbound port. You can specify one port or a range of ports.

You can only establish application-triggered port forwarding for programs that use the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP).

To identify the protocol that a program uses and the ports to which the data should be sent, consult the documentation for that program.

The Motorola Cellular Gateway NC800 additionally allows Inbound port(s) to be mapped to the actual application inbound ports. These mapped ports are configured in the **To Port** fields.

You can specify up to 10 Application Triggered port forwarding entries.

- **Outbound Protocol** – The outbound protocol (TCP or UDP) used by the application.
- **Outbound Port Start** – The start of the range of outbound port numbers used by the application. Valid values are 0 – 65535.
- **Outbound Port End** – The end of the range of outbound port numbers used by the application. To configure a single mapped port number leave the starting or ending mapped port number empty. Valid values are 0 – 65535.
- **Inbound Protocol** – The inbound protocol (TCP or UDP) used by the application.
- **Inbound Port Start** – The start of the range of port numbers on which responses can be received. Valid values are 0 – 65535.
- **Inbound Port End** – The end of the range of port numbers on which responses can be received. To configure a single UDP port number, leave the starting or ending inbound port number empty.
- **To Port Start** – The start of the range of application port numbers to which the inbound ports are mapped. This mapping is optional. Valid values are 0 – 65535.
- **To Port End –** The end of the range of application port numbers to which the inbound ports are mapped. This mapping is optional. To configure a single mapped port number leave the starting or ending mapped port number empty. Valid values are 0 – 65535.
- **Enabled –** Tick this box to activate the entry.

Port forwarding is an advanced function. No changes should be made to the settings without a thorough understanding of the relevant networking concepts.

Any PC exposed to the Internet using the Application Triggered Port Forwarding feature should have its DHCP client functionality disabled and should have a new static IP address assigned to it. This is because its IP address may change when using the DHCP function.

Firewall-> MAC Address Filtering

If you want to block specific users from accessing the Motorola Cellular Gateway NC800 via the LAN interface then you can use the **MAC Address Filtering** feature.

A MAC address is a 12-digit code assigned to a unique piece of hardware for identification, like a social security number. The MAC address component is fixed and is independent of the component's IP address. This means that you can block a specific component irrespective of the component's IP address.

The Motorola Cellular Gateway NC800 supports up to 20 MAC filtering entries.

- **MAC Filter Mode**
  - **Disabled –** No MAC filtering is done.
  - **Allow –** Allow only the specified MAC addresses access to the LAN interface. This is the most secure method, but requires you to add each MAC address individually. It has the advantage that all unknown MAC addresses are blocked.
  - **Deny –** Prevent the specified MAC addresses from accessing the LAN interface. Use this method to block specific users.

- • **LAN MAC Filters –** You can specify a list of up to 20 MAC addresses that will be filtered according to the MAC Filter Mode. MAC Addresses must be in the format xx:xx:xx:xx:xx:xx where xx are Hexadecimal digits.

If the MAC address list is empty you must set the **MAC Filter Mode** to **Disabled** or **Deny.** An empty MAC address table does not allow LAN workstations to communicate with the Motorola Cellular Gateway NC800 if the **MAC Filter Mode** field is not set to **Disabled** or **Deny**.

Firewall-> Port Filtering

This function blocks specific internal users (on the LAN side) from accessing the Internet (on the WAN side). TCP and/or UDP packets are filtered on any combination of the following:

- • The source IP address
- • The destination port number (UDP or TCP)
- • Day of the Week
- • Time of the Day

You can specify up to 10 TCP/UDP packet filters.

- **LAN IP Address Range** – The IP address range of LAN users to block. To configure a single IP address leave the first or second entry empty. To block TCP/UDP ports for all LAN users type * in the IP address fields. Dotted-Decimal notation must be used.
- **Protocol** – The protocol type (TCP or UDP) for this LAN IP Address Range.
- **Destination Port Range** – The start and end port numbers of the range of ports to block for LAN users. Decimal numbers between 0 and 65535 only.
- **From Day** – Select the day of the week to activate the filter.
- **To Day** – Select the day of the week to deactivate the filter (the filter is still active for this day, but not from the next day onwards).
- **From Hour** – Select the hour of the day to activate the filter.
- **To Hour** – Select the hour of the day to deactivate the filter (the filter is still active for this hour, but not from the next hour onwards).
- **Enabled –** Tick this box to activate the entry.

Firewall-> DMZ Host

This feature allows *a single* computer on your local network to be exposed to all users on the Internet allowing unrestricted two-way communication. The host computer therefore exists in a demilitarised zone (DMZ) and bypasses all the firewall security. You may want to expose a single computer to allow certain applications such as internet-gaming and video conferencing using for example Microsoft's NetMeeting.
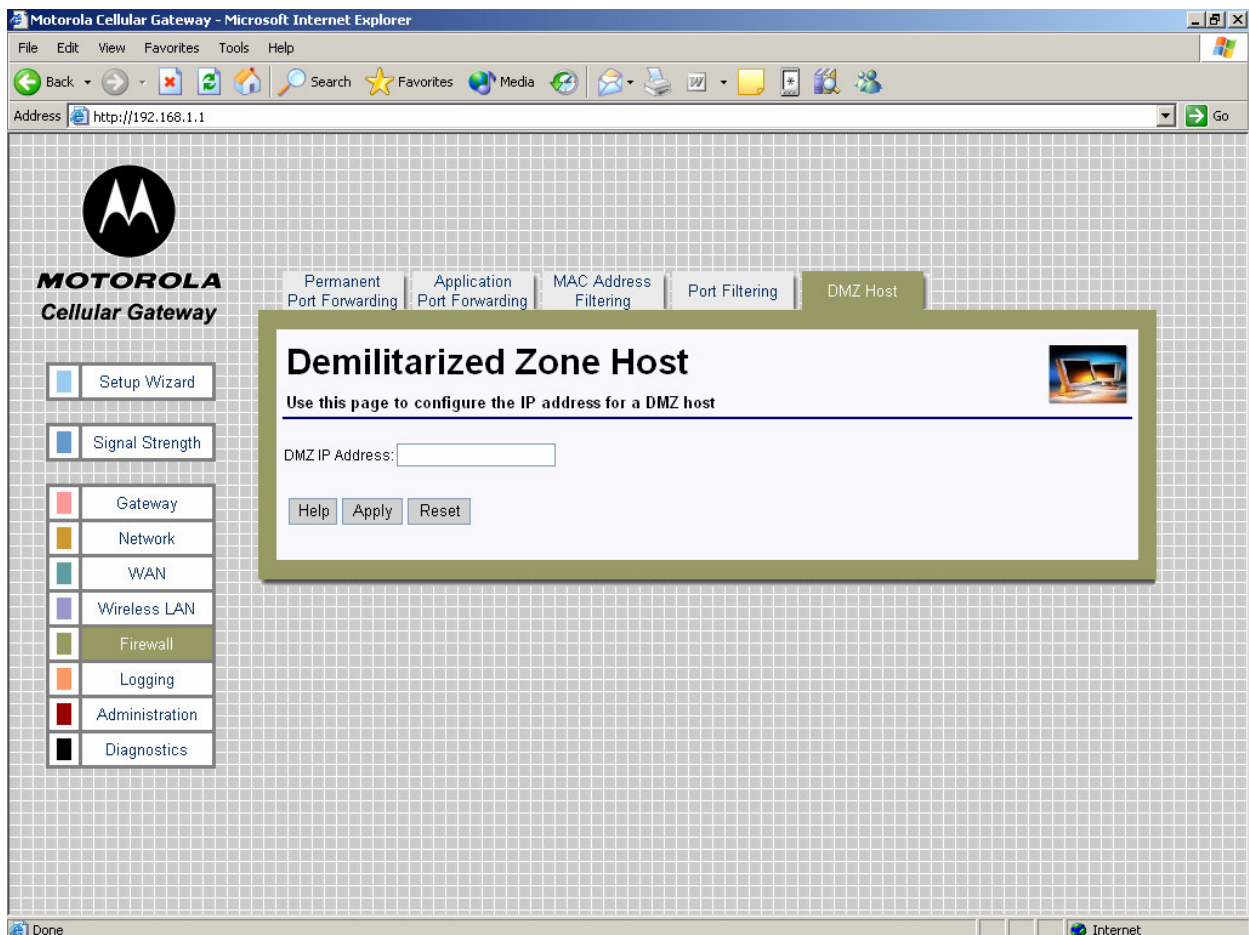
DMZ hosting forwards all the ports (TCP and UDP) at the same time to one specified computer.

- **DMZ IP Address –** The only setting required is the IP address of the computer to expose to the Internet. The exposed computer will receive all data packets that are sent to the Motorola Cellular Gateway NC800's WAN IP address. Leave this blank if you do not want to specify a DMZ Host. Decimal number specified in dotted notation.

⚠️ **Important:** DMZ Hosting is an Advanced function. No changes should be made without a thorough understanding of networking concepts.

⚠️ **Warning:** Any Internet user who knows this address can connect to the exposed computer. There are methods to scan for open ports on the exposed computer so using this feature is a security risk.

💡 Any PC exposed to the Internet using the DMZ Host feature should have its DHCP client functionality disabled and should have a new static IP address assigned to it. This is because its IP address may change when using the DHCP function.

Logging

There are three pages in the Logging category:

Logging-> Statistics Logging   This page is used to start statistics collection.
Logging-> Internet Site Logging   This page is used to start logging of connections
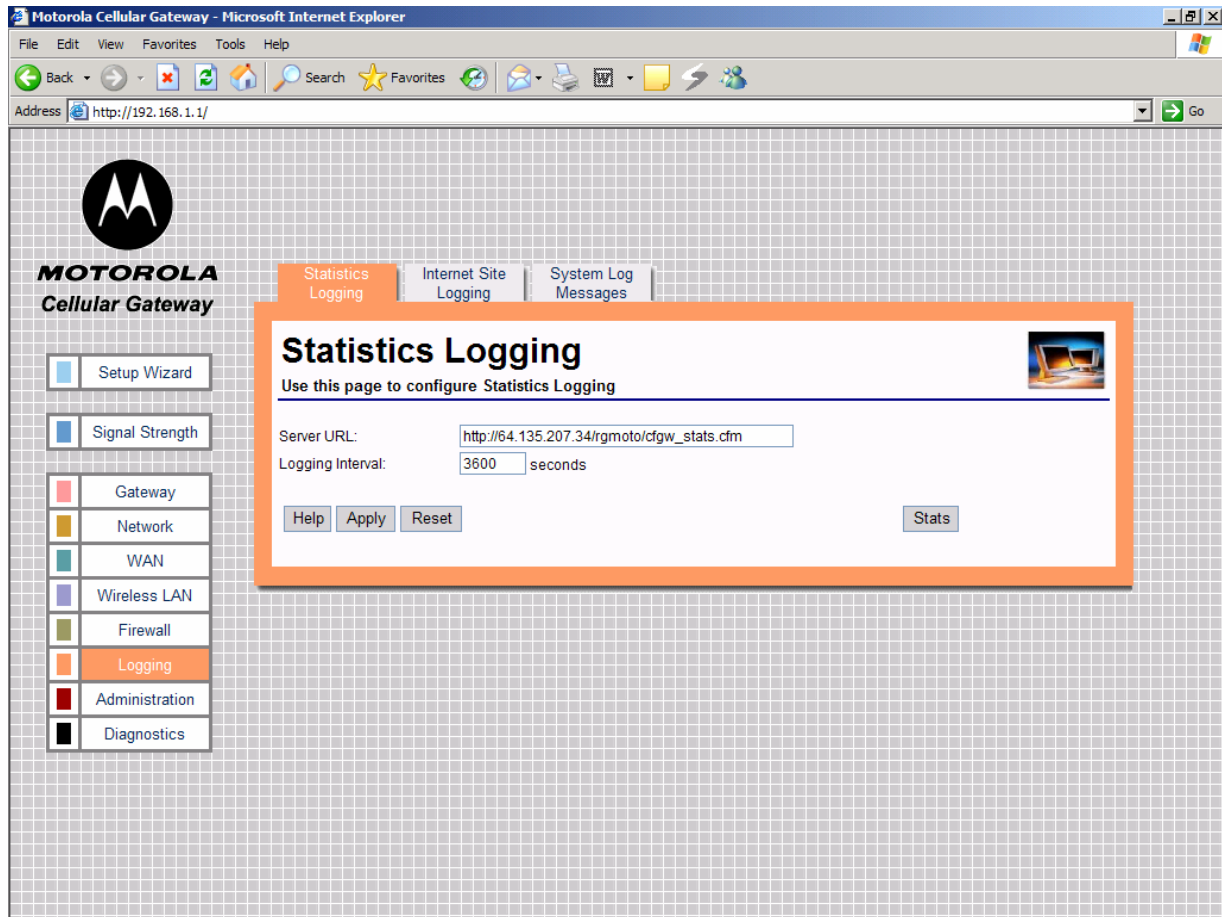**Logging-> System Log Messages**   This page is used to start logging of system messages.

Logging-> Statistics Logging

You can configure the Motorola Cellular Gateway NC800 to periodically log Statistic Information to a web-server running a script that is supplied on the CD accompanying the Motorola Cellular Gateway NC800. Refer to Section 7 in this document for a description of the contents of the statistics files that are generated if the feature on this page is enabled. Section 7 also provides more information on how to set up a Web server.

💡 The statistics logging server URL will be provided to you by your ISP if it has not already been configured by default on the Motorola Cellular Gateway NC800.

- **Server URL** – the full URL of the script that is used for statistics logging. You should set this to be: http://<IP>/Moto3G/gateway_stats.asp where <IP> is the IP address of the server that is running the statistics logging script and **Moto3G** is the name of the directory on the web server where the script is stored. Maximum of 4095 characters beginning with the string "http://". The Statistics Server can be located on the local LAN or anywhere on the Internet.
- **Logging Interval** – The interval in seconds between logging of statistics. Decimal value between 60 and 65535. Default is 3600 seconds (1 hour).

Special Buttons:

   Send the statistics information immediately.

You can configure the Motorola Cellular Gateway NC800 to periodically log all incoming and outgoing URLs accessed through the Motorola Cellular Gateway NC800 to a web-server running a script that is supplied on the CD accompanying the Motorola Cellular Gateway NC800. Refer to Section 7 in this document for a description of the contents of the logging files that are generated if the feature on this page is enabled. Section 7 also provides more information on how to set up a Web server.

The Internet Site logging server URL will be provided to you by your ISP if it has not already been configured by default on the Motorola Cellular Gateway NC800.


- **Server URL** – the full URL of the script that is used for statistics logging. You should set this to be: http://<IP>/Moto3G/gateway_stats.asp where <IP> is the IP address of the server that is running the statistics logging script and **Moto3G** is the name of the directory on the web server where the script is stored. Maximum of 4095 characters beginning with the string "http://". The Statistics Server can be located on the local LAN or anywhere on the Internet.
- **Logging Interval** – The interval in seconds between logging of statistics. Decimal value between 60 and 65535. Default is 3600 seconds (1 hour).
- **Internet Site Log Level**
  - ○ **Disabled –** Do not log any information.
  - ○ **Denied –** Log only those connections that are denied by the Motorola Cellular Gateway NC800's firewall.
  - ○ **Accepted –** Log only those connections that are accepted by the firewall.
  - ○ **Both –** Log all denied and accepted connections.

- **Logging Timer Interval** – The interval in seconds between logging of statistics. Decimal value between 60 and 65535. Default is 3600 seconds (1 hour).
- **Connection Log** – Display the current contents of the connection log. This log contains a maximum of 16KB of information. If the log is full, the oldest information is overwritten.

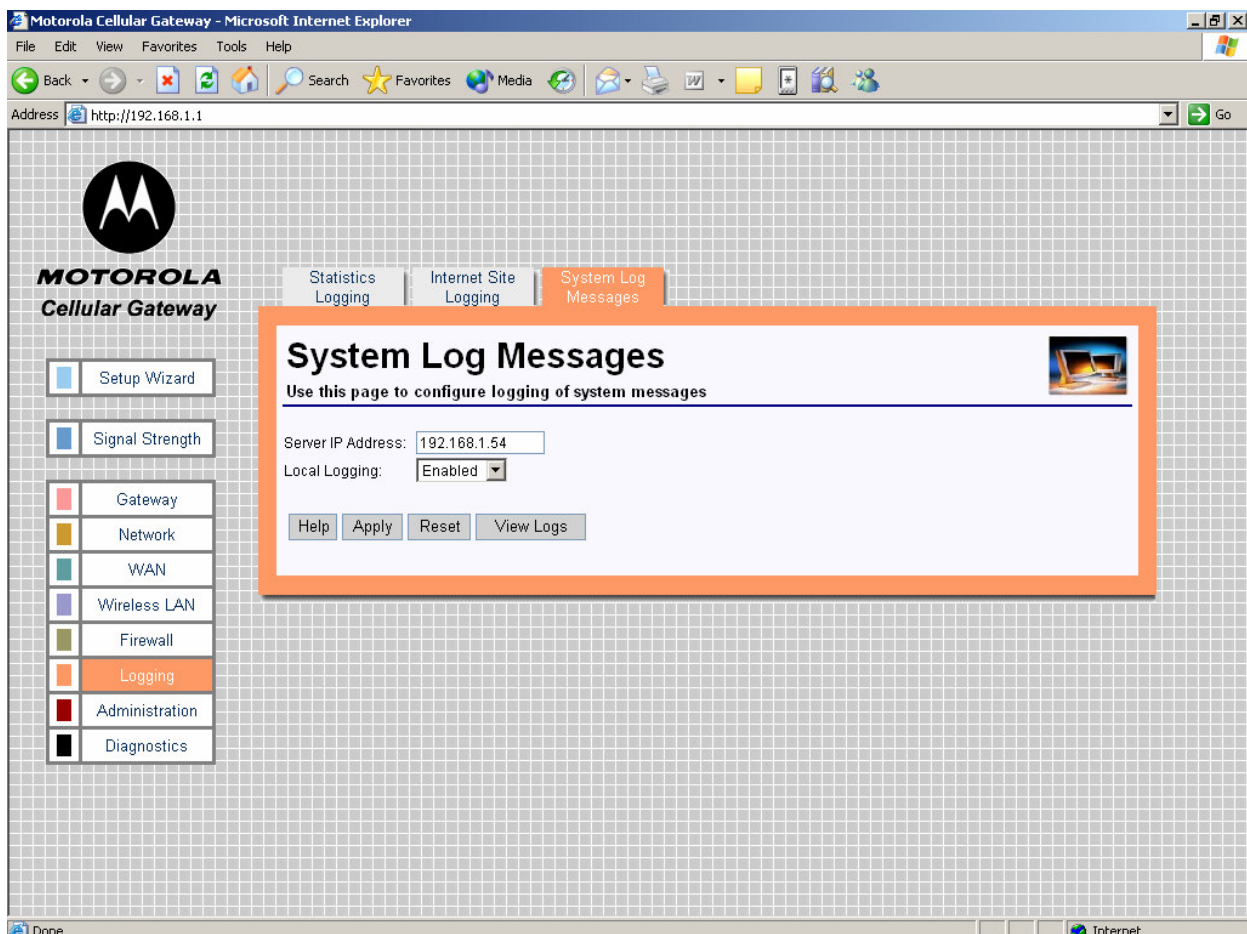**Special Buttons:**

| Log | Send the log information immediately. |

Logging-> System Log Messages

The Motorola Cellular Gateway NC800 generates system log messages that contain information on Motorola Cellular Gateway NC800 events and errors.

You can log these messages to a server that is running a program that can receive and process the messages. Under Linux this program is called a Syslog Daemon. Windows does not natively support syslog messages, but you can download and install programs from the Internet to process syslog messages. Refer to Section 7 in this document for an example of system log messages that are generated if the feature on this page is enabled. Section 7 also provides more information on how to set up a Syslog Interpreter.

The system logging server URL will be provided to you by your ISP if it has not already been configured by default on the Motorola Cellular Gateway NC800.

- **Server IP Address** – The IP address of the system log server. If you do not want to log any system messages, leave this field empty. The server should be on the same subnet as the LAN network.
- **Local Logging**
    - **Enabled** – All events and alarms are written to a circular buffer which can be displayed on the Motorola Cellular Gateway NC800 upon request.
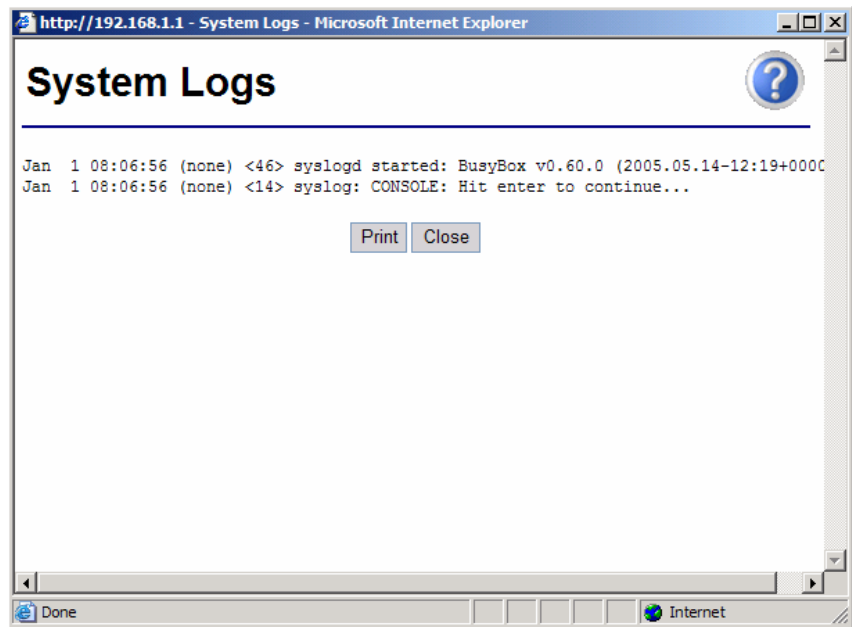   - **Disabled** – No circular logging takes place.

A popular Windows Syslog program can be downloaded from: www.kiwisyslog.com
For a comprehensive description of the syslog protocol, see: www.rfc-archive.org/getrfc.php?rfc=3164

Special Buttons:

View Logs — Shows a log of recent events on the Motorola Cellular Gateway NC800.

Administration

There are four pages in the Administration category:

Administration-> Status	This page shows a summary of the current Motorola Cellular Gateway NC800 status.
Administration-> Support Server Registration	This page allows the Support Server Registration to be set.
Administration-> Firmware Upload	A firmware upgrade is initiated from this page.
Administration-> Restore	This returns all the Motorola Cellular Gateway NC800 settings to the factory defaults.

Administration-> Status

This page displays a summary of the current Motorola Cellular Gateway NC800 status; it reflects the data and selections you've entered using the various setup pages.

- **Gateway Identifier** – The MAC address of the primary LAN interface is used as the Motorola Cellular Gateway NC800 identifier.
- **System Up Time** – The up time of the system since the Motorola Cellular Gateway NC800 was booted.
- **Primary LAN Status** – Indicates whether the Ethernet link on the primary LAN interface is up or down.
- **Secondary LAN Status** – Indicates whether the Ethernet link on the secondary LAN interface is up or down.
- **WLAN Status** – The current state of the wireless LAN interface (Enabled / Disabled).
- **WAN Link Status** – The current state of the WAN link. If there is a WAN connection then this will show "Connected".

Special Buttons:

Refresh   Refreshes the list to the most recent status.

Full   Displays the Full Status Information. (see next page)